بسم الله الرحمن الرحيم

مبانی امنیت اطلاعات

انتشارات آتیه نگر

انتشارات آتیه نگر وابسته به بانک ملت

عنوان اثر:مبانی امنیت اطلاعات

پدیدآورنده: شرکت نرم افزاری امن پرداز

سفارش دهنده: اداره کل آموزش بانک ملت

نوبت چاپ: چاپ اول، بهار ۱۳۹۷

چاپ: چاپ خانه بانک ملت

تیراژ : ۱۰۰۰ نسخه

قیمت : ۲۴۰,۰۰۰ ریال

نشانی: خیابان جمهوری اسلامی، حدفاصل چهارراه استانبول و خیابان لاله زار،

روبروی مجتمع تجاری پروانه، پلاک ۳۰۳، اداره کل آموزش بانک ملت

کد پستی : ۱۱۴۵۸۵۶۱۱۴ تلفن: ۱۴- ۳۳۹۱۰۰۱۲ فاکس: ۳۳۹۱۰۰۱۱

مبانی امنیت اطلاعات

گردآوری و تدوین: شرکت نرم افزاری امن پرداز

بازنگری

فهرست مطالب

مقدمه ناشر	۹
پیشگفتار مولف	۱۰
راهنمای مطالعه	۱۱
فصل اول: آشنایی با مفاهیم امنیت اطلاعات	**۱۳**
جلسه اول: مفهوم امنیت اطلاعات و دارایی های اطلاعاتی	**۱۴**
اهداف یادگیری	۱۵
پیش آزمون	۱۶
لزوم برقراری امنیت	۱۸
اطلاعات و انواع آن	۱۸
امنیت اطلاعات	۲۰
عناصر امنیت اطلاعات	۲۱
گام‌های اساسی برقراری امنیت	۲۵
میزان دستیابی به اهداف یادگیری	۲۶
خودآزمایی	۲۷
سه دوم: ضرورت امنیت اطلاعات در بانک	**۳۲**
اهداف یادگیری	۳۳
پیش آزمون	۳۴
لزوم تأمین امنیت اطلاعات در بانک‌ها	۳۶
لزوم نهادینه کردن امنیت اطلاعات در کارکنان	۳۸
میزان دستیابی به اهداف یادگیری	۴۳
خودآزمایی	۴۵
خلاصه فصل اول	
فصل دوم: امنیت فیزیکی و محیطی	**۵۰**
جلسه سوم: امنیت فیزیکی و محیطی و انواع آن	
اهداف یادگیری	۵۱
پیش آزمون	۵۲
امنیت فیزیکی و محیطی	۵۴
انواع راهکارهای امنیت فیزیکی و محیطی	۵۶
استفاده از حصارهای مناسب امنیت فیزیکی	۶۷
حفظ امنیت ورودي ساختمان‌ها و مراکز داده حساس	۷۲
استقرار و حفاظت از تجهیزات	۷۳
محافظت در برابر تهدیدات بیرونی و محیطی	۷۴
تهیه نسخ پشتیبان از اطلاعات و ایجاد سایت‌های پشتیبان	۷۵
رعایت امنیت در کابل کشی	۷۵

رعایت ملاحظات امنیتی در خروج دارایی‌ها ۷۵
حفظ امنیت تجهیزات خارج از سازمان ۷۶
رعایت امنیت تجهیزات بدون مراقبت کاربر ۷۷
آموزش کارکنان ۷۸
میزان دستیابی به اهداف یادگیری ۸۲
خودآزمایی

جلسه چهارم: محافظت در برابر تهدیدات فیزیکی و محیطی ۸۴
۲،۱. اهداف یادگیری ۸۶
۲،۲. پیش آزمون ۸۷
۲،۳. انواع تهدیدات فیزیکی و محیطی ۸۷
۲،۳،۱. بلایای طبیعی و حوادث غیر مترقبه ۸۸
۲،۳،۲. تهدیدات انسانی ۸۸
۲،۳،۳. مشکلات فنی ۹۱
۲،۴. برنامه ریزی برای پاسخگویی به حوادث غیرمترقبه ۹۳
۲،۴،۱. مرحله آماده‌سازی پیش از وقوع حادثه ۹۵
۲،۴،۲. مرحله وقوع حادثه ۹۶
۲،۴،۳. مرحله بازیابی پس از وقوع حادثه ۹۸
۲،۵. میزان دستیابی به اهداف یادگیری ۱۰۱
۲،۶. خودآزمایی ۱۰۲
۳. خلاصه فصل دوم ۱۰۴

فصل سوم: تهدیدات امنیتی در شبکه‌های رایانه‌ای ۱۰۵
جلسه پنجم: انواع حملات سایبری و تکنیک‌های هک ۱۰۶
اهداف جلسه آموزشی ۱۰۷
پیش‌آزمون ۱۰۸
شبکه‌های رایانه‌ای و فضای سایبری ۱۱۰
انواع حملات سایبری ۱۱۰
نمونه هایی از حملات سایبری ۱۱۲
مهندسی اجتماعی ۱۱۳
حملات فیشینگ ۱۱۳
اخذ اطلاعات از طریق کلیدنگار ۱۱۷
میزان دستیابی به اهداف آموزشی ۱۱۸
خودآزمایی

جلسه ششم: انواع بدافزارها ۱۲۳
اهداف جلسه آموزشی ۱۲۴
پیش‌آزمون ۱۲۶

انواع بدافزارها ۱۲۶
میزان دستیابی به اهداف آموزشی ۱۲۹
خودآزمایی ۱۳۱
خلاصه فصل سوم ۱۳۲

فصل چهارم: امن سازی در مقابله با تهدیدات امنیتی ۱۳۳
جلسه هفتم: ارتقای امنیت رایانه ها
اهداف یادگیری ۱۳۵
پیش آزمون ۱۳۶
۱۴۰
اهمیت بهروزرسانی رایانه ، نرم‌افزارها و سامانه ها ۱۴۱
سیستمعامل‌ها و برنامه‌های کاربردی ۱۴۲
اهمیت بهروزرسانی و ارتقای سیستمعامل‌ها و برنامه‌های کاربردی ۱۴۴
نرم‌افزار ضد بدافزار و بهروزرسانی آن ۱۴۸
تهیه نسخه پشتیبان ۱۴۹
میزان دستیابی به اهداف آموزشی ۱۴۹
خودآزمایی ۱۵۰

جلسه هشتم: ارتقای امنیت در استفاده از سامانه ها و اینترنت ۱۵۱
اهداف یادگیری ۱۵۴
پیش‌آزمون ۱۵۵
توجه به نکات امنیتی در استفاده از سامانه‌ها ۱۵۶
رمز عبور و مدیریت آن ۱۶۰
انتخاب رمز عبور مناسب **۱۶۱**
راهکارهای محافظت از رمز عبور **۱۶۲**
امنیت در هنگام استفاده از اینترنت ۱۶۳
ابزارهای اصالت سنجی ۱۶۴
پروتکل ارتباطی SSL ۱۶۶
میزان دستیابی به اهداف آموزشی ۱۶۸
خودآزمایی ۱۷۱

جلسه نهم: سیاست میز و صفحه نمایش پاک ۱۷۶
اهداف یادگیری ۱۸۱
پیش‌آزمون ۱۸۲
سیاست میز کار پاک و صفحه نمایش پاک **۱۸۶**
الزامات سیاست میز کار پاک و صفحه نمایش پاک ۱۸۷
میزان دستیابی به اهداف آموزشی ۱۸۸
خودآزمایی ۱۹۰
خلاصه فصل چهارم ۱۹۲

فصل پنجم: امنیت تجهیزات قابل حمل ۱۹۲

جلسه دهم: امنیت در رسانه‌های ذخیره‌سازی و رایانه های قابل حمل ۱۹۷

اهداف یادگیری ۱۹۸

پیش‌آزمون ۲۰۰

رسانه ذخیره‌سازی قابل حمل ۲۰۱

نکات امنیتی در بکارگیری رسانه‌های ذخیره‌سازی قابل حمل

اهمیت امنیت در رایانه های قابل حمل

نکات امنیتی در رایانه های قابل حمل

میزان دستیابی به اهداف آموزشی

خودآزمایی

جلسه یازدهم: امنیت در تلفن های هوشمند

اهداف یادگیری

پیش‌آزمون

اهمیت امنیت در تلفن‌های هوشمند

نکات امنیتی در استفاده از تلفن‌های هوشمند

میزان دستیابی به اهداف یادگیری

خودآزمایی

خلاصه فصل پنجم

فصل ششم: توصیه‌های امنیتی در خدمات بانکی

جلسه دهم: امنیت در کاربرد کارت های بانکی و خرید های اینترنتی

اهداف یادگیری

پیش آزمون

امنیت در کاربرد کارت‌های بانکی و خریدهای اینترنتی

ملاحظات امنیتی در کاربرد کارت‌های بانکی

ملاحظات امنیتی در استفاده از دستگاه‌های خودپرداز (ATM) و پایانه‌های فروش (POS)

ملاحظات امنیتی در درگاه های پرداخت اینترنتی و خرید اینترنتی

میزان دستیابی به اهداف یادگیری

خودآزمایی

جلسه یازدهم: امنیت بانکداری اینترنتی و همراه بانک

اهداف یادگیری

پیش آزمون

نکات امنیتی در استفاده از سامانه بانکداری اینترنتی

نکات امنیتی در استفاده از سامانه همراه بانک

نکات امنیتی در استفاده از تلفنبانک

میزان دستیابی به اهداف یادگیری

۲,۷. خودآزمایی ۱۲۶
خلاصه فصل ششم ۱۲۹

فصل هفتم: جرایم رایانه ای و تعهدنامه عدم افشاء اطلاعات ۱۳۱
جلسه دوازدهم: جرایم رایانه‌ای و قوانین آن در ایران ۱۳۲
اهداف یادگیری ۱۳۳
پیش آزمون ۱۳۵
تعریف جرایم رایانه‌ای ۱۳۶
تاریخچه وقوع جرایم رایانه ای در ایران ۱۴۰
قانون جرایم رایانه‌ای در ایران ۱۴۱
تعریف تخلفات الکترونیک حوزه فناوری اطلاعات بانک ملت ۱۴۲
میزان دستیابی به اهداف یادگیری ۱۴۴
خودآزمایی ۱۴۸

جلسه دوازدهم: تعهدنامه عدم افشای اطلاعات (NDA) ۱۴۹
اهداف یادگیری ۱۴۹
پیش آزمون ۱۵۰
تعهدنامه عدم افشای اطلاعات (NDA) ۱۵۱
تعهدات عمده طرفین قرارداد در تعهدنامه عدم افشای اطلاعات (NDA) ۱۵۴
میزان دستیابی به اهداف یادگیری ۱۵۵
خودآزمایی ۱۵۶
خلاصه فصل هفتم ۱۶۰

فصل هشتم: پیاده‌سازی امنیت در سازمان ها ۱۶۱
جلسه دوازدهم: سیستم مدیریت امنیت اطلاعات (ISMS) ۱۶۲
اهداف یادگیری ۱۶۳
پیش آزمون ۱۶۴
راهکار مناسب تأمین امنیت اطلاعات ۱۶۶
سیستم مدیریت امنیت اطلاعات (ISMS) ۱۶۸
پیاده‌سازی سیستم مدیریت امنیت اطلاعات(ISMS) در بانک ملت ۱۷۱
خطمشی سیستم مدیریت امنیت اطلاعات (ISMS) ۱۷۶
میزان دستیابی به اهداف یادگیری ۱۸۱
خودآزمایی ۱۸۲

جلسه سیزدهم: تشکیلات سازمانی امنیت و نقش نیروی انسانی در تأمین امنیت سازمان ۱۸۶
اهداف یادگیری ۱۸۷
پیش آزمون ۱۸۸
تشکیلات سازمانی امنیت اطلاعات ۱۹۰
۱۹۲

شرح وظایف کلی ساختار امنیت اطلاعات بانک ملت ۱۹۲
نقش نیروی انسانی در تأمین امنیت اطلاعات ۱۹۷
میزان دستیابی به اهداف یادگیری ۱۹۸
خودآزمایی ۲۰۰

جلسه چهاردهم: لزوم وجود سیاست‌های امنیتی و ضرورت انطباق با آن‌ها

اهداف یادگیری
پیش آزمون
سیاست‌های امنیتی و لزوم وجود آن‌ها
ضرورت انطباق با سیاست‌های امنیتی
میزان دستیابی به اهداف یادگیری
خودآزمایی
خلاصه فصل هشتم

مقدمه ناشر :

کتاب حاضر یکی از خروجی های پروژه "شناسایی درخت دانش صنعت بانکی" است که در چارچوب برنامه کلان " مرکز تأیید صلاحیت حرفه‌ای صنعت بانکی" در اداره کل آموزش بانک ملت تعریف شده است. هدف پروژه مذکور آن است که با درنظرگرفتن استانداردهای جهانی صنعت بانکی و نیز مقتضیات این صنعت در کشور ما، درخت دانش صنعت بانکی شناسایی شود و در گام بعدی محتوای آموزشی متناسب با شاخه‌های شناسایی‌شده، در فرآیندی علمی به رشته تحریر درآید.

ویژگی این مجموعه محتواهای درحال تدوین که با عنوان سری کتاب‌های "بانک برتر" به مخاطبین گرامی عرضه خواهد شد آن است که تمامی این مجموعه‌ها در قالبی مشابه نگارش می‌شوند که حاصل بررسی‌های کارشناسی مفصلِ یک تیم کارشناسی زبده است. در طراحی این قالب تلاش شده تا با بهره‌گیری از آخرین یافته‌های حوزه روانشناسی یادگیری، مطالب آموزشی به گونه‌ای نگاشته شود که آموزه‌های آن بدون نیاز به تدریس یا توضیح تکمیلی، قابل فراگیری باشد تا از این طریق امکان یادگیری به شکل خودخوان فراهم آید (توضیحات جامع در بخش راهنمای مطالعه آورده شده است).

همان‌گونه که اشاره شد پروژه "شناسایی درخت دانش صنعت بانکی" یکی از پروژه‌های برنامه کلان "مرکز تأیید صلاحیت حرفه‌ای صنعت بانکی"است. این مرکز، نخستین نهاد تخصصی سنجش و تأیید صلاحیت حرفه‌ای در صنعت بانکی کشور محسوب می‌شود و قادر است با بهره‌گیری از طیفی از ابزارهای متنوع، توانایی افراد را درمورد حوزه‌های دانشی/مهارتی شناسایی‌شده در صنعت بانکی مورد سنجش حرفه‌ای قرار دهد و اقدام به صدور گواهینامه حرفه‌ای مربوطه کند.

در پایان بر خود لازم میدانم از زحمات کلیه کسانی که به نحوی در آماده سازی این اثر همکاری داشته‌اند، به ویژه سرکار خانم نسرین جباری سپاسگزاری نمایم.

پیشگفتار مولفین :

مفهوم امنیت در دنیای واقعی، مفهومی حیاتی و شناخته شده برای بشر است. امنیت یعنی حفاظت از آنچه برای ما ارزشمند است. امنیت از ابتدا برای افراد و جوامع مورد توجه و یک نیاز بوده و در گذر زمان با پیشرفت تمدن و تغییرات ایجادشده در نحوه زندگی ، موضوع امنیت مفهوم گسترده تری پیدا کرده و در جنبه های مختلف زندگی با عناوینی نظیر حریم خصوصی ، امنیت اجتماعی ، امنیت مالی و .... مطرح شده است. در عصر حاضر نیز که فناوری اطلاعات با زندگی روزمره افراد گره خورده و تغییرات اساسی در نحوه کسب و کارهای بزرگ و کوچک ایجاد کرده است ، موضوع امنیت اطلاعات به عنوان بخش دیگری از مقوله امنیت در زندگی اضافه شده است.

موضوعاتی نظیر سرقت اطلاعات، سوء استفاده از اطلاعات و افشاء اطلاعات ، موضوعاتی هستند که تقریباً همه افراد را در زندگی روزمره و سازمان ها و شرکت های بزرگ را در فضای کسب و کار تهدید می کنند. پس محافظت از دارایی های اطلاعاتی و به عبارت بهتر امنیت اطلاعات ، بعنوان یک رکن اساسی در سبک زندگی امروزه و نوع کسب و کار سازمان ها مطرح است.

امنیت اطلاعات فرایندی مداوم و مستمر بوده و آگاهی اولین گام در اجرای این فرایند است. لذا در مستند پیش رو سعی بر آن شده تا در یک نگاه جامع و ساده ، مفاهیم ، اصول و اقداماتی را که توجه به آنها موجب محافظت افراد از بسیاری از مخاطرات و تهدیدات امنیتی می گردد، بیان شود. بکارگیری مطالب و نکات مطروحه در این کتاب برای محافظت از دارایی های اطلاعاتی در زندگی روزمره و شخصی توصیه می گردد. بدیهی است، توجه به نکات امنیتی عنوان شده و استفاده به صورت روزمره در ارتقاء فرهنگ امنیت اطلاعات در سازمان محل خدمت نیز تأثیر گذار خواهد بود. به یاد داشته باشیم ، ارتقاء سطح امنیت و محافظت از دارایی های اطلاعاتی سازمان با توجه و کمک همه کارکنان امکانپذیر خواهد بود. پس همگی در حیطه وظایف خود ، دارای مسئولیت هستیم. در واقع نقش هر یک از کارکنان در این فرایند به مثابه این مثال است :

سازمان ما مانند دوچرخه ای است که اگر رکاب نزنیم، زمین خواهد خورد. همه ما بر این دوچرخه سوار هستیم.

فروردین ۹۷

راهنمای مطالعه

همانطور که در مقدمه کتاب ذکر شد، کتاب حاضر از سری کتاب های آموزشی با عنوان «بانک برتر» بوده که بر مبنای «درخت دانش صنعت بانکی» تهیه و تدوین شده است. درخت دانش صنعت بانکی نیز خود یکی از پروژه های برنامه کلان «مرکز تایید صلاحیت حرفه ای بانکداری» می باشد.

مجموعه کتابهای آموزشی «بانک برتر» دارای ساختاری کاملاً منحصر به فرد می باشد که مبتنی بر تئوری های روانشناسی یادگیری در قالب کتاب های آموزشی «خودخوان» طراحی و تدوین گردیده است. «خودخوان» بودن کتابها به این معنی است که فراگیر بتواند با مطالعه کتاب بدون نیاز به شرکت در دوره های آموزشی حضوری و یا مجازی و بدون نیاز به مدرس، مطالب را فراگرفته و به تسلط نسبی، به گونه ای که به سطح آمادگی لازم جهت کسب موفقیت در آزمون حرفه ای مربوطه دست یابد.

هر کتاب آموزشی شامل تعدادی فصل می‌باشد که به منظور تسهیل امر خواندن و یادگیری مباحث، هر فصل بر اساس حجم مطالب، به یک یا چند جلسه درس تقسیم شده است. هر جلسه از نظر حجم مطلب تقریباً معادل نود دقیقه مطالعه است. هر جلسه شامل اهداف یادگیری، پیش آزمون، متن درس (شامل نکته، مثال، یادآوری، نوار یادداشت)، میزان دستیابی به اهداف یادگیری و خودآزمایی می باشد. به علاوه در انتهای کتاب تعدادی مطالعه موردی و یک آزمون جامع آورده شده است.

در ذیل بخش های اصلی کتاب به صورت مختصر توصیف می شود:

اهداف یادگیری

در ابتدای هر جلسه آموزشی، اهداف یادگیری در نظر گرفته شده است. اهداف یادگیری بیانگر آن است که فراگیر پس از مطالعه متن،می بایست چه دانش و یا مهارتی را کسب نماید. بنابراین از فراگیر انتظار می رود تا قبل از شروع مطالعه متن، اهداف یادگیری را ملاحظه نماید تا مطالب جلسه مزبور را به صورت هدفمند مطالعه و پیگیری نماید.

میزان دستیابی به اهداف یادگیری

اهداف یادگیری بیان شده در ابتدای هر جلسه، مجدداً در انتهای جلسه ذکر می‌شود. فراگیر پس از مطالعه مباحث آموزشی، اهداف یادگیری را مجدداً مرور نموده و با درج علامت تایید (✓) دستیابی

خـود بـه نتایـج مـورد انتظـار را ثبـت می‌نمایـد. تـا چنانچـه یادگیـری کامـل مبحثـی محقـق نشـده اسـت، مشـخص گـردد و فراگیـر بـه مـرور دوبـاره آن قسـمت بپـردازد.

پیش آزمون

در ابتـدای هـر جلسـه درسـی، پیش‌آزمـون درنظـر گرفتـه شـده اسـت کـه هـدف از طراحـی آن، آگاهـی فراگیـر از سـطح دانـش خـود و ایجـاد آمادگـی ذهنـی جهـت شروع مطالعـه بـه صـورت چالـش پرسـش و پاسـخ، قبـل از مطالعـه جلسـه مزبـور می‌باشـد.

خودآزمایی

فراگیـر پـس از مطالعـه کامـل مـتن، در بخـش خودآزمایـی بـه سـوالاتی کـه از جلسـه مـورد نظـر طراحـی و اسـتخراج گردیـده پاسـخ می دهـد. هـدف اصلـی از انجـام خودآزمایـی، بررسـی میـزان یادگیـری حاصـل شـده از مطالعـه جلسـه مـی باشـد. هـدف دیگـر مقایسـه نتیجـه خودآزمایـی بـا نتیجـه پیـش آزمـون بـه منظـور بررسـی میـزان یادگیـری حاصـل شـده اسـت.

نکته

در هـر کجـا از مـتن درس،اگـر مطلبـی نیـاز بـه تاکیـد و توجـه بیشـتر داشـته باشـد در قالـب نکتـه در مـتن درس مشـخص گردیـده اسـت.

مثال

در متن درس جهت تفهیم بیشتر مطلب از مثال استفاده شده است.

مطالعه موردی

در بخـش مطالعـه مـوردی، یـک مثـال کلـی آورده شـده اسـت تـا بـه صـورت عینـی کاربـرد مطالـب ارائـه شـده در کتـاب، در قالـب یـک مـورد عملـی مـورد بررسـی و دقـت نظـر قـرار گیـرد. مطالعـه مـوردی کمـک خواهـد کـرد تـا بـا مراجعـه مجـدد بـه مطالـب کتـاب سـعی شـود از مطالـب آموختـه شـده جهـت تجزیـه و تحلیـل مـورد عملـی ذکـر شـده بهـره گرفتـه شـود.

نوار یادداشت

در تمامـی صفحـات کتـاب، فضایـی بـه عنـوان نـوار یادداشـت در نظـر گرفتـه شـده اسـت. از فراگیـر انتظـار مـی رود تـا بـه منظـور مطالعـه اثربخـش تـر در حیـن مطالعـه مـتن درس، چکیـده مطلـب و مـوارد مهـم در هـر صفحـه را در فضـای مذکـور یادداشـت نمایـد. ایـن امـر بـه یادگیـری هـر چـه بهـتر مطالـب و مـرور آنهـا کمـک مـی نمایـد.

فصل اول

آشنایی با مفاهیم امنیت اطلاعات

جلسه اول:
مفهوم امنیت اطلاعات و ارتباطات و دارایی های اطلاعاتی

جلسه دوم:
ضرورت امنیت اطلاعات در بانک

فصل دوم:
امنیت فیزیکی و محیطی

فصل سوم:
تهدیدات امنیتی در شبکه های رایانه ای

فصل چهارم:
امنیت در مقابله با تهدیدات فضای سایبری

فصل پنجم:
امنیت تجهیزات قابل حمل

فصل ششم:
توصیه های امنیتی در خدمات بانکی

فصل هفتم:
جرایم رایانه ای و تعهدنامه عدم افشای اطلاعات

فصل هشتم:
پیاده سازی امنیت در سازمان ها

جلسه اول

مفهوم امنیت اطلاعات و دارایی های اطلاعاتی

۱۵	اهداف یادگیری
۱۶	پیش آزمون
۱۸	لزوم برقراری امنیت
۱۸	اطلاعات و انواع آن
۲۰	امنیت اطلاعات
۲۱	عناصر امنیت اطلاعات
۲۵	گام های اساسی برقراری امنیت
۲۶	میزان دستیابی به اهداف یادگیری
۲۷	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. مفهوم دارایی اطلاعاتی و انواع آن را شرح دهد.
۲. مفهوم امنیت اطلاعات را دریابد و عناصر مثلث امنیت اطلاعات را نام ببرد.
۳. گام‌های اساسی برقراری امنیت را توضیح بدهد.

پیش‌آزمون جلسه اول :

۱. امنیت اطلاعات به چه منظور مورد نیاز است؟
الف) حصول اطمینان از تداوم کسب و کار سازمان
ب) حفظ دارایی‌های اطلاعاتی سازمان
ج) کاهش خسارت و افزایش بهره‌وری سازمان
د) همه موارد

۲. حصول اطمینان از اینکه اطلاعات تنها در اختیار افراد مجاز قرار می گیرند، به چه موردی اشاره دارد؟
الف) اطلاعات مجاز ب) حقوق دسترسی کارکنان ج) محرمانگی د) دسترس‌پذیری

۳. کدامیک از موارد زیر، از گام‌های اساسی در برقراری امنیت می‌باشد؟
الف) پیشگیری ب) نگهداری ج) واکنش د) همه موارد

۴. تهیه نسخه پشتیبان از اطلاعات، کدامیک از عناصر امنیت اطلاعات را برآورده می‌سازد؟
الف) محرمانگی ب) دسترس‌پذیری ج) یکپارچگی د) هیچ کدام

پاسخ‌نامه

پیش‌آزمون جلسه اول

:

	الف	ب	ج	د
۱				
۲				
۳				
۴				

لزوم برقراری امنیت

:

امروزه با رشد سریع تکنولوژی و کاربرد گسترده اینترنت، کاربران بسیاری برای انجام امور مختلفی نظیر ارتباطات، سفر، سرگرمی، خرید، تجارت و غیره، از رایانه، تلفن‌های هوشمند، تبلت، لپ تاپ و سایر تجهیزات در خانه‌ها و سازمان‌ها استفاده می‌کنند. با ظهور بسیاری از خرابکاری‌ها و حملات اینترنتی، همه این کاربران در معرض خطرات امنیتی قرار دارند و این امر اهمیت دادن به ایمن سازی این ابزارها، تجهیزات و اطلاعات موجود در آن‌ها را بیش از پیش برجسته می‌سازد.

صدماتی که یک کاربر یا سازمان ممکن است به خاطر نقص‌های امنیتی متحمل شود، شامل مواردی از قبیل موضوعات زیر است:

• زیان مالی

اگر سیستم‌های یک سازمان به دلیل حملات امنیتی متوقف شوند، ممکن است آن سازمان مقادیر زیادی پول از دست دهد. ممکن است این حملات باعث از بین رفتن اسرار تجاری دارای ارزش مالی بالای در سازمان شود. اگر حساب‌های بانکی یا اطلاعات کارت‌های اعتباری افشا شود و در معرض خطر قرار بگیرد، حتی کاربران خانگی هم دچار زیان مالی خواهند شد.

• از بین رفتن اعتبار و شهرت

نقص امنیتی می‌تواند به از دست دادن اعتماد مشتری یک سازمان منتهی شود. به طور مثال فرض کنید حساب‌های مشتریان یک بانک توسط چند هکر خالی شود، آیا شما حاضرید پول خود را در آن بانک نگهداری کنید؟

• از دست دادن اطلاعات

ممکن است اطلاعات مهم و حساسی روی سیستم سازمان یا خانه شما وجود داشته باشد، عدم رعایت نکات امنیتی می‌تواند باعث پاک شدن و یا سرقت این اطلاعات شود.

اطلاعات و انواع آن

:

هر چیزی که برای فرد یا سازمان دارای ارزش باشد، دارایی نامیده می‌شود. اطلاعات یکی از با ارزش‌ترین و حساس‌ترین دارایی‌های افراد و سازمان است و نیازمند حفاظت مناسب می‌باشد. به عبارت ساده تر، دستیابی به اطلاعات مورد نیاز و عرضه به موقع و مناسب آن، همواره نقشی کلیدی و سرنوشت ساز دارد. برخی از دارایی های اطلاعاتی عبارت اند از:

• بانک‌های اطلاعاتی (مانند شماره حساب و اطلاعات بانکی، اطلاعات کارت اعتباری، اطلاعات شخصی، اطلاعات سازمانی)

• نرم‌افزار (مانند سیستم عامل، برنامه‌های کاربردی، سامانه های بانکی، سامانه های پرسنلی)

• سخت‌افزار (مانند رایانه، تجهیزات ارتباطی، هارد، فلش مموری)

• خدمات (پردازشی، ارتباطی و پشتیبانی)

• دانش پرسنل

• مستندات اعم از کاغذی و الکترونیک

• هر آنچه مرتبط با اطلاعات و هویت سازمان باشد (مانند برند سازمان)

اطلاعات را می‌توان به شکل‌های مختلف نگهداری کرد. می‌توان آن را روی کاغذ نوشت، چاپ کرد، به‌صورت الکترونیک ذخیره کرد، به‌وسیله روش‌های مرسوم یا الکترونیک آن را ارسال کرد، به‌وسیله فیلم به نمایش درآورد و یا آن را در قالب نوارهای صوتی یا گفتاری ارایه نمود.

بدون در نظر گرفتن چگونگی دریافت اطلاعات و روش به اشتراک گذاشتن و ذخیره آن، همیشه باید از اطلاعات به نحو مناسب و قابل قبولی محافظت کرد.

امنیت اطلاعات

:

امنیت به معنای حفاظت از دارایی‌ها در برابر حملات و رویدادهای عمدي و غیرعمدی می‌باشد. همان طور که آرامش در زندگي روزمره بدون امنیت امکان‌پذیر نیست، بدون اطمینان از امن بودن سیستم‌ها و دارایی‌های اطلاعاتي، اعتماد به آن‌ها محال خواهد بود. همچنین، حفظ و نگهداری اطلاعات شرط لازم برای تداوم فرایند کسب و کار سازمان‌ها به ویژه مؤسسات مالی و بانکی است. پس، پرداختن به امنیت اطلاعات به معنی توجه به حفظ دارایی‌های اطلاعاتی سازمان است.

امنیت اطلاعات فرایندی است که براساس آن از اطلاعات و دارایی‌های اطلاعاتی در برابر حملات و تهدیدات مختلف محافظت می‌شود.

عناصر امنیت اطلاعات

:

امنیت اطلاعات از طریق به‌کارگیری مجموعه‌ای از فرایندهای کنترلی به دست می‌آید، این فرایندها دسترسی به عناصر امنیت اطلاعات را امکان‌پذیر می‌سازد. این عناصر عبارت اند از:

محرمانگی (C) : ویژگی محافظت از دسترسی به اطلاعات توسط افراد، موجودیت‌ها یا فرایندهای غیرمجاز.

به عبارت دیگر، اطلاعات نباید فاش شود و فقط باید در دسترس افراد مُجاز قرار گیرد که این امر معمولاً با محدود کردن دسترسی و یا با رمزنگاری اطلاعات قابل اجراست.

پس، محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز. به عنوان مثال چنانچه فردی به هر نحوی به اطلاعات کارت اعتباری شما دست یابد، نقض محرمانگی رخ داده است. نقض محرمانگی می‌تواند موارد مختلفی داشته باشد: خواندن اطلاعات محرمانه نمایشگر رایانه شما از روی دست‌تان، یا به سرقت رفتن لپ‌تاپ حاوی اطلاعات و تصاویر خانوادگی شما و یا ارائه اطلاعات محرمانه از طریق تلفن و افشای اطلاعات کارت بانکی شما که همه از موارد نقض محرمانگی است.

هرگونه نقض محرمانگی می‌تواند منجر به ضرر مالی شود. سازمان‌های زیادی وجود دارند که به دلیل افشای اطلاعاتشان نزد سازمان‌های رقیب ورشکسته شده‌اند. همچنین، فاش شدن اطلاعات و تصاویر شخصی و خانوادگی نیز می‌تواند زندگی افراد را دچار بحران سازد. بنابراین، حفظ محرمانگی اطلاعات شخصی و سازمانی یکی از عناصر کلیدی برقراری امنیت اطلاعات تلقی می شود.

اطلاعات فقط باید در دسترس افراد مجاز باشد.

یکپارچگی (I) : ویژگی حفظ صحت و تمامیت دارایی‌ها.

یکپارچگی به معنی اطمینان از این است که اطلاعات، دقیق، کامل، قابل اعتماد و به شکل اصلی‌شان باشد. هرگونه تخریب یا تغییر اطلاعات می‌تواند ارزش اطلاعات را کاهش دهد یا از بین ببرد. چنانچه هنگام ارسال یک ایمیل محرمانه متن ایمیل دستخوش تغییر شود و به آن عبارتی اضافه یا از آن کم شود، نقض یکپارچگی ایمیل رخ داده است. به عبارت دیگر، یکپارچگی یعنی حصول اطمینان از اینکه اطلاعات درحین انتقال بین مبدأ (فرستنده) و مقصد (گیرنده)، دستکاری و مخدوش نمی‌شود و اطلاعاتی که از مبدأ فرستاده شده است، عیناً به مقصد می‌رسد. در ادامه، مثالی عامیانه و قدیمی در خصوص نقض یکپارچگی، آورده شده است.

نقل است یکی از بزرگان تبریز مورد خشم رضا شاه واقع شده بود. رضا شاه دستور اعدامش را صادر کرد. اطرافیان آن شخص نزد رضا شاه رفتند و با التماس وخواهش او را قانع کردند تا از اعدام این فرد صرفنظر کند. با اصرار زیاد آن ها، رضا شاه دستور داد تلگرافی به تبریز ارسال کنند که «بخشش، لازم نیست اعدامش کنید» تلگرافچی در هنگام ارسال نامه، ویرگول بعد از بخشش را نادیده گرفته و تلگراف را چنین نوشت:

«بخشش لازم نیست، اعدامش کنید» و به این طریق حکم رضا شاه نادیده گرفته شد و آن بیچاره اعدام گردید.

بنابراین، یک تغییر کوچک در اطلاعات به صورت سهوی یا عمدی می‌تواند صحت آن اطلاعات را از بین ببرد و یکپارچگی آن را دستخوش تغییر نماید.

اطلاعات باید سالم و بدون دستکاری باشد.

دسترس‌پذیری (A) : ویژگی در دسترس و قابل استفاده بودن، به محض تقاضای یک فرد مجاز.

در واقع دسترس‌پذیری یعنی حصول اطمینان از اینکه اطلاعات در زمان نیاز، بدون تاخیر در دسترس افراد مجاز قرار گیرد. بنابراین، باید شرایطی مهیا کرد که در همه حال حتی به علت قطع برق، خرابی سخت‌افزار، از بین رفتن ناگهانی اطلاعات و سایر حوادث، اطلاعات و دارایی‌های اطلاعاتی در دسترس باقی بمانند و یا در کوتاه ترین زمان ممکن قابل دسترس شوند. به عنوان مثال، داشتن سیستم‌ها و تجهیزات جایگزین در زمان خرابی‌ها، تهیه نسخه پشتیبان از اطلاعات، داشتن UPS و ژنراتور در زمان قطعی برق می‌تواند از راهکارهای افزایش دسترس‌پذیری باشند.

اطلاعات در زمان مورد نیاز، برای افراد مجاز، باید در دسترس باشد.

شکل ۱: مثلث امنیت یا CIA

بنابراین، تامین امنیت اطلاعات عبارت است از: فراهم کردن امکانی که اطلاعات درست در زمان مناسب، در دسترس افراد مُجاز قرار گیرد و سه پارامتر محرمانگی، یکپارچگی و دسترس‌پذیری آن حفظ شود.

به‌عنوان پرسنل یک سازمان و همچنین در زندگی شخصی، باید به اصول حفاظت از اطلاعات توجه کنیم تا همواره بتوانیم امنیت پایه را برقرار کنیم. یکی از مهم‌ترین اصول حفاظت از اطلاعات، شناسایی و طبقه‌بندی آن‌هاست. بسیاری از سازمان‌ها و افراد قصد دارند از همه اطلاعات خود در یک سطح محافظت کنند و در این راه با شکست مواجه می‌شوند، زیرا نمی‌دانند چه اطلاعاتی برای کسب و کار یا زندگی آن‌ها حیاتی است و از بین رفتن یا افشای آن اطلاعات چه تأثیراتی بر کسب وکار یا زندگی آنها دارد.

در واقع باید اطلاعات، براساس سطح محرمانه بودن آنها، طبقه‌بندی و وزن‌دهی شوند و با توجه به درجه اهمیت شان در کسب‌وکار نسبت به حفظ محرمانگی، یکپارچگی و دسترس‌پذیری آنها سیاست‌گذاری و مدیریت شوند.

در تأمین امنیت اطلاعات رعایت تعادل، امری ضروری است. امنیت نباید آنقدر بالا باشد که دسترسی افراد را دچار مشکل کند و هیچ‌کس نتواند از اطلاعات و دارایی‌های اطلاعاتی استفاده کند و نه آنقدر پایین باشد تا همه بتوانند به راحتی از آن‌ها سوء استفاده کنند. بلکه باید براساس سطح محرمانگی و میزان اهمیت و حیاتی بودن اطلاعات، از آنها حفاظت شود.

گام‌های اساسی برقراری امنیت :

برای امن‌سازی دارایی‌های شخصی و سازمانی، رعایت سه گام زیر مهم است:

۱. احتیاط و پیشگیری
۲. نگهداری
۳. واکنش

احتیاط و پیشگیری:

احتیـاط و پیشـگیری عملـی از پیـش تعییـن شـده بـرای حفاظـت از دارایی‌هـای شـخصی یـا سـازمانی در مقابـل تهدیـدات و خطـرات احتمالـی اسـت. در صورتـی کـه فـرد یـا سـازمانی پیـش از بـروز خطـا، آن را شناسـایی و پیش‌بینـی نمایـد و تدابیـر لازم بـرای جلوگیـری از بـروز آن بیندیشـد و علـل رخ دادن خطـا را شناسـایی و حـذف کنـد، اقـدام پیشـگیرانه انجـام داده اسـت. هزینـه پیشـگیري از يـك حادثـه امنیتـي همیشـه کمـتر از بازيـابي و کنـترل آن اسـت.

البتـه توجـه بـه ایـن نکتـه هـم ضروری اسـت کـه اقدامـات پیشـگیرانه بایـد متناسـب بـا ارزش دارایـی انجـام شـود و بـرای یـک دارایـی بـا ارزش کـم نبایـد اقدامـات پیشـگیرانه پـر هزینـه‌ای انجـام داد. برخـی از اقدامـات پیشـگیرانه بـرای حفاظـت از دارایی‌هـای اطلاعاتـی سـازمان شـامل مـوارد زیـر اسـت:

- استفاده از کلمات عبور پیچیده برای حساب‌های کاربری و تغییر آن در بازه‌های زمانی مشخص
- نصب نرم افزار ضد ویروس بر روی رایانه‌ها و تلفن‌های هوشمند و به‌روزرسانی مستمر آن
- آگاهی‌رسانی مستمر در قبال حملات سایبری به کارمندان سازمان و افراد خانواده
- تهیه نسخه پشتیبان از دارایی‌های اطلاعاتی مهم
- تهیه چک‌لیست‌های امنیتی و انجام بازدیدهای دوره‌ای

نگهداری:

نگهـداری شـامل فعالیت‌هـای مکمـل اقدامـات پیشـگیرانه اسـت. اقدامـات پیشـگیرانه بـه تنهایـی کافـی نیسـتند و لازم اسـت افـراد و سـازمان به‌طـور پیوسـته از برنامه‌هـای نگهـداری بـرای محافظـت از دارایی‌هـا و سیسـتم‌های خـود اسـتفاده کننـد. برخـی از ایـن اقدامـات بـه شرح زیـر اسـت:

- به‌روزرسانی مستمر برنامه‌ها و نرم‌افزارها نظیر ضدویروس
- انجام برنامه‌های نگهداری و تعمیرات دوره‌ای
- بازنگری دوره ای سیاست‌های امنیتی

واکنش:

حتـی اگـر اقدامـات پیشـگیرانه و نگهـداری انجـام شـود، بـاز هـم امـکان وقـوع حـوادث امنیتـی وجـود خواهـد داشـت. در ایـن زمـان، لازم اسـت تیمـی در سـازمان وجـود داشـته باشـد کـه بتوانـد بـرای کاهـش و رفـع خرابی‌هـای ناشـی از وقـوع حادثـه امنیتـی، سریعـاً وارد عمـل شـود.

طبـق نظـر آقـای اسـپافورد، مدیـر بخـش عملیـات کامپیوتـری و تکنولـوژی امنیـت دانشـگاه پُـردو امریـکا: تنهـا سیسـتمی کـه به معنـای واقعـی، امـن محسـوب می‌شـود، سیسـتمی اسـت کـه خامـوش بـوده، از اتصـال بـرق کشـیده شـده باشـد، داخـل یـک گاو صنـدوق تیتانیومـی قـرار داده شـده، در یـک تانکـر بتنـی دفـن شـده باشـد و پیرامـون آن را بـا گاز کشـنده اعصاب و محافظین زبده محصورکرده باشند.

حتی با این شرایط حاضر نیستم روی امنیت این سیستم شرط‌بندی کنم!

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید،
در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- مفهوم دارایی اطلاعاتی و انواع آن را شرح دهید.	
۲- مفهوم امنیت اطلاعات را تشریح و عناصر مثلث امنیت اطلاعات را نام ببرید.	
۳- گام‌های اساسی برقراری امنیت را توضیح بدهید.	

خودآزمایی جلسه اول :

۱. هدف از تأمین امنیت اطلاعات در سازمان چیست؟
الف) حفظ محرمانگی، کارایی و یکپارچگی اطلاعات
ب) حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات
ج) حفظ کارایی، یکپارچگی و دسترس‌پذیری اطلاعات
د) حفظ محرمانگی، کارایی و دسترس‌پذیری اطلاعات

۲. کدامیک از گزینه های زیر بیانگر مفهوم دسترس‌پذیری می باشد؟
الف) تهیه نسخه پشتیبان
ب) استفاده از رمز عبور
ج) ارسال نامه با سربرگ شرکت
د) هیچ کدام

۳. ارسال یک ایمیل محرمانه بدون آنکه متن آن تغییری کند، یعنی حفظ:
الف) محرمانگی
ب) یکپارچگی
ج)دسترس‌پذیری
د) هیچ کدام

۴. در صورتی که فرد یا سازمان پیش از بروز خطا، آن را شناسایی کند و تدابیر لازم را برای جلوگیری از بروز آن بیندیشد و علل رخ دادن خطا را شناسایی و حذف کند، کدامیک از اقدامات زیر است؟
الف) اقدام نگهدارنده
ب) اقدام واکنشی
ج) اقدام پیشگیرانه
د) اقدام اصلاحی

پاسخ‌نامه تشریحی

خودآزمایی جلسه اول

:

۱.پاسخ صحیح، گزینه «ب»

تأمین امنیت اطلاعات عبارت است از فراهم کردن امکانی که اطلاعات درست در زمان مناسب، در دسترس افراد مُجاز قرار گیرد و سه پارامتر محرمانگی، یکپارچگی و دسترس‌پذیری آن حفظ شود.

۲.پاسخ صحیح، گزینه «الف»

دسترس‌پذیری یعنی حصول اطمینان از اینکه تا زمانی که اطلاعات، مورد نیاز افراد مُجاز است بدون تأخیر در دسترس آن‌ها باشد. بنابراین، تهیه نسخه پشتیبان از اطلاعات، می‌تواند یکی از راهکارهای حفظ دسترس‌پذیری باشد.

۳.پاسخ صحیح، گزینه «ب»

یکپارچگی به معنی اطمینان از این است که اطلاعات، دقیق، کامل، قابل اعتماد و به شکل اصلی‌شان باشد. چنانچه هنگام ارسال یک ایمیل محرمانه متن ایمیل دستخوش تغییر شود، به آن عبارتی اضافه و یا از آن کم شود، نقض یکپارچگی ایمیل رخ داده است.

۴.پاسخ صحیح، گزینه «ج»

در صورتی که فرد یا سازمانی پیش از بروز خطا، آن را شناسایی و پیش‌بینی کند و تدابیر لازم را برای جلوگیری از بروز آن بیندیشد و علل رخ دادن خطا را شناسایی و حذف کند، اقدام پیشگیرانه انجام داده است.

جلسه دوم

ضرورت امنیت اطلاعات در بانک

۳۳	اهداف یادگیری
۳۴	پیش‌آزمون
۳۶	لزوم تأمین امنیت اطلاعات در بانک‌ها
۳۸	لزوم نهادینه کردن امنیت اطلاعات در کارکنان
۴۳	میزان دستیابی به اهداف یادگیری
۴۵	خودآزمایی
۴۶	خلاصه فصل اول

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. ضرورت تأمین امنیت اطلاعات در بانک را درک کند.
۲. لزوم نهادینه کردن فرهنگ امنیت اطلاعات در کارکنان بانک را درک کند.

پیش‌آزمون جلسه دوم :

۱. به نظر شما کدامیک از موارد زیر در انتخاب یک بانک یا موسسه مالی حائز اهمیت می باشد؟

الف) حسن شهرت

ب) تنوع در ارائه خدمات

ج) حفظ امنیت اطلاعات مشتری

د) همه موارد

۲. به نظر شما کدامیک از موارد زیر می‌تواند امنیت اطلاعات سازمان را به خطر بیندازد؟

الف) عدم وجود پرسنل آگاه

ب) فقدان مشتریان وفادار

ج) فقدان فرایند آموزش و فرهنگ سازی امنیتی

د) گزینه الف و ج

پاسخ‌نامه

پیش‌آزمون جلسه دوم

:

	الف	ب	ج	د
۱				
۲				

لزوم تأمین امنیت اطلاعات در بانک‌ها

:

با گسترش فناوري اطلاعات، امنیت به یکي از مهم‌ترین مباحث در فرایند طراحي و مدیریت سازمان‌ها تبدیل شده است. در دنیایی که فناوری سطح بالا و ارتباطات گسترده از مشخصه‌های اصلی آن است، هر سازمانی نیاز به برقراری امنیت اطلاعات دارد. در هر لحظه، خطرات مختلفی از بیرون و درون سازمان توسط هکرها، رقبا، پرسنل و یا افراد سودجو، منافع و دارایی‌های سازمان را تهدید می‌کند. به‌ویژه در بانک‌ها و موسسات مالی یکي از اصلي‌ترین مسایل مطرح، تأمین امنیت لازم براي انواع سیستم‌ها و سرویس‌هاي بانکي است. با گسترش روزافزون تبادلات حساس بانک از طریق شبکه‌های رایانه‌ای و سرویس‌های الکترونیک و سامانه‌های بانکی، برقراری امنیت اطلاعاتی که بر روی این بسترها در حال پردازش و جابه‌جایی هستند، امری بسیار ضروری است.

امروزه در سطح جهان، وجود خدمات بسیار متنوع و پیشرفته در حوزه بانکداری باعث شده‌اند، مشتریان یکی از ملاک‌های اصلی در ارزیابی و انتخاب بانک مورد علاقه خود را، تنوع و کیفیت این‌گونه خدمات قرار دهند. و از سوی دیگر ملاک دیگر در انتخاب یک بانک، حسن شهرت آن بانک است و مشتری هیچ‌گاه به سراغ بانکی که از لحاظ امنیتی، شهرت خوبی ندارد، نخواهد رفت. اطلاعات، یکی از مهم ترین سرمایه‌های بانک‌ها و موسسات مالی است و حفاظت از اطلاعات برای ایجاد و حفظ اعتماد بین بانک و مشتریان آن ضروری می‌باشد. طبق پژوهشی که در سال‌های اخیر انجام شده است، در صدر دلایلی که بانکها مشتاق به سرمایه گذاری در امر امنیت هستند، کسب اعتماد مشتریان است. بحث اعتماد شاید در هیچ صنعت دیگری این‌قدر اهمیت نداشته باشد. ممکن است هک یک کارت بانکی، ضرر مالی چندانی به بار نیاورد، اما جنبه اعتماد عمومی آن ارزش بسیار بالایی دارد.

در عین حال، تمرکز مهاجمان نیز بر روش های جدید کلاهبرداری از طریق زیرساخت‌های الکترونیک شکل گرفته است. روند رو به رشد حملات سازمان‌یافته به بنگاه‌های مالی و ظهور تهدیدات امنیتی نشان می‌دهد، مسئله پایش و نظارت دایمی و مراقبت از امنیت اطلاعات مشتریان، یکی از دغدغه‌های اساسی بانک‌ها بوده و یک ضرورت اجتناب‌ناپذیر است.

یکی دیگر از دلایل اهمیت امنیت اطلاعات این است که باعث افزایش دسترس‌پذیری و تداوم کسب‌وکار سازمان‌ها می‌شود. زمانی‌که یک حادثه امنیتی رخ دهد، ممکن است باعث از بین رفتن منابع یا سرویس‌های جاری سازمان شود و همین امر منجر به از کار افتادن و یا به تعویق افتادن روند کاری سازمان گردد. از کار افتادن یا ایجاد وقفه در فرایندها و سرویس‌های حیاتی و اصلی سازمان، یعنی هدر رفتن منابع، زمان و البته تحمیل هزینه‌های زیاد. همانطور که در بخش قبلی اشاره شد، هزینه پیشگیري از یك حادثه امنیتي همیشه کم‌تر از بازیابي و کنترل آن است. بنابراین، حفظ امنیت اطلاعات و انجام اقدامات امنیتی پیشگیرانه، باعث صرفه‌جویی در زمان و منابع مالی سازمان می‌شود. اگر بر اثر وقوع یک حادثه امنیتی، شبکه یک بانک دچار اختلال شود و برای مدتی سامانه‌ها و سرویس‌های آن بانک از کار بیفتند و از دسترس خارج شوند، قطعاً ضررهای زیادی، هم از نظر مالی و هم از نظر اعتباری به بانک وارد می‌شود، اگر اقدامات امنیتی در جهت افزایش سطح دسترس‌پذیری از قبل برای این بانک اجرا شده باشد، هدر رفتن منابع، حذف و یا کاهش خواهد یافت.

لزوم نهادینه کردن امنیت اطلاعات در کارکنان

:

همان‌طور که در ابتدای این بخش گفته شد، با گسترش خدمات بانکداری الکترونیک و افزایش روزافزون تعداد تراکنش‌های مالی در این بستر، بُروز تهدیدات امنیتی نیز به شکل قابل توجهی، رشد یافته است و هکرها و مهاجمان، سالانه مبالغ بسیار بالایی از راه نفوذ به سامانه‌های بانکی و استفاده از انواع روش‌های غیرمجاز، به بانک‌ها و موسسات مالی ضرر می‌رسانند. لذا بکارگیری راهکارهای امنیتی جهت تأمین و استقرار امنیت اطلاعات در این سازمان‌ها امری ضروری می‌باشد. البته توجه به این نکته نیز بسیار حائز اهمیت است که نباید مقوله امنیت اطلاعات در سازمان‌ها در سطح فن آوری محدود شود و صرفاً با خرید تجهیزات امنیتی بیشتر، این تصور ایجاد شود که به امنیت بیشتری دست خواهیم یافت. تا زمانی که برداشت ما از مفهوم استقرار امنیت در یک سازمان، صرفاً توجه

بـه مسـائل فنـی امنیـت در سـامانه‌ها باشـد، می‌تـوان گفـت متأسـفانه، چنـدان موثـر عمـل نکرده‌ایـم.
نیـروی انسـانی و کارکنـان سـازمان، بـه مراتـب نقـش کلیدی‌تـری در ارتقـای سـطح امنیـت دارنـد. صرف‌نظـر از موفقیـت و یـا عـدم موفقیـت مهاجـمان و بـا وجـود بکارگیـری راهکارهـای امنیتـی مختلـف در یـک سـازمان، بـه ویـژه در یـک بانـک یـا موسسـه مالـی، نبـود دانـش و آگاهـی کافـی کارکنـان در حـوزه امنیـت، همـواره به‌عنـوان مهم‌تریـن تهدیـد امنیتـی، مطـرح شـده و نبـود پایبنـدی و رعایـت اصـول و الزامـات امنیتـی از سـوی نیـروی انسـانی، می‌توانـد زمینـه سـاز ایجـاد بسـترهایی جهـت اسـتفاده مهاجـمان و باعـث بُـروز مشـکلات امنیتـی در سـازمان گـردد.
افـراد بـه صورت‌هـای مختلفـی در بُـروز مشـکلات امنیتـی تأثیـر دارنـد. بعضـی از کارکنـان، بـه دلیـل نداشـتن دانـش و آگاهـی کافـی نسـبت بـه نـکات امنیتـی و مطلـع نبـودن از نتایـج کارهایـی کـه انجـام می‌دهنـد، سـهواً بـه وقـوع رخدادهـای امنیتـی کمـک می‌کننـد. حتـی گاهـی اشـتباه سـهوی آن‌هـا، می‌توانـد زمینـه موفقیـت نفوذگـران (مهاجـمان، هکرهـا و سـایر سـوء اسـتفاده کننـدگان) را فراهـم نمایـد. طبـق آمارهـای بـه دسـت آمـده در دنیـا، خطاهـای کارکنـان و منابـع انسـانی، بیشـترین میـزان خسـارت بـه سیسـتم‌های اطلاعاتـی سـازمان را بـه خـود اختصـاص داده اسـت. بنابرایـن، اگـر درصـد بُـروز اشـتباهات و نقض‌هـای امنیتـی از سـوی کاربـران کاهـش یابـد، بـه هـمان نسـبت نیـز شـانس موفقیـت مهاجـمان کاهـش خواهـد یافـت.
همچنیـن، یکـی دیگـر از مهم‌تریـن چالش‌هـا در حـوزه امنیـت بانکـداری الکترونیـک، نبـود آگاهـی مشـتریان از تهدیـدات امنیتـی و کم‌توجهـی آنـان نسـبت بـه توصیه‌هـای امنیتـی ارائـه شـده از طـرف بانک‌هـا و موسسـات مالـی اسـت. ازایـن‌رو لازم اسـت بانک‌هـا و موسسـات مالـی بـرای پاسـخگویی بـه ایـن چالش‌هـا و مدیریـت مؤثـر امنیـت اطلاعـات، برنامه‌هـای آموزشـی و آگاهی‌رسـانی در حـوزه امنیـت اطلاعـات را بـرای کارکنـان و مشـتریان خـود بـه صـورت مسـتمر در نظـر بگیرنـد و نهادینه‌سـازی فرهنـگ امنیـت اطلاعـات را بـه عنـوان یـک ضرورت، مـورد توجـه قـرار دهنـد.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- ضرورت تأمین امنیت اطلاعات در بانک را درک کردید.	
۲- لزوم نهادینه کردن فرهنگ امنیت اطلاعات در کارکنان بانک را درک کردید.	

خودآزمایی جلسه دوم :

۱. دلایل اصلی که بانک‌ها به سراغ تأمین امنیت اطلاعات می‌روند، شامل کدامیک از موارد زیر می‌شود؟
الف) کسب اعتماد مشتریان
ب) حفاظت از اطلاعات مشتریان
ج) حفظ تداوم و دسترس‌پذیری سامانه‌ها و سرویس‌های بانکی
د) همه موارد

۲. کدامیک از جملات زیر صحیح نمی‌باشد؟
الف) هزینه انجام اقدامات امنیتی و پیشگیری از یک حادثه امنیتی از هزینه بازیابی و کنترل آن بیشتر خواهد بود.
ب) حفظ امنیت اطلاعات و انجام اقدامات امنیتی پیشگیرانه، باعث صرفه‌جویی در زمان و منابع مالی سازمان می‌شود.
ج) ایجاد وقفه در فرایندها و سرویس‌های حیاتی و اصلی سازمان، باعث هدر رفتن منابع مالی می‌شود.
د) هیچ کدام

۳. کدامیک از موارد زیر می‌تواند امنیت اطلاعات یک بانک را با مخاطره مواجه سازد؟
الف) عدم دانش و آگاهی کافی کارکنان نسبت به نکات امنیتی
ب) ناآگاهی مشتریان از تهدیدات امنیتی و کم‌توجهی آنان نسبت به توصیه‌های امنیتی
ج) نبود نهادینه‌سازی فرهنگ امنیت اطلاعات در سازمان
د) همه موارد

۴. کدامیک از جملات زیر صحیح نیست؟
الف) وجود خدمات متنوع و پیشرفته در حوزه بانکداری یکی از ملاک های انتخاب مشتریان بانک‌ها است.
ب) حفاظت از اطلاعات برای ایجاد و حفظ اعتماد بین بانک و مشتریان آن، ضروری است.
ج) به دلیل گسترش روزافزون تبادلات حساس بانک از طریق شبکه‌های رایانه‌ای و سرویس‌های الکترونیک، برقراری امنیت اطلاعاتی دارای اولویت نیست.
د) تمرکز مهاجمان نیز بر روش‌های جدید کلاهبرداری از طریق زیرساخت‌های الکترونیک شکل گرفته است.

پاسخ‌نامه تشریحی

خودآزمایی جلسه دوم

:

۱. پاسخ صحیح، گزینه «د»
لـزوم تأمیـن امنیـت اطلاعـات در بانک‌هـا به جهت کسـب اعتماد مشـتریان، حفاظت از اطلاعات مشـتریان و حفظ تـداوم و دسـترس‌پذیری سـامانه‌ها و سرویس‌هـای بانکی می‌باشـد.

۲. پاسخ صحیح، گزینه «الف»
هزینه پیشگیري از يك حادثه امنيتي هميشه كم‌تر از بازيابي و كنترل آن است.

۳. پاسخ صحیح، گزینه د»
عـدم دانـش و آگاهـی کافـی کارکنان نسـبت به نـکات امنیتـی، ناآگاهی مشـتریان از تهدیدات امنیتـی و کم‌توجهی آنـان نسـبت بـه توصیه‌هـای امنیتـی و نبـود نهادینه‌سـازی فرهنـگ امنیت اطلاعـات در سـازمان، امنیـت اطلاعات بانـک را بـه خطـر می انـدازد.

۴. پاسخ صحیح، گزینه «ج»
بـا توجـه بـه گسـترش روزافـزون تبـادلات حسـاس بانـک از طریـق شـبکه‌های رایانـه‌ای و سرویس‌هـای الکترونیک، برقـراری امنیـت اطلاعـات همـواره دارای اهمیـت و اولویت اسـت.

خلاصه فصل اول

جلسه اول

اطلاعات، همانند سایر دارایی‌های مهم سازمان، دارای ارزش بوده و نیازمند حفاظت مناسب می‌باشد. امنیت اطلاعات فرایندی است که براساس آن از اطلاعات در برابر حملات و تهدیدات مختلف محافظت می‌شود. تأمین امنیت اطلاعات عبارت است از فراهم نمودن امکانی که اطلاعات درست در زمان مناسب، در دسترس افراد مجاز قرار گیرد و سه پارامتر محرمانگی (C)، یکپارچگی (I) و دسترس‌پذیری (A) آن حفظ شود.

در تأمین امنیت اطلاعات، رعایت سه گام پیشگیری، نگهداری و واکنش، بسیار حائز اهمیت می‌باشد. تمرکز اصلی در تأمین امنیت اطلاعات انجام اقدامات پیشگیرانه است. هزینه پیشگیري از يك حادثه امنيتي همیشه کمتر از بازيابي و کنترل آن است. اما اقدامات پیشگیرانه به تنهایی کافی نیستند و لازم است سازمان به‌طور پیوسته از برنامه‌های نگهداری برای محافظت از دارایی‌ها و سیستم‌های خود استفاده کند. همچنین در صورت بروز یک حادثه امنیتی، قابلیت واکنش در برابر حوادث، بسیار حائز اهمیت است.

جلسه دوم

روند رو به رشد حملات سازمان‌یافته به بنگاه‌های مالی و ظهور تهدیدات امنیتی نشان می‌دهد، مسئله پایش و نظارت دایمی و مراقبت از امنیت اطلاعات مشتریان، یکی از دغدغه‌های اساسی بانک‌ها بوده و یک ضرورت اجتناب‌ناپذیر است. اطلاعات یکی از مهم‌ترین سرمایه‌های بانک‌ها و موسسات مالی است و حفاظت از اطلاعات برای ایجاد و حفظ اعتماد بین بانک و مشتریان آن ضروری می‌باشد. یکی از مهم ترین دلایلی که بانک‌ها مشتاق به سرمایهگذاری در امر امنیت هستند، کسب اعتماد مشتریان است. یکی دیگر از دلایل اهمیت امنیت اطلاعات این است که باعث افزایش دسترس‌پذیری و تداوم کسب و کار بانک می‌شود.

در تأمین امنیت اطلاعات توجه به این نکته ضروری است که نباید مقوله امنیت اطلاعات در سازمان‌ها در سطح فناوری محدود شود. نیروی انسانی و کارکنان سازمان، به مراتب نقش کلیدی‌تری در ارتقای سطح امنیت دارند. در یک سازمان، به ویژه در یک بانک یا موسسه مالی، عدم وجود دانش و آگاهی کافی کارکنان در حوزه امنیت، همواره به‌عنوان مهمترین تهدید امنیتی، مطرح است و نبود پایبندی و رعایت اصول و الزامات امنیتی از سوی نیروی انسانی، می‌تواند زمینه ایجاد پتانسیل‌هایی جهت استفاده مهاجمان را فراهم آورد و باعث بُروز مشکلات امنیتی در سازمان گردد. همچنین، ناآگاهی مشتریان از تهدیدات امنیتی و کم‌توجهی آنان نسبت به توصیه‌های امنیتی ارائه شده از طرف بانک‌ها و موسسات مالی نیز می‌تواند یکی از عوامل مؤثر بر امنیت اطلاعات باشد.

بنابراین، لازم است بانک‌ها و موسسات مالی برای مدیریت مؤثر امنیت اطلاعات، برنامه‌های آموزشی و آگاهی‌رسانی در حوزه امنیت اطلاعات را برای کارکنان و مشتریان خود به صورت مستمر در نظر بگیرند و نهادینه‌سازی فرهنگ امنیت اطلاعات را به عنوان یک ضرورت، مورد توجه قرار دهند.

فصل دوم

امنیت فیزیکی و محیطی

جلسه سوم:
امنیت فیزیکی و محیطی و انواع آن

جلسه چهارم:
محافظت در برابر تهدیدات فیزیکی و محیطی

فصل سوم:
تهدیدات امنیتی در شبکه های رایانه‌ای
فصل چهارم:
امنیت در مقابله با تهدیدات فضای سایبری
فصل پنجم:
امنیت تجهیزات قابل حمل
فصل ششم:
توصیه های امنیتی در خدمات بانکی
فصل هفتم:
جرایم رایانه‌ای و تعهدنامه عدم افشای اطلاعات
فصل هشتم:
پیاده سازی امنیت در سازمان ها

جلسه سوم

امنیت فیزیکی و محیطی و انواع آن

۵۱	اهداف یادگیری
۵۲	پیش آزمون
۵۴	امنیت فیزیکی و محیطی
۵۵	انواع راهکارهای امنیت فیزیکی و محیطی
۵۶	استفاده از حصارهای مناسب امنیت فیزیکی
۶۷	حفظ امنیت ورودی ساختمان ها و مراکز داده حساس
۷۲	استقرار و حفاظت از تجهیزات
۷۳	محافظت در برابر تهدیدات بیرونی و محیطی
۷۴	تهیه نسخ پشتیبان از اطلاعات و ایجاد سایت های پشتیبان
۷۵	رعایت امنیت در کابل کشی
۷۵	رعایت ملاحظات امنیتی در خروج دارایی ها
۷۵	حفظ امنیت تجهیزات خارج از سازمان
۷۶	رعایت امنیت تجهیزات بدون مراقبت کاربر
۷۷	آموزش کارکنان
۷۸	میزان دستیابی به اهداف یادگیری
	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. انواع راهکارهای امنیت فیزیکی و محیطی را بشناسد.
۲. لزوم برقراری امنیت فیزیکی و محیطی را درک نماید.

پیش‌آزمون جلسه سوم :

۱. کدامیک از موارد زیر درباره امنیت فیزیکی و محیطی صحیح می‌باشد؟

الف) پیشگیری از دسترسی فیزیکی غیرمجاز و خسارت به اطلاعات و دارایی‌های سازمان

ب) جلوگیری از وقوع حوادث و بلایای طبیعی

ج) شناسایی و پاسخگویی سریع به حوادث و تهدیدات محیطی و بیرونی

د) گزینه الف و ج

۲. کدامیک از جملات زیر صحیح نمی‌باشد؟

الف) صفحه نمایش رایانه‌ها باید به‌گونه‌ای باشد که ریسک رویت اطلاعات توسط اشخاص غیرمجاز در زمان استفاده کاهش یابد.

ب) آوردن لپ تاپ و رسانه‌های ذخیره سازی قابل حمل شخصی به داخل سازمان بلامانع است.

ج) باید حتی‌الامکان از خوردن، آشامیدن و سیگار کشیدن در نزدیکی تجهیزات پردازش اطلاعات خودداری شود.

د) کارکنان باید در زمان ترک میز کار، صفحه نمایش خود را قفل کنند.

پاسخ‌نامه

پیش‌آزمون جلسه سوم

:

	الف	ب	ج	د
۱				
۲				

امنیت فیزیکی و محیطی

:

از اینکه افراد اتومبیل خود را در پارکینگ می‌گذارند یا روی آن دزدگیر نصب می‌کنند، برای ویلای خود سگ نگهبان می‌گذارند، یا دور محیط‌های نظامی را حصار یا سیم خاردار می‌کشند و تنها به افراد خاصی مجوز ورود به مراکز حیاتی و حساس سازمان را می‌دهند، چه هدفی را دنبال می‌کنند؟
هرگاه صحبت از تأمین امنیت به میان می‌آید، اولین اقدامات امنیتی که به فکرمان می‌رسد، انجام راهکارهای فنی همچون استفاده از نرم افزارهای ضد ویروس، بکارگیری کلمات عبور قوی، استفاده از دیواره آتش و غیره می‌باشد. اما با وجود تمام این راهکارهای امنیتی و صرف هزینه‌های زیاد، چنانچه امنیت فیزیکی و محیط کار شما مناسب نباشد، یک دزد یا فرد سودجو می‌تواند به راحتی وارد شود و اطلاعات محرمانه شما را کپی کند یا سیستم‌های شما را به سرقت ببرد. همچنین اگر درب اتاق بایگانی اسناد محرمانه، قفل مناسبی نداشته باشد و یا کلید آن در اختیار همه باشد، خرید و یا اجرای راهکارهای امنیتی گران قیمت، بی فایده خواهد بود.
امنیت فیزیکی و محیطی چیزی است که ما همه روزه با آن درگیر هستیم و نمی‌توانیم ادعا کنیم که امنیت فیزیکی و محیط پیرامون ما اهمیت چندانی ندارد. هدف اصلی امنیت فیزیکی و محیطی، پیشگیری از دسترسی فیزیکی غیرمجاز و خسارت به اطلاعات و دارایی‌های شخصی و سازمانی و همچنین شناسایی و پاسخگویی سریع به حوادث و تهدیدات محیطی و بیرونی می‌باشد.

انواع راهکارهای امنیت فیزیکی و محیطی

:

راهکارها و اقدامات کنترلی زیادی برای تأمین امنیت فیزیکی و محیطی وجود دارد که در ادامه به معرفی مهم‌ترین آنها می‌پردازیم.

استفاده از حصارهای مناسب امنیت فیزیکی

:

• باید تمام درب ها به‌طور مناسب در برابر دسترسی غیرمجاز با روش‌های کنترلی مناسب از جمله قفل ها، سامانه‌های هشداردهنده و غیره محافظت شوند.
• درب ها و پنجره ها زمانی که مراقبت وجود ندارد، قفل شوند و حفاظ بیرونی برای پنجره‌ها، به‌خصوص برای پنجره هایی که در طبقات پایین قرار دارند، در نظر گرفته شود.

حفظ امنیت ورودی ساختمان‌ها و مراکز داده حساس

:

• تمامی کارکنان سازمان باید جهت ورود به ساختمان از کارت پرسنلی (یا سایر سیستم‌های ثبت ورود و خروج) استفاده کنند.
• کنترل ورود و خروج به ساختمان‌ها باید توسط نگهبان یا حراست کنترل شود.
• ورود و خروج سایر مراجعین اعم از پیمانکاران، نمایندگی ها، شرکت های همکار و غیره باید با استفاده از فرم کنترل تردد ثبت شود. ورود و خروج مشتریان به شعب باید توسط دوربین‌های مدار بسته کنترل شود.

• کلیه ورود و خروج ها به اتاق سرور و اماکن با پردازش اطلاعات حساس و همچنین کلیه فعالیت های انجام شده در این مکان ها باید توسط دوربین های مدار بسته به طور کامل و به صورت تمام وقت تصویربرداری و ضبط شوند.

استقرار و حفاظت از تجهیزات

:

• تجهیزات باید به گونه ای مستقر یا محافظت شوند تا احتمال وقوع آسیب های ناشی از تهدیدات و خطرات فیزیکی و محیطی مانند سرقت، آتش‌سوزی، انفجار، دود، آب، گردو غبار و غیره و فرصت های دسترسی غیرمجاز، کاهش یابند.
• صفحه نمایش رایانه‌ها به گونه‌ای باشد که احتمال رویت اطلاعات توسط اشخاص غیرمجاز در زمان استفاده کاهش یابد.
• در هنگام استفاده از لپ تاپ و تبلت‌های شخصی یا سازمانی در اماکن عمومی باید مراقب بود تا صفحه نمایش آنها توسط افراد غیرمجاز رویت نشود.
• بهتر است از خوردن، آشامیدن و سیگار کشیدن در نزدیکی تجهیزات پردازش اطلاعات خودداری شود.
• تعمیر و سرویس تجهیزات سازمانی باید فقط توسط کارکنان مجاز انجام شود. در صورت استفاده از پیمانکاران و سایر اشخاص جهت انجام تعمیرات تجهیزات، لازم است اطلاعات حساس از تجهیزات پاک شده و موارد امنیتی رعایت شوند.
• برای تعمیر تجهیزات و رسانه‌های ذخیره سازی شخصی نیز باید مراقب تصاویر خانوادگی و اطلاعات شخصی ذخیره شده بر روی آنها بود و پیش از تحویل به تعمیرکار، اطلاعات مهم و شخصی را پاک نمود.
• باید از صحت عملکرد دوربین‌های مدار بسته اطمینان حاصل نمود تا در صورت وجود خرابی و مشکل در ضبط تصاویر، سریعاً نسبت به رفع مشکل اقدام شود.
• رسانه‌های ذخیره‌سازی نظیر کاغذها، CD، DVD، فلش یا هارد دیسک که حاوی اطلاعات محرمانه و حساس سازمان باشند، لازم است از روشهای امن از بین بروند و امحا شوند. به عبارت دیگر به جای اینکه راهی سطل زباله شوند و به راحتی قابل سرقت و سوءاستفاده باشند، برای کاغذ، CD و DVD باید از طریق دستگاه کاغذ یا CD خرد کن امحا شوند و در مورد فلش و هارد دیسک از ابزارها ونرم افزارهای مخصوص پاکسازی اطلاعات استفاده نمود. این باعث می‌شود که همه به این کار عادت کنند و هیچ اطلاعات بی مصرفی به دست افراد سوءاستفاده‌گر نیفتد.
• در صورت خرابی رسانه‌های ذخیره‌سازی شخصی نیز که دیگر قابل تعمیر نمی‌باشند باید قبل از دور انداختن آنها، اطلاعات ذخیره شده بر روی آنها را از بین برد و پاک نمود. برای مثال CD یا DVDها را شکست و به تکه‌های کوچک تبدیل کرد، کاغذها را به تکه‌های ریز خرد نمود، فلش و هارد دیسک را با کمک ابزار و یا وسایل سنگین، شکست و از بین برد. در این صورت چنانچه رسانه‌های ذخیره‌سازی شما بعد از دور ریختن، در اختیار افراد سودجو قرار گیرند، بازیابی اطلاعات داخل آنها سخت و یا غیر ممکن خواهد بود.

محافظت در برابر تهدیدات بیرونی و محیطی

:

• مواد آتش زا و خطرناک باید در مکانی حفاظت شده و دور از اتاق های حاوی اطلاعات و سیستم های پردازش اطلاعات نگهداری شوند.
• مواد قابل اشتعال نباید در اتاق سرور و مراکز دارای اطلاعات حساس نگهداری شوند.
• کپسول های آتش نشانی باید در مکان های مختلف جهت مهار آتش نصب شده و در بازه‌های زمانی مشخص

بـه منظـور اطمینـان از صحـت کارکـرد بازبینـی شـوند.

• لازم اسـت اثـرات ناشـی از هـر حادثـه قابـل وقـوع در نزدیکـی سـازمان، از قبیـل آتش‌سـوزی در سـاختمان هـای مجـاور، نشـت آب در سـقف طبقـات پاییـن تـر یـا انفجـار در خیابـان هـای مجـاور، در نظـر گرفتـه شـود.

• طراحـی و انتخـاب مـکان هـای حـاوی اطلاعـات و سیسـتم هـای پـردازش اطلاعـات بایـد بـه صورتـی انجـام شـود کـه ریسـک حاصـل از تهدیداتـی نظیـر سرقـت، آتش‌سـوزی، انفجـار، آب‌گرفتگـی، تجمیـع گردوغبـار، تداخـل امـواج حاصـل از دسـتگاه‌های الکتریکـی و تشعشـعات الکترومغناطیسـی بـه حداقـل برسـند.

تهیه نسخ پشتیبان از اطلاعات و ایجاد سایت‌های پشتیبان

:

• یکـی از مهم‌تریـن کارهـای هـر فـرد یـا سـازمان تهیـه نسـخه پشـتیبان از اطلاعـات اسـت. امـا محـل نگهـداری نسـخ پشـتیبان نیـز از اهمیـت بالایـی برخـوردار اسـت. لازم اسـت نسـخ پشـتیبان را بـه صـورت رمزنـگاری شـده تهیـه و بـر روی یـک رسـانه ذخیره‌سـازی مناسـب، در مـکان امنـی نگهـداری نمـود.

فرامـوش نکنیـد، اگـر روزی هـارد دیسـک رایانـه شـما از کار بیفتـد، اطلاعـات ذخیـره شـده روی رایانـه بـه دلیلـی از بیـن بـرود و یـا لـپ تـاپ شـما مفقـود گـردد، از اینکـه از فایـل هـای مهـم خـود نسـخه پشـتیبان تهیـه کـرده ایـد بسـیار خوشـحال و راضی خواهیـد بـود.

• سـازمان‌ها می‌بایسـت سـایت‌های پشـتیبانی (مراکـز داده پشـتیبان) را بـا شرایـط سـایت اصلـی (مرکـز داده اصلـی) در نظـر گیرنـد تـا در مواقـع بحرانـی و وقـوع حـوادث غیرمترقبـه، فعالیت‌هـای متوقف شـده در مرکـزداده اصلی سـازمان، از طریق این سـایت‌ها از سر گرفتـه شـود. لازم بـه ذکـر اسـت کـه بانـک ملـت چنیـن شرایطـی را فراهم نموده اسـت.

شـکل ۱:تهیه نسخ پشتیبان

رعایت امنیت در کابل کشی

:

• بایـد کابـل هـای بـرق و ارتباطـات مـورد اسـتفاده بـرای انتقـال داده یـا پشـتیبانی از خدمـات اطلاعاتـی (به‌ویـژه در شـعب بانـک)، در برابـر قطـع شـدن (بـرق یـا شـبکه) یـا وارد آمـدن خسـارت، محافظـت شـوند و بـه صـورت مناسـب در داخـل داکت قـرار گیرنـد.

بـا لحـاظ روش‌هـای ارزش‌گـذاری فـوق می‌تـوان گفت بهای تمام‌شـده تاریخـی، ارزش متعارف جاری مؤسسـه را گـزارش نمی‌کند بلکـه معـرف انـدازه‌ای از حقـوق صاحبـان سـهام اسـت کـه مسـتقیماً متأثـر از اندازه‌گیری‌هـای بـه‌کار رفتـه بـرای دارایی‌هـا و بدهی‌هـا در زمـان مبادلـه بوده اسـت.

رعایت ملاحظات امنیتی در خروج دارایی ها

:

• تجهیزات، اطلاعات یا نرم افزارها، نباید بدون مجوز قبلی از سازمان خارج شوند.
• ورود و خروج دارایی های سازمان باید توسط نگهبانی یا حراست کنترل شود و تنها با رویت مجوز خروج دارایی، اجازه خروج داده شود.

حفظ امنیت تجهیزات خارج از سازمان

:

• باید برای دارایی های خارج از محوطه سازمان، با توجه به مخاطرات مختلف ناشی از انجام کار در خارج از مرز فیزیکی سازمان، امنیت برقرار شود.
• تجهیزات و رسانه هایی که به خارج از محوطه سازمان برده می شوند، نباید بدون حضور فرد مجاز در محل های عمومی رها شوند. مسئولیت نگهداری و حفظ امنیت تجهیزات خارج از محوطه سازمان بر عهده شخص امانت گیرنده است، از این رو می بایست از آن دارایی در برابر آسیب، سرقت یا سایر بلایا محافظت نماید.

رعایت امنیت تجهیزات بدون مراقبت کاربر

:

• کاربران باید اطمینان داشته باشند که تجهیزات بدون متصدی، حفاظت مناسبی دارند. لذا ضرورت دارد در زمان ترک میز کار، صفحه نمایش خود را قفل کرده و حتی در زمان ترک اتاق کار، در صورت نیاز، درب اتاق خود را نیز قفل کنند.
• کاربران بهتر است حتی الامکان از برنامه های کاربردی و خدمات شبکه در زمانی که مورد نیاز نیستند، خارج شوند.
• باید از استفاده غیرمجاز از تجهیزات نسخه برداری و سایر فناوری های تکثیر (مثلاً دستگاه کپی، اسکنرها، پرینترها) جلوگیری شود و این تجهیزات بدون مراقبت کاربر رها نشوند.
• مستندات محرمانه و رسانه های ذخیره سازی قابل حمل همچون لپ تاپ، تبلت، فلش مموری و غیره باید در ساعات غیر کاری و در مواقعی که کاربر مربوطه به آنها نیازی ندارد، در یک محل امن و قفل دار به عنوان مثال در کشو یا گاوصندوق یا کمد نگهداری شوند.

آموزش کارکنان

:

• مهم ترین نکته در تأمین امنیت، آموزش کارکنان می باشد. لازم است همهٔ نکات مربوط به امنیت فیزیکی و محیطی به کارکنان سازمان آموزش داده شود و کارکنان از انواع تهدیدات فیزیکی و محیطی و خطرات ناشی از عدم رعایت نکات امنیتی در این حوزه آگاه باشند..

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید،
در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- انواع راهکارهای امنیت فیزیکی و محیطی را شناختید.	
۲- لزوم برقراری امنیت فیزیکی و محیطی را درک کردید.	

خودآزمایی جلسه سوم :

۱. کدامیک از اقدامات زیر از راهکارهای تأمین امنیت فیزیکی و محیطی می‌باشد؟
الف) امنیت تجهیزات خارج از سازمان
ب) تهیه و نگهداری نسخ پشتیبان
ج) امنیت تجهیزات بدون مراقبت کاربر
د) همه موارد

۲. کدامیک از اقدامات زیر جهت محافظت در برابر تهدیدات بیرونی و محیطی لازم است انجام شود؟
الف) مواد آتش زا و خطرناک باید در مکانی حفاظت شده و دور از اتاق های حاوی اطلاعات و سیستم های پردازش اطلاعات نگهداری شوند.
ب) تعمیر و سرویس تجهیزات باید فقط توسط کارکنان مجاز انجام شود.
ج) تجهیزات، اطلاعات یا نرم افزارها، نباید بدون مجوز قبلی از سازمان خارج شوند.
د) کارکنان در زمان ترک میز کار خود، باید صفحه نمایش خود را قفل کنند.

۳. جهت از بین بردن مستندات کاغذی کدام گزینه صحیح‌تر است ؟
الف) جهت جلوگیری ازدسترسی افراد غیرمجاز ، آن ها را خرد کرده و داخل سطل زباله بیندازیم.
ب) جهت از بین بردن اطلاعات محرمانه، آن ها را از طریق دستگاه کاغذ خرد کن امحا کنیم.
ج) مستندات کاغذی محرمانه را دور نریخته و در جای امنی نگهداری کنیم.
د) همه موارد

۴. کدام گزینه در خصوص امنیت ورودی ساختمان ها ومراکز داده صحیح است ؟
الف) کنترل ورود و خروج به ساختمان‌ها باید توسط نگهبان یا حراست انجام شود.
ب) ورود و خروج مراجعین اعم از پیمانکاران، نمایندگی ها، شرکت های همکار و غیره باید با استفاده از فرم کنترل تردد ثبت شود.
ج) کلیه ورود و خروج ها به اتاق سرور و اماکن با پردازش اطلاعات حساس باید توسط دوربین های مدار بسته به طور کامل و به صورت تمام وقت تصویربرداری و ضبط شوند.
د) همه موارد

پاسخ‌نامه تشریحی

خودآزمایی جلسه سوم

۱. پاسخ صحیح، گزینه «د»

برخی از راهکارها و اقدامات کنترلی جهت تأمین امنیت فیزیکی و محیطی عبارت‌اند از:

- استفاده از حصارهای مناسب امنیت فیزیکی
- امنیت ورودی ساختمان‌ها و مراکز داده‌های حساس
- استقرار و حفاظت تجهیزات
- محافظت در برابر تهدیدات بیرونی و محیطی
- تهیه نسخ و سایت‌های پشتیبان
- امنیت کابل کشی
- خروج دارایی‌ها
- امنیت تجهیزات خارج از سازمان
- امنیت تجهیزات بدون مراقبت کاربر

۲. پاسخ صحیح، گزینه «الف»

مواد آتش زا و خطرناک باید در مکانی حفاظت شده و دور از اتاق های حاوی اطلاعات و سیستم های پردازش اطلاعات نگهداری شوند.

۳. پاسخ صحیح، گزینه «ب»

حتی المقدور بهتر است جهت از بین بردن اسناد حاوی اطلاعات محرمانه، آنها را از طریق دستگاه کاغذ خرد کن امحا نمود.

۴. پاسخ صحیح، گزینه «د»

همهٔ موارد ذکرشده لازم است رعایت گردند.

جلسه چهارم

محافظت در برابر تهدیدات فیزیکی و محیطی

۸۳	اهداف یادگیری
۸۴	پیش آزمون
۸۶	انواع تهدیدات فیزیکی و محیطی
۸۷	بلایای طبیعی و حوادث غیر مترقبه
۸۷	تهدیدات انسانی
۸۸	مشکلات فنی
۸۸	برنامه ریزی برای پاسخگویی به حوادث غیرمترقبه
۹۱	مرحله آماده سازی پیش از وقوع حادثه
۹۳	مرحله وقوع حادثه
۹۵	مرحله بازیابی پس از وقوع حادثه
۹۶	میزان دستیابی به اهداف یادگیری
۹۸	خودآزمایی
۱۰۱	خلاصه فصل دوم

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. انواع تهدیدات فیزیکی و محیطی را بشناسد.
۲. با نحوه پاسخگویی به حوادث غیرمترقبه آشنا شود.

پیش‌آزمون جلسه چهارم :

۱. در زمان‌های قدیم، ساخت قلعه‌ها، دیوارهای بلند، دکل‌های دیده‌بانی، سنگرها جهت تأمین ..... انجام می‌گرفت.

الف) امنیت ارتباطات

ب) امنیت فیزیکی و محیطی

ج) امنیت عملیات

د) هیچ کدام

۲. به نظر شما، کدامیک از عوامل انسانی زیر می‌تواند مهم‌ترین تهدید برای سازمان محسوب شود؟

الف) کارکنان ناراضی

ب) رقبا

ج) هکرها

د) دولت‌های خارجی

۳. کدامیک از اقدامات زیر می‌تواند منجر به کاهش خسارات ناشی از وقوع حوادث غیرمترقبه شود؟

الف) آموزش کارکنان

ب) تدوین طرح‌های مدیریت و پاسخگویی به حوادث

ج) انجام مانورهای از پیش تعیین شده نظیر مانور زلزله

د) همه موارد

پاسخ‌نامه

پیش‌آزمون جلسه چهارم

:

	الف	ب	ج	د
۱				
۲				
۳				

انواع تهدیدات فیزیکی و محیطی

:

انسان از بدو خلقت با انواع تهدیدات فیزیکی و محیطی مواجه بوده است. از همان ابتدا ایده ساخت قلعه‌ها، دیوارهای بلند، دکل‌های دیده بانی، سنگرها و غیره جهت محافظت در برابر هجوم دشمنان و بلایای محیطی شکل گرفت. در دنیای مدرن امروزی نیز تهدیدات فیزیکی و محیطی زیاد و متنوعی در خصوص امنیت وجود دارد. این نوع تهدیدات به سه دسته زیر تقسیم می‌شوند:

- بلایای طبیعی و حوادث غیر مترقبه
- تهدیدات انسانی
- مشکلات فنی

بلایای طبیعی و حوادث غیرمترقبه

:

تبلایای طبیعی به مجموعه‌ای از حوادث زیان‌بار گفته می‌شود که منشأ انسانی ندارند. این حوادث معمولاً غیرقابل پیش‌بینی بوده و یا حداقل از مدت‌های طولانی قبل، نمی‌توان وقوع آنها را پیش‌بینی نمود. بلایای طبیعی و حوادث غیرمترقبه ممکن است به انواع و اشکال مختلفی رخ دهد. زلزله، سیل، طوفان، گردباد، سونامی، تگرگ، بهمن، رعد و برق، تغییرات شدید درجه حرارت، خشکسالی و آتشفشان نمونه‌هایی از بلایای طبیعی هستند.

برخی از بلایای طبیعی، بطور غیرمستقیم، ناشی از عملکردهای انسانی هستند. برای مثال بلایای ناشی از افزایش آلودگی هوا و یا گرم شدن زمین و همچنین سیل ناشی از تخریب جنگل‌ها به دست انسان، از این جمله اند.

شکل ۱: انواع بلایای طبیعی

تهدیدات انسانی

:

تهدیدات انسانی یکی دیگر از موارد مهمی است که می بایست در خصوص امنیت فیزیکی به آن توجه نمود. در مقابل تهدیداتی مثل گردبادها، سیل و سونامی‌ها شاید نتوان کار خاصی را انجام داد، اما در برابر تهدیدات انسانی تا حد

زیـادی می‌تـوان از وقـوع آنهـا جلوگیـری کـرد.
تهدیـدات انسـانی بـه دو دسـته عمـدی و غیرعمـدی (سـهوی) دسـته بنـدی می‌شـوند. تهدیـدات عمـدی، شـامل افـراد یـا گروهـی هسـتند کـه بـه عمـد و بـا نیـت بدخواهانـه اعمالـی همچـون دزدی و سرقـت، شـنود، هـک، دسترسـی غیرمجـاز، جعـل هویـت، شـورش و اعتصـاب و غیـره انجـام می‌دهنـد. ایـن گـروه می‌توانـد شـامل هکرهـا، رقبـا، کارکنـان ناراضـی سـازمان، افـراد سـودجو و خرابـکار، دزد و غیـره باشـد.
تهدیـدات غیرعمـدی، افـرادی هسـتند کـه سـهواً و بـه دلیـل عـدم دانـش و آگاهـی کافـی اقداماتـی همچـون خطـای کاربـری، حـذف سـهوی اطلاعـات و افشـای سـهوی اطلاعـات محرمانـه ماننـد اطلاعـات مشـتریان و غیـره را انجـام می‌دهنـد.
صرف‌نظـر از موفقیـت و یـا عـدم موفقیـت مهاجـمان و بـا وجـود بکارگیـری راهکارهـای امنیتـی مختلـف در یـک سـازمان، عـدم وجـود دانـش و آگاهـی کافـی کاربـران در حـوزه امنیـت اطلاعـات، همـواره به‌عنـوان مهم‌تریـن تهدیـد امنیتـی مطـرح اسـت و نبـود پایبنـدی و رعایـت اصـول و سیاسـت‌های امنیتـی تدویـن شـده، می‌توانـد موجـب ایجـاد پتانسـیل‌هایی شـود کـه توسـط مهاجـمان، اسـتفاده شـده و باعـث بُـروز مشـکلات امنیتـی در سـازمان گـردد.
همچنیـن نمونه‌هـای مختلفـی از قانـون شـکنی‌ها و تخلفـات امنیتـی وجـود دارد کـه یـک ویژگـی مشـترک در همـه آنهـا دیـده می‌شـود؛ "همـه آنهـا توسـط افـراد بـه وقـوع پیوسـته‌اند." به‌عنـوان مثـال، افـراد، عوامـل نفـوذ و هکرهـا بوده‌انـد، ویروس‌هـای رایانـه‌ای توسـط افـراد نوشـته شـده‌اند و رمزهـای عبـور را نیـز افـراد دزدیده‌انـد. ایـن افـراد بـه صورت‌هـای مختلفـی در بُـروز مشـکلات امنیتـی تأثیـر دارنـد، بعضـی از آنهـا بـا دنبـال نکـردن سیاسـت‌ها و روال‌هـای امنیتـی سـازمان، بـه فراموشـی سـپردن ملاحظـات امنیتـی و مطلـع نبـودن از نتایـج، کارهایـی انجـام می‌دهنـد کـه سـهواً بـه وقـوع رخدادهـای امنیتـی کمـک می‌کننـد. حتـی گاهـی اشـتباه سـهوی آنهـا، می‌توانـد زمینـه موفقیـت دیگران(مهاجـمان و هکرهـا) را فراهـم نمایـد. طبـق آمارهـای بـه دسـت آمـده در دنیـا، خطاهـای کارکنـان و منابـع انسـانی، بیش‌تریـن میـزان خسـارت بـه سیسـتم‌های اطلاعاتـی سـازمان را بـه خـود اختصـاص داده اسـت. بنابرایـن، اگـر کاربـران درصـد بُـروز اشـتباهات و نقض‌هـای امنیتـی خـود را کاهـش دهنـد، بـه هـمان نسـبت نیـز شـانس موفقیـت مهاجـمان و تهدیـدات عمـدی کاهـش پیـدا خواهـد کـرد.

مشکلات فنی :

احتـمال وقـوع مشـکلات فنـی بـر خـلاف بلایـای طبیعـی، بسـیار زیـاد اسـت. ایـن مشـکلات عمدتـاً بـا خرابـی تجهیـزات، قطعـی سیسـتم‌های ارتباطـی و شـبکه و خسـارت بـه امکانـات عمومـی اتفـاق می‌افتـد. برخـی از آنهـا از جملـه مـوارد ذیـل مـی باشـند:
• خرابـی تجهیـزات: تجهیـزات خواسـته یـا ناخواسـته در طـول زمـان دچـار مشـکل و خرابـی می‌شـوند. بنابرایـن وجـود تیـم نگهـداری و تعمیـرات و پشـتیبانی فنـی تجهیـزات در همـه سـازمان‌ها مـورد نیـاز اسـت.
• قطعـی سیسـتم‌های ارتباطـی و شـبکه: امـروزه سیسـتم‌های ارتباطـی از نـوع داده و صـدا نقـش حیاتـی را در سـازمان‌ها ایفـا می‌کننـد. قطعـی ارتباطـات می‌توانـد شـامل قطعـی خطـوط ارتباطـی صـوت و یـا ارتباطـات شـبکه اطلاعاتـی نیـز شـود.
• خسـارت بـه امکانـات عمومـی: امکانـات عمومـی شـامل سیسـتم‌های ارتباطـی، آب‌رسـانی، گازرسـانی، بـرق، خنـک کننده‌هـا، سیسـتم‌های گرمایشـی و غیـره می‌باشـند. ورود خسـارت بـه ایـن امکانـات عمومـی، باعـث بـروز مشـکلات زیـادی بـرای سـازمان می‌شـود و رونـد کاری سـازمان را دچـار اختـلال و وقفـه می‌کنـد. وجـود ژنراتورهـای بـرق و سیسـتم‌های بـرق اضطـراری(UPS) و ارتباطـی جایگزیـن، می‌توانـد تـا حـد زیـادی کمـک کننـده باشـد. انـواع ایـن مشـکلات در سـازمان‌های مختلـف، خسـارت‌های مختلفـی بـه دنبـال دارد. شـاید قطعـی سیسـتم‌های خنـک کننـده یـک سـازمان در شـهرهای جنوبـی کشـور در روزهـای گـرم، منجـر بـه ایجـاد وقفـه در کسـب و کار آن سـازمان شـود، یـا قطعـی بـرق در یـک سیسـتم بانکـی حتـی بـرای ۵ دقیقـه هـم قابـل قبـول نباشـد، زیـرا منجـر بـه ضرر بسـیار زیـادی بـرای کسـب و کار بانـک خواهـد شـد.

برنامه ریزی برای پاسخگویی به حوادث غیرمترقبه

:

با آنکه اغلب بلایای طبیعی، خارج از کنترل انسان است، امّا خسارات و آسیب های ناشی از آنها، به‌طور چشمگیر قابل کنترل است. این موضوع ارتباط مستقیمی با اقدامات پیشگیرانه توسط انسان دارد. برای مثال، استحکام ساختمان‌ها جهت کاهش خسارات ناشی از زلزله یا ایجاد پوشش گیاهی و ساخت بندها و سدها جهت کاهش خسارات ناشی از سیل، از جمله موارد پیشگیرانه می‌باشند. بنابراین، اگر مشکلات و خرابی‌های احتمالي ناشي از این حوادث پیش‌بیني نشود، هزینه بازسازي و ترمیم صدمات ناشي از آن، زیاد خواهد شد.

البته ممکن است اقدامات پیشگیرانه، همیشه مانع از بروز حوادث نشود. بنابراین، در نظر گرفتن تمهیدات و راهکارهایی برای مدیریت و کاهش صدمات ناشی از حوادث غیرمترقبه و برنامه‌ریزی و پاسخگویی به این نوع حوادث می‌تواند در کاهش آسیب‌های ناشی از حوادث و بلایای طبیعی مؤثر باشد. به عنوان نمونه، یکی از این راهکارها، تهیه نسخه پشتیبان از اطلاعات و نگهداری آن ها در داخل گاوصندوق یا مکانی امن است که در زمان بروز حادثه، اطلاعات از بین رفته به حداقل برسد و اطلاعات مهم حفظ گردند.

پس، وجود طرح‌ها و راهکارهای مناسب در زمان وقوع حادثه، از یك سو باعث تقویت پایه و اساس سازمان می‌شود و از سوي دیگر، میزان خسارات ناشی از این حوادث را به شدت کاهش مي‌دهد.

یکی دیگر از راه‌های کاهش آثار مخرب بلایای طبیعی، آموزش است. آموزش، می‌تواند به کاهش اثرات روانی منفی در بلایای طبیعی کمک کند. انجام مانورهای زلزله یکی از اقدامات آموزشی برای آمادگی در زمان مواجه شدن با زلزله می شوند.

اقداماتی که جهت مدیریت و پاسخگویی به حوادث غیرمترقبه و بلایاي طبیعي انجام می‌شوند، شامل مراحل کلی زیر می‌شوند:

مرحله آماده‌سازی پیش از وقوع حادثه

:

اقداماتی که در این مرحله انجام می‌شود شامل موارد زیر می‌باشد:

- انجام فرایند شناسایی نقاط آسیب پذیر و حوادث بالقوه
- پیش‌بینی و ارزیابی آسیب‌های احتمالی ناشی از وقوع حوادث غیرمترقبه
- تعیین استراتژی‌ها و تهیه طرح‌های اجرایی مدیریت حوادث
- تعیین تیم مدیریت و پاسخگویی به حوادث، تدوین شرح وظایف و آموزش آن‌ها
- آموزش نیروی انسانی و انجام مانورهای آموزشی همچون مانور زلزله و آتش سوزی

مرحله وقوع حادثه

:

در این مرحله، قاعدتاً زماني براي برنامه‌ریزي و تصمیم‌گیري‌هاي عمده وجود ندارد و همه چیز باید از قبل در مرحله آماده‌سازی پیش‌بیني شده باشد و فقط دستورالعمل‌هاي حاصل از سناریوهاي متناسب با حادثه، به مرحله اجرا گذاشته شوند. اقدامات زیر در این مرحله انجام می‌شوند:

- شناسایی حادثه
- اعلام و آگاه‌سازی تیم‌های مدیریت حوادث
- تحلیل و ارزیابی حادثه

• عملیاتی کردن طرح‌های مدیریت حوادث
• اطلاع رسانی به ذینفعان سازمان

مرحله بازیابی پس از وقوع حادثه

:

معمـولاً پـس از وقـوع حادثـه آنچـه اهمیـت دارد اقداماتي اسـت که جهـت بازگردانـدن وضعیت به شرایـط عادي انجام می‌شـود.
اقدامـات اجرایـي ایـن مرحلـه عبارت‌اند از:
• برآورد خسارت و آسیب‌های وارده ناشی از وقوع حادثه
• تخمین زمان لازم براي بازیابی
• بازیابی فرایندهای کلیدی و باقی‌مانده
• محدودسازی، ریشه‌کنی و ترمیم حادثه
• بازگشت به عملکرد نرمال

شکل۳: مدیریت پاسخگویی به حوادث غیر مترقبه

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- انواع تهدیدات فیزیکی و محیطی را شناختید.	
۲- با نحوه پاسخگویی به حوادث غیرمترقبه آشنا شدید.	

خودآزمایی جلسه چهارم :

۱. کدامیک از موارد زیر از انواع تهدیدات فیزیکی و محیطی می‌باشد:
الف) بلایای طبیعی و حوادث غیرمترقبه
ب) تهدیدات انسانی
ج) مشکلات فنی
د) همه موارد

۲. کدامیک از موارد زیر جزو اقدامات انجام شده در مرحله آماده‌سازی پیش از وقوع حادثه نمی‌باشد؟
الف) پیش‌بینی و ارزیابی آسیب‌های ناشی از وقوع حوادث غیرمترقبه
ب) تعیین تیم مدیریت و پاسخگویی به حوادث، تدوین شرح وظایف و آموزش آن‌ها
ج) عملیاتی کردن طرح‌های مدیریت حوادث
د) آموزش نیروی انسانی و انجام مانورهای آموزشی همچون مانور زلزله و آتش سوزی و...

۳. "برآورد خسارت و آسیب‌های وارده ناشی از وقوع حادثه" از اقدامات کدام مرحله از پاسخگویی به حوادث غیرمترقبه می‌باشد؟
الف) مرحله آماده‌سازی پیش از وقوع حادثه
ب) مرحله وقوع حادثه
ج) مرحله بازیابی پس از وقوع حادثه
د) گزینه ب و ج

۴. قطع خدمت‌رسانی یک سامانه بر اثر ایجاد دسترسی غیرمجاز سهوی یک کارمند، از چه گروه تهدیداتی محسوب می شود؟
الف) تهدید انسانی عمدی
ب) تهدید انسانی غیر عمدی
ج) مشکلات فنی
د) هیچ‌کدام

پاسخ‌نامه تشریحی

خودآزمایی جلسه چهارم

۱. پاسخ صحیح، گزینه «د»

در دنیای مدرن امروزی، تهدیدات فیزیکی و محیطی زیاد و متنوعی در خصوص امنیت وجود دارد. این نوع تهدیدات به سه دسته زیر تقسیم می‌شوند:

- بلایای طبیعی و حوادث غیر مترقبه
- تهدیدات انسانی
- مشکلات فنی

۲. پاسخ صحیح، گزینه «ج»

اقداماتی که در مرحله آماده‌سازی پیش از وقوع حادثه انجام می‌شود شامل موارد زیر می شود:

- انجام فرایند شناسایی نقاط آسیب پذیر و حوادث بالقوه
- پیش‌بینی و ارزیابی آسیب‌های ناشی از وقوع حوادث غیرمترقبه
- تعیین استراتژی‌ها و تهیه طرح‌های اجرایی مقابله با بحران و مدیریت حوادث
- تعیین تیم مدیریت و پاسخگویی به حوادث، تدوین شرح وظایف و آموزش آن‌ها
- آموزش نیروی انسانی و انجام مانورهای آموزشی همچون مانور زلزله و آتش سوزی و ...

۳. پاسخ صحیح، گزینه «ج»

برآورد خسارت و آسیب‌های وارده ناشی از وقوع حادثه، در مرحله بازیابی پس از وقوع حادثه انجام می گردد.

۴. پاسخ صحیح، گزینه «ب »

قطع سرویس دهی یک سامانه بر اثر ایجاد دسترسی غیرمجاز سهوی یک کارمند از نوع تهدیدات انسانی غیرعمدی محسوب می گردد.

خلاصه فصل دوم

جلسه پنجم

هدف اصلی امنیت فیزیکی و محیطی، پیشگیری از دسترسی فیزیکی غیرمجاز و خسارت به اطلاعات و دارایی‌های سازمان و همچنین شناسایی و پاسخگویی سریع به حوادث و تهدیدات محیطی و بیرونی می‌باشد.

برخی از راهکارها و اقدامات کنترلی جهت تأمین امنیت فیزیکی و محیطی عبارت‌اند از:

- استفاده از حصارهای مناسب امنیت فیزیکی
- رعایت امنیت ورودي ساختمان‌ها و مراکز داده‌های حساس
- استقرار و حفاظت از تجهیزات
- محافظت در برابر تهدیدات بیرونی و محیطی
- تهیه نسخ پشتیبان از اطلاعات و ایجاد سایت‌های پشتیبان
- رعایت ملاحظات امنیتی در خروج دارایی‌ها
- رعایت امنیت تجهیزات خارج از سازمان
- حفظ امنیت تجهیزات بدون مراقبت کاربر
- آموزش کارکنان

جلسه ششم

در دنیای مدرن امروزی، تهدیدات فیزیکی و محیطی زیاد و متنوعی در خصوص امنیت وجود دارد. این نوع تهدیدات به سه دسته زیر تقسیم می‌شوند:

- بلایای طبیعی و حوادث غیرمترقبه مانند: زلزله، سیل، طوفان، گردباد، سونامی، تگرگ، بهمن، رعد و برق، تغییرات شدید درجه حرارت، خشکسالی و آتشفشان
- تهدیدات انسانی شامل دو دسته عمدی(مثل دزدی و سرقت، شنود، هک، دسترسی غیرمجاز، جعل هویت، شورش و اعتصاب) و غیرعمدی(مثل خطای کاربری و حذف یا افشای سهوی اطلاعات)
- مشکلات فنی شامل: خرابی تجهیزات، قطعی سیستم‌های ارتباطی و شبکه و خسارت به امکانات عمومی

اقداماتی که جهت پاسخگویی و مدیریت حوادث غیر مترقبه انجام می‌شود شامل مراحل زیر می‌شود:

- مرحله آماده‌سازی پیش از وقوع حادثه شامل: شناسایی نقاط آسیب پذیر و حوادث بالقوه، پیش‌بینی آسیب‌های احتمالی ناشی از وقوع حوادث، تدوین طرح‌های مدیریت حوادث، تعیین تیم مدیریت و پاسخگویی به حوادث، آموزش کارکنان و انجام مانورهای آموزشی
- مرحله وقوع حادثه شامل: شناسایی حادثه، اعلام به تیم مدیریت حادثه، تحلیل و ارزیابی حادثه، عملیاتی کردن طرح‌های تدوین شده و اطلاع رسانی به ذینفعان
- مرحله بازیابی پس از وقوع حادثه شامل: برآورد خسارات وارده، تخمین زمان بازیابی، بازیابی فرایندهای کلیدی، ریشه کنی و ترمیم حادثه و بازگشت به حالت نرمال

فصل اول: آشنایی با مفاهیم امنیت اطلاعات

فصل دوم: امنیت فیزیکی و محیطی

فصل سوم

تهدیدات امنیتی در شبکه‌های رایانه‌ای

جلسه پنجم:
انواع حملات سایبری و تکنیک‌های هک

جلسه ششم:
انواع بدافزارها

فصل چهارم:
امن‌سازی در مقابله با تهدیدات امنیتی

فصل پنجم:
امنیت تجهیزات قابل حمل

فصل ششم:
توصیه‌های امنیتی در خدمات بانکی

فصل هفتم:
جرایم رایانه‌ای و تعهدنامه عدم افشای اطلاعات

فصل هشتم:
پیاده‌سازی امنیت در سازمان‌ها

جلسه پنجم

انواع حملات سایبری و تکنیک های هک

۱۰۷	اهداف جلسه آموزشی
۱۰۸	پیش‌آزمون
۱۱۰	شبکه‌های رایانه‌ای و فضای سایبری
۱۱۰	انواع حملات سایبری
۱۱۲	نمونه هایی از حملات سایبری
۱۱۳	مهندسی اجتماعی
۱۱۳	حملات فیشینگ
۱۱۷	اخذ اطلاعات از طریق کلیدنگار
۱۱۸	میزان دستیابی به اهداف آموزشی
	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با مفهوم شبکه‌های رایانه‌ای و فضای سایبری آشنا شود.
۲. با مفهوم هک و حملات سایبری آشنا شود.
۳. با انواعی از تکنیک‌های هک و حملات سایبری آشنا شود.

پیش‌آزمون جلسه پنجم :

۱. به هر شبکه رایانه‌ای که متشکل از کاربران، اطلاعات، نرم‌افزار و سخت‌افزار باشد، ..... گفته می‌شود؟

الف) رایانه ب) فضای سایبری ج) سیستم د) فضای رایانه‌ای

۲. در حملات سایبری، مهاجمان و هکرها قصد انجام کدامیک از اقدام زیر را دارند؟

الف) افشا ب) منع دسترسی ج) تخریب د) همه موارد

۳. به تکنیک سوء استفاده از اطمینان یا فریب عوامل انسانی برای دسترسی به اطلاعات محرمانه چه گفته می شود؟

الف) مهندسی اجتماعی ب) هک ج) فریب دادن د) هیچ کدام

پاسخ‌نامه

پیش‌آزمون جلسه پنجم

:

	الف	ب	ج	د
۱				
۲				
۳				

شبکه‌های رایانه‌ای و فضای سایبری

:

شبکه رایانه‌ای که اغلب به طور خلاصه به آن شبکه گفته می‌شود، گروهی از رایانه‌ها و دستگاه‌هایی است که توسط کانال‌های ارتباطی به هم متصل شده‌اند. شبکه رایانه‌ای باعث تسهیل ارتباطات میان کاربران میشود و اجازه می‌دهد کاربران منابع خود را به اشتراک بگذارند. اینترنت یک شبکه جهاني است که از اتصال رایانه‌های مختلف در سراسر جهان به یکدیگر به وجود آمده است و هر کدام از آنها با ارائه خدمات، به کاربران این امکان را دهد که اطلاعات به روش‌هاي مختلف، در اختیار سایر افراد در سراسر جهان قرار گیرد یا با یکدیگر ارتباط برقرار کنند. اینترانت نیز مانند اینترنت یک شبکه است، اما در اینترانت امکان تبادل اطلاعات فقط به صورت خصوصي یا داخل سازماني وجود دارد و فقط کاربران داخلي اجازه استفاده از خدمات مختلف آن را دارند .

امروزه به هر شبکه رایانه‌ای که متشکل از کاربران، اطلاعات، نرم افزار و سخت افزار باشد، فضای سایبری گفته می‌شود. از فضای سایبری به عنوان محیطی برای انتقال داده‌ها و اطلاعات نام برده می‌شود و تنها شامل اینترنت نمی‌شود، بلکه تمامی شبکه‌ها و سیستم‌های ارتباطی- اطلاعاتی را در برمی‌گیرد. برای مثال، یك سیستم آنلاین در محیط اینترنت یا اینترانت، نمونه‌اي از فضاي سایبری است که کاربران آن مي‌توانند از طریق ایمیل یا سایر ابزارهای ارتباطی با یکدیگر ارتباط برقرار کنند.

انواع حملات سایبری

:

در دنیای امروز، تهدیدات در قالب شبکه‌های رایانه‌ای رو به افزایش است و فضای سایبری به مکانی ایده‌آل برای حملات سایبری توسط هکرها و سایر مهاجمان تبدیل شده است. هدف از حملات سایبری، دستیابی به اطلاعات افراد، سازمان‌ها و کشورها، ایجاد وقفه در کسب‌وکار ، ایجاد خدشه و آسیب رساندن بهیرساخت‌های آنها و یا اهداف مالی می‌باشد.

حملات سایبری معمولاً یک یا چندین ضلع از مثلث امنیت اطلاعات(CIA) را مورد هدف قرار می‌دهند. همان‌طور که در فصل اول توضیح داده شد، مثلث امنیت اطلاعات شامل سه پارامتر محرمانگی(C)، یکپارچگی (I) و دسترس‌پذیری(A) اطلاعات است. در حملات سایبری، مهاجمان و هکرها قصد انجام سه اقدام زیر را با اطلاعات دارند:

- افشا
- تخریب
- انکار

این سه عمل دقیقاً برعکس مثلث CIA هستند و از آن‌ها به عنوان مثلث نفوذگران نام برده می‌شود.

افشاء:

افشاء متضاد محرمانگی است. به‌منظور جلوگیری و کاهش احتمال افشای اطلاعات، سازمان‌ها باید اطلاعات خود را براساس میزان محرمانگی آن، طبقه‌بندی کنند و براساس سطح محرمانگی اطلاعات، از آن محافظت نمایند. به‌عنوان مثال می‌توان اطلاعات را بر این اساس طبقه‌بندی نمود:

- محرمانه: اطلاعاتی که تنها در اختیار کارکنان دارای مجوز ، مدیران ارشد یا اعضای هیئت مدیره سازمان قرار می‌گیرند و افشای آن صدمات قابل توجه و جدی به کسب‌وکار وارد می‌کند. مانند اطلاعات مربوط به مسائل مالی، درآمدها و مشتریان یک سازمان.
- درون سازمانی: اطلاعاتی که با درجه حساسیت پایین‌تر، فقط در اختیار پرسنل سازمان یا افراد خاص قرار می‌گیرند. مانند دستورالعمل‌ها و بخشنامه‌های داخلی یک سازمان.
- عمومی: اطلاعاتی که همگانی هستند و بازگو نمودن آن‌ها برای عموم آزاد است. مانند بخشنامه‌ها و اطلاعیه‌های عمومی سازمان، آگهی برگزاری مناقصات و بروشورهای تبلیغاتی.

لازم است کارکنان از طبقه محرمانگی اطلاعات و نحوه‌ی نگهداری و برخورد با آن آگاه شوند. طبقه‌بندی اطلاعات کمک می‌کند از یک‌سو افراد مراقبت بیشتری در برخورد با اطلاعات محرمانه داشته باشند و از سوی دیگر افشای سهوی اطلاعات کاهش یابد.

برای مثال فرض کنید کارمند یکی از شعب یک بانک، از میزان محرمانه بودن اطلاعات تماس مشتریان بانک آگاه نباشد، در این‌صورت اگر شخصی به بانک مراجعه کرده و از کارمند مذکور تقاضا کند که اطلاعات تماس یکی از مشتریان بانک را به وی بدهد تا او بتواند طلب شخصی خود را از مشتری بانک وصول کند، ممکن است کارمند بدون اینکه از عواقب افشای این اطلاعات باخبر باشد، این اطلاعات را از روی خیرخواهی و دلسوزی در اختیار فرد درخواست کننده قرار دهد و به دنبال آن، مشکلاتی برای مشتری یا بانک ایجاد نماید. حال آنکه اگر کارمند از میزان محرمانگی اطلاعات مشتری و از عواقب افشای این اطلاعات آگاه باشد، هیچ‌گاه این اطلاعات را سهواً در اختیار افراد غیرمجاز قرار نخواهد داد.

تخریب:

تخریب متضاد یکپارچگی است. بعد از اینکه اطلاعات مهم و محرمانه سازمان و میزان حیاتی بودن آن‌ها تعیین شد، قادرید مشخص کنید که اگر اطلاعات دستکاری شوند یا از بین بروند چه اتفاقی می‌افتد. سازمان‌ها باید راهکارهایی برای این‌گونه مشکلات داشته باشند و از خود بپرسند، هکرها و مهاجمان بیشتر تمایل دارند چه اطلاعاتی را نابود کنند یا در آن‌ها تغییراتی ایجاد کنند. این موضوع برای هر سازمانی متفاوت است و الگوی خاصی ندارد.

انکار:

انکار یا منع دسترسی، متضاد دسترس‌پذیری است. حملاتی که باعث از کار افتادن یک سرویس در سازمان می‌شود، حمله از نوع انکار یا منع دسترسی می‌باشد. برای مثال وب سایت یک سازمان در صورتی که مورد این نوع حملات قرار بگیرد، از دسترس خارج خواهد شد. حال تصور کنید که سازمانی که تجارت اصلی آن مبتنی بر فروش آنلاین است، این نوع حملات منجر به ایجاد وقفه در کسب و کار آن سازمان می شود و ضرر زیادی به آن سازمان وارد خواهد نمود.

همچنین یادآوری می‌شود که واژه هک به معنی نفوذ به سیستم‌های رایانه‌ای و دسترسی غیرمجاز به اطلاعات رایانه و یا نفوذ در شبکه با اهداف خرابکارانه‌ای که قبلاً شرح داده شد، اطلاق می‌گردد و شخصی که این کار را انجام می دهد، هکر نامیده می‌شود.

نمونه هایی از حملات سایبری

:

هکرها و مهاجمان از راه‌های زیادی برای هک کردن و حمله و نفوذ به سیستم‌ها و اطلاعات استفاده می‌کنند و مثلث CIA را به مخاطره می‌اندازند. در ادامه، نمونه هایی از متداول‌ترین حملات سایبری بیان می‌گردد.

مهندسی اجتماعی

:

مهندسی اجتماعی به عبارت ساده، سوء استفاده از اطمینان یا فریب عوامل انسانی برای دسترسی به اطلاعات محرمانه است. به عبارتی پروسه‌ای برای فریب دادن کاربران یک سیستم و متقاعد کردن آن‌ها به انجام کارهای پرفایده برای هکر می‌باشد. مثل گرفتن اطلاعاتی از آن‌ها که بتوان در شکستن یا دور زدن مکانیزم امنیتی استفاده کرد. در این روش، فرد مهاجم اعتماد افراد را جلب کرده و زیرکانه فرد را به فاش کردن اطلاعات شخصی یا سازمانی یا انجام کارهایی خاص متقاعد می‌کند. مهاجم در روش مهندسی اجتماعی، به جای استفاده از روش‌های معمول و مستقیم نفوذ (جمع‌آوری اطلاعات و عبور از دیواره آتش برای دسترسی به سیستم‌های سازمان و پایگاه داده‌ها و دارایی‌های اطلاعاتی) از تکنیک فریفتن افرادی که به این اطلاعات دسترسی دارند، برای جمع‌آوری اطلاعات استفاده می‌کند. یک مهندس اجتماعی معمولاً از تلفن یا اینترنت برای فریب افراد استفاده می‌کند.

مثالی ساده از یک مهندسی اجتماعی:

تصور کنید بانکی را که از یک نرم‌افزار سازمانی جهت اتوماسیون اداری و کنترل دارایی خود و مشتریانش استفاده می‌کند. در این نرم‌افزار هیچ‌گونه آسیب پذیری و نقطه ضعفی شناسایی نشده است و شبکه بانک نیز در سطح

مناسب امنیت قرار دارد و هزینه زیادی صرف امنیت سخت‌افزاری و نرم‌افزاری آن شده است. مهاجم برای نفوذ به سیستم بانک امکان دسترسی به روش‌های معمول هک را ندارد یا اصلاً دانش فنی آن را ندارد، امّا در این سازمان کارمندانی مشغول به کار هستند که آموزش لازم در زمینه مهندسی اجتماعی را ندیده‌اند. مهاجم با انجام تحقیقات قبلی، جلب اطمینان و دریافت اطلاعات، به هدف خود نزدیک می شود. مهاجم با خونسردی در تماس با یکی از کارمندان، خود را مسوول شبکه یا مسوول پشتیبانی نرم‌افزار معرفی می‌کند و با اطلاعاتی همچون نام، اطلاعات اولیه واحدها، نوع نرم‌افزار مورد استفاده و موارد مشابه‌ای که قبلاً به‌دست آورده است با یکی از کارمندان تماس تلفنی برقرار می‌کند:

مهاجم: سلام، قهرود هستم مسوول IT. در حال ارتقای نسخه نرم‌افزار X هستیم. لطفاً رمز خود را به Newversion۵ تغییر دهید. ضمناً تا یک ربع وارد سیستم نشوید، چون هر تراکنشی ممکن است باعث اختلال شود.

کارمند: خوب هستید، آقای قهرود؟ الان دارم سند می‌زنم، امکان دارد چند دقیقه دیگر این کار را انجام دهید؟ در ضمن من با USB سیستم هم مشکل دارم.

مهاجم: ما قبلاً به همه واحدها اعلام کرده بودیم امّا اشکالی ندارد، من شما را درک می‌کنم و می‌توانم ارتقای سیستم شما را با ۱۰ دقیقه تأخیر انجام دهم.

کارمند: به بنده اعلام نشده بود. به هر حال ممنونم که همکاری می‌کنید.

مهاجم: خواهش می‌کنم. در خصوص مشکل‌تان هم در فرصت مناسب‌تری با واحد ما تماس بگیرید، نام‌تان را بگویید تا سریع کارتان انجام شود، فرمودید شما آقای؟

کارمند: رسول‌زاده هستم.

مهاجم: پس جناب رسول‌زاده! شما رمزتان را الان تغییر بدهید، بنده هم از ده دقیقه بعد برنامه را ارتقا می‌دهم، راستی نام کاربری‌تان چه بود؟

کارمند: مثل بقیه، نام خانوادگی

به همین آسانی، مهاجم با روش مهندسی اجتماعی، اطلاعات محرمانه بسیار با ارزش سیستم نرم‌افزاری سازمان را از کارمندی که تصور می‌کرد در حال مکالمه با مسوول شبکه سازمان است، دریافت کرد و ممکن است نقشه‌های دیگری مثل نفوذ به سطح بالاتر به روش‌های دیگر یا ایجاد کاربر جدید و غیره نیز داشته باشد، به‌علاوه، اکثر نام‌های کاربری در سیستم نیز در اختیار مهاجم قرار گرفت.

تکنیک‌های مشخص و از پیش تعریف شده‌ای برای مهندسی اجتماعی وجود ندارد و هر بار کلاهبرداران و مهاجمان مهندسی اجتماعی روشی جدید را به کار می‌گیرند که اگر محرمانگی و طبقه‌بندی اطلاعات و آموزش‌های لازم به درستی رعایت شود، تا حدود زیادی جلوی این معضل گرفته خواهد شد.

شکل ۱: به‌دست آوردن اطلاعات به وسیله مهندسی اجتماعی

در ادامه، مثال‌هایی از تکنیک‌های مهندسی اجتماعی آورده شده است:

• مشاهده اطلاعات به صورت پنهانی : در این روش، کلمه عبور و اطلاعات محرمانه از طریق نگاه کردن به دست فرد مثلاً هنگام وارد شدن به سیستم و یا وارد کردن رمز کارت بانکی در پشت دستگاه ATM مشاهده می شود. یک هکر می‌تواند رمز یا کلمه عبور صحیح کاربر را تماشا کند و سپس از آن برای دسترسی به سیستم یا حساب بانکی او استفاده کند.

• استفاده از زباله‌دان (آشغال‌گردی): یک تکنیک برای پیدا کردن اطلاعات نوشته شده بر روی تکه‌های کاغذ یا نتایج چاپی رایانه از طریق جستجو در سطل زباله است. هکرها غالباً کلمات عبور، اسامی فایل‌ها و یا دیگر اطلاعات محرمانه و مهم را از این طریق پیدا می‌کنند. عمدتاً افراد در سازمان‌ها، کاغذهای باطله خود را که حاوی اطلاعات محرمانه و مهم می‌باشد، با مچاله کردن یا تکه‌تکه کردن به داخل سطل زباله می‌اندازند. افراد سودجو و هکرها می‌توانند از طریق آشغال‌گردی و کنار هم قراردادن این تکه‌های کاغذ، به اطلاعات مورد نیاز خود برای نفوذ و انجام حملات سایبری استفاده کنند.

• جعل هویت : روشی است که جاعل از طریق آن وانمود می‌کند یکی از افراد شناخته شده در سازمان است و به کسب اطلاعات از پرسنل می‌پردازد.

• استفاده از ابزارهای ارتباطی : این تکنیک با استفاده از ابزارهای ارتباطی نظیر تماس تلفنی، ارسال پیامک از طریق تلفن همراه و روش‌های مبتنی بر رایانه مانند ارسال پست الکترونیک و فایل‌های ضمیمه شده به آن و با عناوین مختلفی نظیر هشدار برای جلوگیری از انتشار یک بدافزار، برنده شدن در قرعه‌کشی، ارایه هدایای رایگان و... صورت می‌گیرد که از این روش، اطلاعات از جمله اطلاعات کارت یا حساب‌های بانکی کاربران درخواست می‌شود. گاهی این روش‌ها منجر به اقدامی جهت انتقال وجه توسط شخص مورد هدف قرار داده شده نیز می گردد.

روش‌های مهندسی اجتماعی بسیار متنوع هستند و محدود به موارد فوق نمی‌شوند و به دلیل این‌که سخت تشخیص داده می‌شوند، همچنین نبود روش‌های خاص اعم از نرم‌افزاری یا سخت‌افزاری ویژه جهت تشخیص و مقابله با آن، تنوع سناریوها و ناآگاهی افراد از اهمیت اطلاعات و امکان سوء استفاده از آن، معمولاً متداول می‌شود و مورد بهره‌جویی سوء استفاده‌کنندگان قرار می‌گیرد.

حملات فیشینگ

:

حملات فیشینگ هم یک نوع مهندسی اجتماعی محسوب می‌شود که در فضای اینترنت اتفاق می‌افتد. در این نوع حمله، کاربر از روش‌های مختلف به وب سایت‌های جعلی و عموماً برای کسب منافع مالی هدایت می گردد. عمدتاً ایمیلی از سوی هکر برای فرد ارسال می‌شود و هکر خود را به عنوان بانک یا دیگر سازمان‌های مالی معرفی می‌کند و اطلاعات بانکی فرد مورد حمله را درخواست می‌نماید. در درخواست‌هایی که دریافت‌کننده، به درخواست هکر پاسخ می دهد، باعث موفقیت هکر و دستیابی او به اطلاعات محرمانه می‌شود. مراحل به این ترتیب است که کاربر بر روی لینک داخل ایمیل کلیک کرده و به صفحه وب‌سایت جعلی هدایت می گردد و بر طبق درخواست هکر که خود را بانک یا هویت دیگری معرفی کرده است، فرد قربانی اطلاعات و رمزهای عبور خود را وارد می‌کند که از این طریق، هکر قادر خواهد بود اطلاعات بانکی قربانی را به‌دست آورده و از آن به منظور کسب منافع مالی استفاده کند. این حمله‌ها افراد معمولی را طعمه خود قرار می‌دهند تا به اطلاعات حساب بانکی و دیگر اطلاعات محرمانه آن‌ها به منظور هک کردن، دسترسی پیدا کنند. از تکنیک‌های متداول دیگر این نوع حملات راه‌اندازی وب‌سایت‌های جعلی مشابه با وب‌سایت‌های پرکاربرد و پربازدید کننده مثل وب‌سایت‌های خرید اینترنتی، درگاه‌های پرداخت و یا وب‌سایت بانکداری اینترنتی به قصد اخذ اطلاعات بانکی و محرمانه افراد است، این وب‌سایت‌ها از نظر ظاهری و نشانی اینترنتی با تغییرات جزئی بسیار شبیه به وب‌سایت اصلی بوده و کاربر را دچار اشتباه و سوء استفاده می‌نمایند.

اخذ اطلاعات از طریق کلیدنگار

:

کلید نگارها یا «ابزارهای سرقت کلمه»، عموماً با واژه Key Logger شناخته شده و بیان می‌گردند. این ابزارها، دارای

انـواع سـخت‌افزاری و نرم‌افـزاری هسـتند کـه کاربـرد آن ثبـت کلیـه کلیدهـای فـشرده شـده کاربـر بـر روی صفحـه کلیـد رایانـه می‌باشـد. بدیهـی اسـت از ایـن طریـق، اطلاعـات محرمانـه و حسـاس نظیـر کدهـای کاربـری و رمزهـای عبـور سـامانه‌های مـورد اسـتفاده در کسـب‌وکار یـا اطلاعـات بانکـی فـرد قربانـی، افشـاء می‌گـردد. بـا توجـه بـه عملکـرد Key Loggerهـا، بـه آن‌هـا واقعه‌نـگار هـم گفتـه می‌شـود. Key Loggerهـا معمـولاً بـه صـورت یـک سـخت‌افزار کوچـک در بخشـی از رایانه(مثـلاً در پـورت صفحـه کلیـد) و یـا نـرم افـزار ناشـناس و مخفی(کـه بـه روشـی روی رایانـه نصـب شـده اسـت)، اطلاعـات کاربـر را سرقـت می‌نماینـد. ایـن ابزارهـا نیـز ماننـد سـایر فن‌آوری‌هـا پیشرفـت کـرده و می‌تواننـد ضمـن ثبـت انـواع اطلاعـات نظیـر صـدا و یـا محتـوای تصویـری عـلاوه بـر ثبـت اطلاعـات صفحـه کلیـد، اطلاعـات ذخیـره شـده را از طریـق دسترسـی اینترنتـی رایانه بـرای مهاجـم ارسـال کننـد.

انـواع حمـلات سـایبری محـدود بـه مـوارد فـوق نیسـتند امـا روش‌هـای ذکـر شـده از عمـده مـواردی هسـتند کـه کاربـران عـادی و فاقـد دانـش و آگاهـی کافـی را مـورد هـدف و سـوء اسـتفاده قـرار می‌دهنـد. همچنیـن موضوعـات دیگـر ایـن حـوزه نظیـر بدافزارهـا در ادامـه مباحـث تشریـح خواهنـد شـد.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- با مفهوم شبکه‌های رایانه‌ای و فضای سایبری آشنا شدید.	
۲- با مفهوم هک و حملات سایبری آشنا شدید.	
۳- با انواعی از تکنیک‌های هک و حملات سایبری آشنا شدید.	

خودآزمایی جلسه پنجم :

۱. کدام‌یک از موارد زیر، متضاد مفهوم یکپارچگی اطلاعات می‌باشد؟
الف) افشا ب) منع دسترسی ج) تخریب د) انکار

۲. حمله‌ای که توسط آن، با ارسال ایمیل و جعل صفحات اینترنتی، هکر به اطلاعات بانکی فرد مورد حمله دست می‌یابد، چه می‌گویند؟
الف) آشغال‌گردی ب) شولدر سرفینگ ج) جعل د) فیشینگ

۳. حملاتی که باعث از کار افتادن یک سرویس در سازمان می‌شود ، چه نامیده می شود؟
الف) انکار
ب) تخریب
ج) افشا
د) نفوذ

۴. کدام گزینه در مورد مهندسی اجتماعی صحیح نمی‌باشد؟
الف) مهندسی اجتماعی پروسه فریب دادن کاربران یک سیستم و متقاعد کردن آنها به انجام کارهای پرفایده برای هکر است.
ب) مهاجم در روش مهندسی اجتماعی، به جای استفاده از روش‌های معمول و مستقیم نفوذ از تکنیک فریفتن افرادی که به این اطلاعات دسترسی دارند، برای جمع‌آوری اطلاعات استفاده می‌کند.
ج) روشی که جاعل از طریق آن وانمود می‌کند یکی از افراد شناخته شده در سازمان است و به کسب اطلاعات از پرسنل می‌پردازد، نوعی مهندسی اجتماعی است.
د) پیدا کردن اطلاعات نوشته شده بر روی تکه‌های کاغذ یا نتایج چاپی رایانه از طریق جستجو در سطل زباله، مهندسی اجتماعی محسوب نمی‌گردد.

پاسخ‌نامه تشریحی

خودآزمایی جلسه پنجم

۱. پاسخ صحیح، گزینه «ج»
تخریب متضاد یکپارچگی است.

۲. پاسخ صحیح، گزینه «د»
حمله‌ای که توسط آن، با ارسال ایمیل و جعل صفحات اینترنتی، هکر به اطلاعات بانکی فرد مورد حمله دست می‌یابد، فیشینگ می‌گویند.

۳. پاسخ صحیح، گزینه «الف»
حملاتی که باعث از کار افتادن یک سرویس در سازمان می‌شود، حمله از نوع انکار یا منع دسترسی می‌باشد.

۴. پاسخ صحیح، گزینه «د»
پیدا کردن اطلاعات نوشته شده بر روی تکه‌های کاغذ یا نتایج چاپی رایانه از طریق جستجو در سطل زباله، نوعی مهندسی اجتماعی با عنوان "استفاده از زباله‌دان" است.

جلسه ششم

انواع بدافزارها

۱۲۳	اهداف یادگیری
۱۲۴	پیش‌آزمون
۱۲۶	نسبت‌های فعالیت
۱۲۶	نسبت‌های موجودی
۱۲۹	نسبت‌های حساب‌های دریافتنی
۱۳۱	دورهٔ گردش عملیات شرکت
۱۳۲	نسبت گردش دارایی‌ها
۱۳۳	نسبت حساب‌های پرداختنی
۱۳۵	میزان دستیابی به اهداف یادگیری
۱۳۶	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با مفهوم بدافزار و عملکرد آن‌ها آشنا شود.
۲. انواع بدافزارها و عملکرد آن‌ها را بشناسد.
۳. اهمیت عملکرد و نفوذ بدافزارها را دریابد.

پیش‌آزمون جلسه ششم :

۱. هر نوع کد نرم‌افزاری که بر روی سیستم شما قرار بگیرد و عملیاتی ناخواسته را انجام دهد، به عنوان ..... شناخته می‌شود؟

الف) ویروس ب) کرم ج) بدافزار د) جاسوس

۲. به نظر شما کدامیک از بدافزارهای زیر قابلیت تکثیر شدن دارند؟

الف) ویروس ب) باج‌گیر ج) کرم د) گزینه الف و ج

پاسخ‌نامه

پیش‌آزمون جلسه ششم

:

	الف	ب	ج	د
۱				
۲				

انواع بدافزارها

:

بدافـزار یـک اصطـلاح فراگیـر و جامـع اسـت و بـه هـر برنامـه نرم‌افـزاری اطـلاق می‌شـود کـه بـرای انجـام اعـمال غیرمجـاز و گاهـی مـضر ایجـاد شـده اسـت. ویروس‌هـا، برنامه‌هـای سـارق کلمـه عبـور، بدافـزار جاسوسـی و بدافـزار تبلیغاتـی نمونه‌هایـی از بدافزارهـا هسـتند. در واقـع تمامـی مـوارد ذکـر شـده، کدهـای مخربـی هسـتند کـه در رده بدافزارهـا طبقه‌بنـدی می‌شـوند، بـه صـورت کلـی هـر نـوع کـد نرم‌افـزاری کـه بـر روی سیسـتم شـما قـرار بگیـرد و عملیاتـی ناخواسـته را انجـام دهـد، بـه عنـوان بدافـزار شـناخته می‌شـود. معمـولاً وجـود بدافـزار را یـک آلودگـی رایانـه‌ای می‌نامنـد.

یـک نرم‌افـزار بـر پایـه نیـت سـازنده و عملکـرد آن بـه عنـوان یـک بدافـزار شـناخته می‌شـود. بدافزارهـا عملکردهـای مختلفـی دارنـد، برخـی از بدافزارهـا فقـط کاربـر را آزار می‌دهنـد، مثـلاً او را مجبـور بـه انجـام کاری تکـراری می‌کننـد. امـا برخـی دیگـر سیسـتم رایانـه‌ای و داده‌هـا را مـورد هـدف قـرار می‌دهنـد کـه ممکـن اسـت خسـاراتی بـه بـار آورنـد. مهم‌تریـن پـل ارتباطـی بدافزارهـا بیـن تولیدکننـدگان آن‌هـا و کاربـران، اینترنـت اسـت. گاهـی در روش هـای پیشرفتـه و مدیریـت شـده، بدافزارهـا بـا اهـداف مشـخص تولیـد و بـا قـرار گرفـتن بـر روی رایانـه هـای هـدف، رایانـه یـا شـبکه رایانـه ای یـک سـازمان را تحـت کنـترل قـرار داده و اقـدام بـه سرقـت اطلاعـات و یـا فعالیـت هـای خرابکارانـه می‌نماینـد. بـه عبـارت دیگـر بـد افزارهـا بـه مـرور زمـان هدفمنـد و به‌عنـوان ابزارهـای اخـاذی، سرقـت اطلاعـات و خرابـکاری مـورد بهـره بـرداری قـرار مـی گیرنـد.

بدافزارها براساس نوع عملکرد دسته بندی می شوند، که در ادامه به صورت اجمالی معرفی می گردند:

• ویـروس و کـرم بدافزارهایـی هسـتند کـه خـود را در فایل‌هـای سـالم کپـی و از ایـن طریـق سیسـتم شـما را آلـوده و در واقـع خـود را تکثیـر مي‌کننـد. دقیقـاً مشـابه رفتـار ویروس‌هـا در دنیـای موجـودات زنـده کـه بـا آلـوده کـردن سـلول‌های بیولوژیـک، خـود را تکثیـر کـرده و سیسـتم بـدن انسـان یـا حیـوان را آلـوده می‌کننـد. ویروس‌هـا می‌تواننـد عملکردهـای متفاوتـی داشـته باشـند. در پشـت صحنـه منتظـر بماننـد و کلمـات عبـور شـما را بدزدنـد، تبلیغـات و صفحـات ناخواسـته را بـرای شـما بـه نمایـش درآورنـد، سیسـتم شـما را خامـوش و روشـن کننـد، فایل‌هـای روی سیسـتم شـما را ناپدیـد کننـد، یـک فایـل را تکثیـر کننـد یـا بـه سـادگی منجـر بـه تخریـب سیسـتم شـما و از کار افتـادن برخـی سـخت‌افزارها شـوند. امـا عامـل اساسـی کـه یـک ویـروس را می‌سـازد روشـی اسـت کـه خـود را به‌وسـیله آن تکثیـر می‌کنـد. ویروس‌هـا بـراي آلـوده کـردن رایانه‌هـا نیـاز بـه اجـرا شـدن توسـط کاربـر یـا یـك برنامـه دارنـد. وقتـی بـه اشـتباه یـا بـدون اطـلاع یـک ویـروس را بـر روی سیسـتم خـود اجـرا می‌کنیـد، ایـن ویـروس برنامه‌هـای موجـود بـر روی سیسـتم شـما را آلـوده می‌کنـد. زمانـی کـه برنامه‌هـا یـا فایل‌هـای آلـوده را بـه رایانـه دیگـری منتقـل و اجـرا می‌کنیـد، همیـن اتفـاق بـرای رایانـه جدیـد رخ می‌دهـد. فلـش مموری‌هـا یکـی از مهم‌تریـن ابزارهـا بـرای انتقـال ویروس‌هـا می‌باشـند. برخـلاف ویروس‌هـا، کرم‌هـا بدافزارهایـی هسـتند کـه بـه طـور مسـتقل تکثیـر و اجـرا می‌گردنـد.

• کلیدنگارهـا و جاسـوس افزارهـا نـوع دیگـری از بدافزارهـا هسـتند کـه عملکـرد اصلـی آن‌هـا سرقـت اطلاعـات اسـت. Key Loggerهـا و جاسـوس‌افزارها برنامه‌هایـی هسـتند کـه بـا قـرار گرفـتن در حافظـه سیسـتم، از کلیدهـای زده شـده توسـط کاربـر گـزارش گرفتـه و آن را در قالـب یـک فایـل بـرای نفوذگـر می‌فرسـتند. . ایـن نـوع بدافزارهـا هرگونـه اطلاعاتـی را می‌تواننـد جمـع‌آوری کننـد. ایـن اطلاعـات می‌توانـد بـه اطلاعـات شـخصی کاربـر ماننـد گشـت‌وگذارهای اینترنتـی و یـا مشـخصات حسـاب‌های مختلـف ماننـد حسـاب‌های کاربـری سـامانه‌های مختلـف، بانکـداری اینترنتـی، پسـت الکترونیـک و کلـمات عبـور آن‌هـا، رمـز کارت‌هـای بانکـی و سـایر اطلاعـات حسـاس باشـد. عـلاوه بـر ایـن، می‌تواننـد در کنـترل رایانـه توسـط کاربـر اختـلال ایجـاد کننـد یـا کاربـر را بـه بازدیـد از یـک صفحـه خـاص اینترنتـی مجبـور کننـد و یـا اینکـه بـا تغییـر تنظیـمات، باعـث کاهـش سرعـت اینترنـت شـوند و یـا امـکان دسترسـی غیرمجـاز بـه رایانـه را پیـدا کننـد. سـپس ایـن اطلاعـات جمـع آوری شـده در یـک رایانـه Server بارگـذاری شـده و مهاجـمان و افـراد سـودجو قـادر خواهنـد بـود بـا تحلیـل آن‌هـا نسـبت بـه دریافـت و فاش‌سـازی کلـمات عبـور و اطلاعـات بانکـی و محرمانـه اقـدام کننـد.

• درب‌هـای پشـتی نـوع دیگـری از بدافزارهـا هسـتند کـه عملکـرد تخریبـی دارنـد و نفوذگرهـا به‌وسـیله آن‌هـا می‌تواننـد سیسـتم‌های آلـوده شـده کاربـر را بـه کنـترل خـود در آورنـد. درب‌هـای پشـتی درون شـبکه قابلیـت تکثیـر ندارنـد امـا در صـورت آلـوده شـدن رایانـه کاربـر بـه ایـن بدافـزار، ممکـن اسـت نفوذگـر بـه سـایر سیسـتم‌های اطلاعاتـی سـازمان دسترسـی پیـدا کنـد و عـلاوه بـر سرقـت اطلاعـات، باعـث مختـل شـدن سرویس‌هـای تحـت شـبکه سـازمان شـود. بـه عبـارت دیگـر، درب‌هـای پشـتی، بدافـزار مخربـی اسـت کـه بـه هکـر بـرای اتصـال بـه بخش‌هـای آلـوده شـده سیسـتم هـدف اجـازه می‌دهـد و در نهایـت رایانـه هـدف را تحـت مدیریـت خویـش قـرار می‌دهـد.

• باج‌افزارهـا نیـز نوعـی بدافـزار هسـتند کـه بـا اسـتفاده از الگوریتـم هـای رمزنـگاری پیچیـده، دسترسـی بـه فایل‌هـا را محـدود نمـوده و بـه عبارتـی آن‌هـا را گـروگان می‌گیرنـد و در ازای آزادسـازی اطلاعـات رایانـه از کاربـر، تقاضـای پرداخـت مبلغـی

مشخص (باج) می‌نمایند. عموماً نحوه پرداخت مبالغ درخواست شده از طریق پول های الکترونیک غیر قابل ردیابی متداول نظیر بیت کوین انجام می گردد.

برخی از انواع این بدافزار به سادگی با نمایش یک تصویر حاوی پیام روی صفحه نمایش رایانه، به نحوی که کاربر قادر به بستن و یا بازکردن پنجره دیگری نباشد، از او می‌خواهند که برای ادامه کار سیستم‌عامل، اقدام به واریز مبلغی خاص کند. اما نمونه‌های فوق‌العاده خطرناک آن اقدام به کد کردن و رمزگذاری فایل‌های کاربران است که از آن‌ها می‌خواهند برای دسترسی به این فایل‌ها مبلغی را پرداخت کنند. اگرچه همیشه پرداخت وجه تضمینی به بازگشت اطلاعات به وضعیت اولیه نیست.

این روزها بسیاری از بدافزارها به قصد درآمدزایی تولید می‌شوند و باج‌افزارها نمونه‌ای هوشمند و خوب از آن‌ها به شمار می‌روند. این نمونه بدافزار به سیستم شما آسیب نمی‌رساند، بلکه فقط برای کاربر دردسر ایجاد می‌کند. روش این بدافزار گروگان‌گیری و گروکشی سیستم و فایل‌های کاربر برای کسب درآمد است. به مرور زمان بدافزارهای از نوع باج‌افزار درحال افزایش چشم‌گیر بوده و ضمن پیچیده‌تر شدن عملکردشان، هدفمندتر و با نشانه‌گیری شرکت‌ها و سازمان‌های کوچک و بزرگ، مراکز درمانی و آموزشی و موسسات مالی و بانکی تولید و انتشار می‌یابند. با توجه به آنچه که گفته شد، با پیچیده شدن حملات سایبری و به روز شدن انواع بدافزارها، اکثر بدافزارها دارای خصلت رفتاری متشکل از خصوصیات مخرب تعدادی از بدافزارها هستند. برای مثال، ویروس الزاماً فقط یک ویروس نیست و می‌تواند علاوه بر خصوصیات مخرب یک ویروس، حاوی خصوصیات درب پشتی و Key Logger نیز باشد. به عبارت دیگر، یک بدافزار نسل نوین، دارای عملکرد مخرب مجموعه‌ای از خانواده بدافزارهای نام برده شده را هستند.

از راه های متداول انتشار بدافزارها به ویژه باج افزارها اجرای فایل های پیوست مخرب پست الکترونیک ناشناس و هرزنامه ها (spam) ، و دانلود از طریق لینک‌های دسترسی در وب‌سایت‌های اینترنتی و پست الکترونیک های ناشناس می باشد. گردانندگان این حملات، مرتباً، در حال تغییر ساختار فایل های مخرب هستند تا از شناسایی توسط ابزارهای ضدبدافزار در امان باقی بمانند.

میزان دستیابی به اهداف یادگیری

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید،
در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱. با مفهوم بدافزارها و عملکرد آن ها آشنا شدید.	
۲. انواع بدافزارها و عملکرد آن ها را می شناسید.	
۳. اهمیت عملکرد و نفوذ بدافزارها را می دانید.	

خودآزمایی جلسه ششم :

۱. کدامیک از موارد ذیل از خصوصیات باج افزارها نیست؟

الف) اخاذی　　ب) ایجاد اختلال　　ج) رمزگذاری اطلاعات　　د) تخریب سیستم

۲. عملکرد کدامیک از بدافزارهای زیر، سرقت اطلاعات است؟

الف) ویروس　　ب) کی لاگر　　ج) باج افزار　　د) درب پشتی

۳. کدامیک از بدافزارهای زیر می‌تواند اطلاعات کاربران را رمز کند و از کاربر بخواهد برای دسترسی به این اطلاعاتش مبلغی را پرداخت نماید؟

الف) جاسوس افزار　　ب) باج‌افزار　　ج) کرم　　د) درب پشتی

۴. کدامیک از بدافزارهای زیر عملکرد تخریبی دارند و نفوذگرها به‌وسیله آن‌ها می‌توانند سیستم‌های آلوده شده کاربر را به کنترل خود در آورند؟

الف) جاسوس افزار　　ب) باج افزار　　ج) ویروس　　د) درب پشتی

پاسخ‌نامه تشریحی

خودآزمایی جلسه ششم

:

۱. پاسخ صحیح، گزینه «د»

باج افزارها معمولاً به سیستم آسیبی نمی‌رسانند بلکه با رمزگذاری اطلاعات موجب اختلال شده و با درخواست وجه اخاذی می‌نمایند.

۲. پاسخ صحیح، گزینه «ب»

کی لاگرها نوعی بدافزار هستند که عملکرد اصلی آن‌ها سرقت اطلاعات است.

۳. پاسخ صحیح، گزینه «ب»

برخی از باج‌افزارها به سادگی با نمایش یک پیام کوچک از شما می‌خواهند که برای ادامه کار سیستم‌عامل اقدام به واریز مبلغی خاص کنید. اما نمونه‌های فوق‌العاده خطرناک آن اقدام به کد کردن و رمزگذاری فایل‌های کاربر می‌کنند و از او می‌خواهند که برای دسترسی به این فایل‌ها مبلغی را پرداخت کنند.

۴. پاسخ صحیح، گزینه «د»

درب‌های پشتی نوع دیگری از بدافزارها هستند که عملکرد تخریبی دارند و نفوذگرها به‌وسیله آن‌ها می‌توانند سیستم‌های آلوده شده کاربر را به کنترل خود در آورند.

خلاصه فصل سوم

جلسه هشتم

شبکه رایانه‌ای که اغلب به طور خلاصه به آن شبکه گفته می‌شود، گروهی از رایانه‌ها و دستگاه‌هایی است که توسط کانال‌های ارتباطی به هم متصل شده‌اند. امروزه به هر شبکه رایانه‌ای که متشکل از کاربران، اطلاعات، نرم‌افزار و سخت‌افزار باشد، فضای سایبری گفته می‌شود. شبکه اینترنت و اینترانت نمونه‌ای از فضای سایبری می‌باشند.

امروزه فضای سایبری به مکانی ایده‌آل برای حملات سایبری توسط هکرها و سایر مهاجمان تبدیل شده است. هدف از حملات سایبری، دستیابی به اطلاعات افراد، سازمان‌ها ، ایجاد وقفه در کسب‌وکار و یا ایجاد خدشه و آسیب رساندن به زیرساخت‌های آن‌ها می‌باشد.

حملات سایبری معمولاً یک یا چندین ضلع از مثلث امنیت اطلاعات (CIA) را مورد هدف قرار می‌دهند. در حملات سایبری، مهاجمان و هکرها قصد انجام سه اقدام افشا، تخریب و انکار یا منع دسترسی را با اطلاعات دارند.

هکرها و مهاجمان از راه‌های زیادی برای هک کردن و حمله و نفوذ به سیستم‌ها و اطلاعات استفاده می‌کنند و مثلث CIA را به مخاطره می‌اندازند. مهندسی اجتماعی نمونه ای از یک حمله سایبری می‌باشد. مهاجم در روش مهندسی اجتماعی، به جای استفاده از روش‌های معمول و مستقیم نفوذ، از تکنیک فریفتن و جلب اعتماد افرادی که به این اطلاعات دسترسی دارند، برای جمع‌آوری اطلاعات استفاده می‌کند. آشغال‌گردی و مشاهده پنهانی اطلاعات نمونه‌هایی از تکنیک‌های مهندسی اجتماعی می‌باشند.

حملات فیشینگ هم یک نوع مهندسی اجتماعی محسوب می‌شود که در فضای اینترنت اتفاق می‌افتد. در این نوع حمله، عمدتاً از طریق پست الکترونیک، نامه ای از سوی هکر برای فرد ارسال می‌شود و هکر خود را به عنوان بانک، یا دیگر سازمان‌های مالی جا می‌زند و اطلاعات بانکی فرد مورد حمله را درخواست می‌نماید.

جلسه نهم

بدافزار یک اصطلاح فراگیر و جامع است و به هر برنامه نرم‌افزاری اطلاق می‌شود که برای انجام اعمال غیرمجاز و گاهاً مضر ایجاد شده است. به صورت کلی هر نوع کد نرم‌افزاری که بر روی سیستم قرار بگیرد و عملیاتی ناخواسته را انجام دهد، به عنوان بدافزار شناخته می‌شود.

بدافزارهای زیادی وجود دارند که هر کدام عملکرد متفاوتی دارند. ویروس و کرم، بدافزارهایی هستند که خود را در فایل‌های سالم کپی کرده، از این طریق سیستم شما را آلوده می‌کند و در واقع خود را تکثیر می‌کنند.

Key Loggerها و جاسوس‌افزارها نوع دیگری از بدافزارها هستند که عملکرد اصلی آن‌ها سرقت اطلاعات است. Key Loggerها و جاسوس‌افزارها برنامه‌هایی هستند که با قرار گرفتن در حافظه سیستم، از کلیدهای زده شده توسط کاربر گزارش گرفته و آن را در قالب یک فایل برای نفوذگر می‌فرستند. درب‌های پشتی نیز نوعی بدافزار هستند که عملکرد تخریبی دارند و نفوذگرها به‌وسیله آن‌ها می‌توانند سیستم‌های آلوده شده کاربر را به کنترل خود درآورند. باج‌افزارها نیز نوعی بدافزار هستند که روش عملکرد آن‌ها رمزگذاری فایل‌ها و تقاضای پرداخت پول در ازای اطلاعات گروگان گرفته شده می باشد.

فصل اول: آشنایی با مفاهیم امنیت اطلاعات

فصل دوم: امنیت فیزیکی و محیطی

فصل سوم: تهدیدات امنیتی در شبکه های رایانه‌ای

فصل چهارم

امن سازی در مقابله با تهدیدات امنیتی

جلسه هفتم:
ارتقای امنیت رایانه ها

جلسه هشتم:
ارتقای امنیت در استفاده از سامانه ها و اینترنت

جلسه نهم:
سیاست میز کار پاک و صفحه نمایش پاک

فصل پنجم:
امنیت تجهیزات قابل حمل

فصل ششم:
توصیه های امنیتی در خدمات بانکی

فصل هفتم:
جرایم رایانه‌ای و تعهدنامه عدم افشای اطلاعات

فصل هشتم:
پیاده سازی امنیت در سازمان ها

جلسه هفتم

ارتقای امنیت رایانه ها

۱۴۱	اهداف یادگیری
۱۴۲	پیش آزمون
۱۴۴	اهمیت به روزرسانی رایانه، نرم افزارها و سامانه ها
۱۴۸	سیستم عامل ها و برنامه های کاربردی
۱۴۹	اهمیت به روزرسانی و ارتقای سیستم عامل ها و برنامه های کاربردی
۱۴۹	نرم افزار ضد بدافزار و به روزرسانی آن
۱۵۰	تهیه نسخه پشتیبان
۱۵۱	میزان دستیابی به اهداف آموزشی
۱۵۴	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. ضرورت حفظ امنیت رایانهها و سامانهها را دریابد.
۲. با تعریف سیستم‌عامل و برنامه‌های کاربردی و اهمیت به‌روزرسانی آنها آشنا شود.
۳. با راهکارهای محافظت در برابر انواع بدافزارها آشنا شود.
۴. اهمیت تهیه نسخه پشتیبان از اطلاعات را دریابد.

پیش‌آزمون جلسه هفتم :

۱. ..... نرم‌افزاری است که مدیریت منابع رایانه را برعهده گرفته و بستری را برای اجرا و بهره‌گیری از برنامه‌های کاربردی فراهم می‌کند

الف) سخت‌افزار ب) سیستم عامل ج) نرم‌افزار کاربردی د) هارد

۲. کدام گزینه جزو برنامه‌های کاربردی نیست؟

الف) مجموعه برنامه‌های Office ب) نرم‌افزار اتوماسیون اداری ج) مرورگر فایرفاکس د) سیستم عامل

۳. کدامیک از روش‌های زیر باعث آلودگی سیستم به بدافزارها می‌شود؟

الف) استفاده از USB آلوده

ب) کلیک بر روی لینک‌های ناشناس موجود در سایت‌های نامعتبر

ج) بازدید از سایت‌های مشکوک و ناشناس

د) همه موارد

۴. ..... نرم‌افزاری است که برای مقابله با فعالیتهای مخرب ویروس‌ها و بدافزارها استفاده می‌شود.

الف) ضدویروس ب) ضد اسپم ج) برنامه کاربردی د) سیستم‌عامل

پاسخ‌نامه

پیش‌آزمون جلسه هفتم :

	الف	ب	ج	د
۱				
۲				
۳				
۴				

اهمیت به‌روزرسانی رایانه ، نرم‌افزارها و سامانه ها

:

همانطور که در فصل پیشین بیان شد، فضای سایبری با توجه به داراییهای اطلاعاتی موجود در آن، همواره مورد توجه سوءاستفادهکنندگان قرار دارد. بنابراین، کاربران و استفادهکنندگان از این فضا برای محافظت از داراییهای اطلاعاتی خود، باید اقدامات و نکات امنیتی لازم را در سطوح مختلف مورد توجه مستمر و همیشگی قرار دهند. این اقدامات و ملاحظات امنیتی معمولاً در مورد رایانهها، نرمافزارهای کاربردی، سامانههای مورد استفاده برای کاربردهای شخصی و یا در حیطه کسب وکار از جمله سامانههای بانکی می باشد. همچنین رعایت برخی از نکات و ملاحظات امنیتی مرتبط نیز در مصون ماندن در برابر مخاطرات دارای اهمیت است. در این فصل در نظر داریم در مورد راهکارهایی که کاربران را در ارتقای سطح امنیت تجهیزات و سامانههای مورد استفاده یاری میرساند صحبت کنیم. البته بهتر است بدانید، راهکارهای امنیتی بسته به تکنولوژی و حیطه‌های کسب وکاری مختلف بسیار متنوع و متفاوت می‌باشند، که باید توسط صاحبان کسب وکار مورد توجه قرار بگیرند. آنچه در این فصل بیان می‌شود، حداقلهایی است که هر کاربر در محدوده کارهای روزمره و شخصی خود و یا در نقش پرسنل یک سازمان باید به آن توجه کند.

سیستم‌عامل‌ها و برنامه‌های کاربردی

:

سیستم‌عامل (OS)، نرم‌افزاری است که مدیریت منابع رایانه را برعهده گرفته و بستری را برای اجرا و بهره‌گیری از برنامه‌های کاربردی فراهم می‌کند. منظور از برنامه کاربردی، نرم‌افزاری است که با استفاده مستقیم از منابع و قابلیت‌های رایانه، کاری را مستقیماً برای کاربر انجام می‌دهد. به‌عنوان مثال: نرم‌افزار اتوماسیون اداری، نرم‌افزار مرورگر فایرفاکس، نرم‌افزار نوشتاری Microsoft Word، نمونه‌هایی از برنامه‌های کاربردی هستند. به عبارت دیگر، سیستم عامل وظیفه ایجاد ارتباط بین سخت‌افزار، برنامه‌های کاربردی و کاربر را دارد. همچنین علاوه بر نقش رابط کاربری، وظیفه مدیریت منابع سخت‌افزاری و نرم‌افزارهای کاربردی برعهده سیستم عامل است.

سیستم عامل‌ها در دو نوع سرویس‌گیرنده (یا نسخه کاربری) و سرویس‌دهنده وجود دارند که عمدتاً کاربران عادی برای انجام امور رایانه‌ای شخصی خود از نسخه سرویس‌گیرنده و سازمان‌ها و تولیدکنندگان یک خدمت یا محصول برای انجام امور از نسخه سرویس‌دهنده استفاده می‌کنند. از آنجایی که معمولاً استفاده از محصولات سیستم‌عامل شرکت مایکروسافت گسترش بیشتری داشته است، مثال‌هایی از انواع نسخه‌های موجود سیستم‌عامل‌های شرکت مایکروسافت در جدول زیر آورده شده است:

نمونه نسخه های سیستم عامل مایکروسافت	
نسخه‌های سیستم عامل سرویس‌دهنده	نسخه‌های سیستم عامل سرویس‌گیرنده
Windows Server 2008	Windows 7
Windows Server 2012	Windows 8
Windows Server 2016	Windows 10

جدول۱: نسخه‌های سیستم عامل مایکروسافت

اهمیت به‌روزرسانی و ارتقای سیستم‌عامل‌ها و برنامه‌های کاربردی

:

در سیستم‌عامل و برنامه‌های کاربردی، گاه‌به‌گاه نقص و نقاط آسیب‌پذیری شناسایی می‌شود که از طریق

آن‌ها هکرها امکان نفوذ و سوءاستفاده از دارایی‌های اطلاعاتی روی رایانه را خواهند داشت و یا بدافزارهایی تولید می‌شوند که از طریق حفره‌های امنیتی موجود روی سیستم‌عامل و نرم‌افزارها، رایانه را دچار آلودگی می‌کنند. عموماً وجود نرم‌افزار ضدویروس برای پوشش این نقص‌ها کافی نیست و شرکت‌های تولید کننده محصولات با ارائه نسخه‌های به‌روزرسانی در بازه‌های زمانی مختلف، برای رفع و ترمیم نقاط ضعف شناسایی شده محصولات خود اقدام می‌کنند. بنابراین، به‌روزرسانی زمان‌بندی‌شده و مستمر سیستم عامل و برنامه‌های کاربردی مورد استفاده در رایانه، برای افزایش سطح امنیت سیستم از اهمیت ویژه‌ای برخوردار است. به بسته‌های به‌روزرسانی که معمولاً آخرین حفره‌های امنیتی و نقاط آسیب پذیر نرم‌افزارها را پوشش می‌دهند وصله های امنیتی گفته می‌شود. این وصله‌های به‌روزرسانی که بر اساس محتوا طبقه‌بندی می‌گردند، دو کاربرد کلی ترمیم نقاط ضعف امنیتی شناسایی شده و یا بهبود و ارتقای امکانات و توانمندی‌های سیستم‌عامل یا نرم‌افزار را برعهده دارند. به طور معمول به‌روزرسانی، برای رفع مشکلات امنیتی و آسیب‌پذیری‌های شناسایی شده الزامی و حیاتی و به منظور استفاده از توانمندی‌های غیر امنیتی، اختیاری است. لازم به توضیح است که بیشتر تولیدکنندگان محصولات نرم‌افزاری برای سهولت در به‌روزرسانی محصولات خود امکاناتی را فراهم می‌کنند که دریافت و نصب فایل‌های به‌روزرسانی جدید، به صورت خودکار انجام شود. به این ترتیب کاربران با استفاده از این تنظیمات و با دسترسی به اینترنت، نسبت به موضوع به‌روزرسانی نگرانی نخواهند داشت.

البته در مورد رایانه‌های مستقر در سازمان‌ها و شبکه‌های بزرگ روش به‌روزرسانی متفاوت است. در سازمان‌های بزرگ به دلیل ملاحظاتی نظیر تعداد زیاد رایانه‌ها، جلوگیری از ترافیک زیاد در شبکه ارتباطی، سیاست‌های محدودیت دسترسی به اینترنت، ضرورت سازگاری سامانه‌ها و سرویس‌ها با نسخ به‌روزرسانی جدید و همچنین تطابق با سیاست‌های سازمان، از روش‌های به‌روزرسانی متمرکز استفاده می‌شود. روش‌ها و محصولات مختلفی برای مدیریت و نصب نسخه‌های به‌روزرسانی سیستم‌عامل و نرم‌افزارها وجود دارد که به با عنوان کلی مدیریت متمرکز وصله‌های ترمیمی(Patch Management) نام برده می‌شوند. برای نمونه، شاید واژه WSUS را شنیده باشید، WSUS یکی از راهکارهای به‌روزرسانی متمرکز است که شرکت مایکروسافت برای به‌روزرسانی محصولات خود عرضه کرده است.

علاوه بر رایانه ها، تبلت‌ها و تلفن‌های همراه هوشمند هم دارای سیستم‌عامل (مثلاً IOS و Android) بوده و نرم‌افزارهایی هم بسته به نیاز و علاقه کاربرانشان بر روی آن‌ها نصب شده است. سیستم‌عامل و نرم‌افزارهای این تجهیزات نیز مانند رایانه‌ها در معرض آسیب پذیری قرار دارند و نیازمند به‌روزرسانی هستند. پس به‌روزرسانی سیستم عامل و نرم‌افزارهای منصوب روی تبلت یا تلفن هوشمند خود توجه داشته باشید و همینطور از اعمال تغییراتی که موجب کاهش سطح امنیت آن می گردد (روش‌های شکستن قفل سیستم عامل آن جهت نصب نرم‌افزارهای رایگان و ...) پرهیز کنید.

علاوه بر به‌روزرسانی سیستم‌عامل و برنامه‌های کاربردی، ارتقای آن‌ها نیز دارای اهمیت است. ارتقای یعنی به‌روزرسانی نرم‌افزار که باعث تغییر نسخه آن محصول می‌شود و مجموعه‌ای از تغییرات را در نرم‌افزار اعمال می‌کند. به عبارت دیگر، ارتقا به معنای جایگزینی یک محصول با یک نوع جدید آن است. بیشتر شرکت‌های تولیدکننده نرم‌افزار در دوره‌های مشخصی در زمینه به‌روزرسانی و ارتقای نرم‌افزارهای تولیدی خود اقداماتی انجام می‌دهند. این تغییرات برای رفع یک یا مجموعه ای از نقص ها و یا اضافه شدن قابلیت های جدید در آن محصول انجام می‌شود. معمولاً نسخه های جدید علاوه بر رفع آسیب پذیری و نقاط ضعف، با تغییرات مشهودی از لحاظ کارایی و امکانات ارائه می گردند. بهتر است بدانید، شرکت های تولید کننده پس از ارائه محصولات جدید فقط تا مدت مشخصی نسبت به ارائه نسخه های به‌روزرسانی برای محصولات قدیمی تر اقدام می کنند و پس از پایان زمان خدمات پشتیبانی یک محصول، این نرم‌افزارها در هجمه نفوذ هکرها برای استفاده از نقاط ضعف موجود قرار می گیرند. پس، توصیه می‌شود حتی المقدور از نسخ جدید و به روز شده سیستم عامل و یا نرم‌افزارهای کاربردی استفاده شود و یا در صورت استفاده از نسخ قدیمی تر، از ارائه خدمات پشتیبانی و دریافت وصله های امنیتی توسط شرکت تولید کننده مطمئن باشید. به عنوان مثال ، سیستم عامل Windows XP از زمره سیستم عامل هایی است که دیگر خدماتی از سوی شرکت مایکروسافت برای آن ارائه نمیگردد. همچنین، برای استفاده از نرم‌افزارها ترجیحاً از نسخه‌های قفل شکسته که از لحاظ امنیتی پرمخاطره می‌باشند، استفاده نکنیم و اینگونه محصولات را از منابع معتبر و با لایسنس معتبر تهیه کنید.

نرم‌افزار ضد بدافزار و به‌روزرسانی آن

:

برطبق آنچه در فصل قبل در مورد بدافزارها مطرح شد، رایانه ها، تبلت ها، تلفن‌های هوشمند در معرض خطر آلودگی به انواع بدافزارها قرار دارند. روش‌های زیادی باعث آلودگی این تجهیزات به بدافزارها می‌شود. اقداماتی نظیر اتصال یک رسانه ذخیره سازی آلوده به رایانه، باز کردن فایل پیوست و یا لینک موجود در یک پست الکترونیک ناشناس، اجرای یک فایل آلوده دانلود شده از یک سایت، کلیک روی لینک‌های ناشناس موجود در سایت‌های نامعتبر و شبکه‌های اجتماعی موجب آلوده شدن رایانه و یا تلفن همراه هوشمند می‌شود. همانطور که در قبل عنوان شد، رویکرد بدافزارها به مرور تغییر کرده و بیشتر با هدف تخریب و دزدی اطلاعات منتشر می شوند. از سوی دیگر روال امور شخصی و کار، تکیه بیشتری بر فضای دیجیتال دارد و اکثر مواقع اطلاعات مهم در رایانه و یا تلفن همراه نگهداری می‌شود. بدیهی است در چنین شرایطی آلودگی حتی تلفن به یک بدافزار ، زیان‌های جبران ناپذیری را ممکن است دربرداشته باشد. پس، آگاهی و استفاده از روش‌های پیشگیری از نفوذ بدافزارها امری ضروری و اجتناب ناپذیر است.
نرم‌افزار ضدویروس یا ضد بدافزار همانطور که از نامش پیداست، نرم‌افزاری برای مقابله با فعالیت های مخرب ویروس‌ها و بدافزارها است. نرم‌افزار ضدویروس بعد از نصب بر روی رایانه، خودکار، شروع به کار کرده و وظیفه آن جلوگیری از هرگونه فعالیت مشکوک توسط برنامه‌ها می‌باشد. ضدویروس‌ها، هم عملکرد پیشگیرانه به معنی جلوگیری از آلوده شدن رایانه، تبلت، تلفن‌های هوشمند و سایر تجهیزات ذخیره سازی اطلاعات دارند و هم عملکرد واکنشی به معنی پاکسازی فایل‌های آلوده به ویروس و بدافزار را دارا می‌باشند.
علاوه بر اهمیت نصب نرم‌افزار ضدویروس بر روی رایانه یا سایر تجهیزات، نکته مهم دیگر، به‌روز بودن آن می‌باشد. از آنجایی که در هر روز ویروس‌ها و بدافزارهای جدیدی نوشته و منتشر می‌شوند، بنابراین، لازم است که نرم‌افزار ضدویروس نیز با همین سرعت به‌روز شوند تا توانایی شناسایی ویروس‌ها و بدافزارهای جدید را داشته باشند. برای همین این نرم‌افزارها به صورت روزانه و برخی از آن‌ها به صورت ساعتی نسخه به‌روزرسانی ارائه می کنند. پس، ضرورت دارد رایانه، تبلت و تلفن هوشمند شما به صورت روزانه به اینترنت متصل شود تا نرم‌افزار ضدویروس منصوب روی آن‌ها به روز گردد. تنظیمات این نرم‌افزارها طوری است که در صورت اتصال به اینترنت، نسخه های به‌روزرسانی را خودکار انجام می دهند. نکته قابل توجه دیگر این است که نباید گزینه اسکن خودکار نرم‌افزار ضدویروس را غیرفعال کنید، بلکه باید اجازه دهید که ضدویروس خودکار، سیستم شما را پویش کرده تا بتواند موارد مشکوک و آلوده را شناسایی نماید. همچنین هنگام اتصال رسانه های ذخیره سازی جانبی مثل فلش قبل از هرگونه اقدامی از طریق نرم‌افزار ضدویروس آن را پویش نمایید. معمولاً پویش رسانه های ذخیره سازی در صورت اتصال در تنظیمات پیش فرض قرار دارند، امّا اگر روی رایانه شما این چنین نیست، حتماً به این امر توجه کنید و یا برای اعمال تنظیمات از افراد متخصص کمک بگیرید.
به‌روزرسانی نرم‌افزار ضدویروس برای رایانه های مستقر در سازمان‌ها و شبکه‌های بزرگ متفاوت است و به روش‌های متمرکز مدیریت و به‌روزرسانی می شوند. روش‌های متمرکز علاوه بر داشتن مزایایی نظیر ممانعت از ایجاد بار ترافیک زیاد در شبکه ارتباطی و عدم لزوم دسترسی رایانه ها به اینترنت، از طریق کنسول های مدیریتی این امکان را ایجاد می‌کند که گزارشاتی از میزان به روز بودن رایانه های موجود در شبکه و یا بدافزارهای شناسایی شده در اختیار مسئولین ذیربط در سازمان قرار بگیرد.
نکته دیگر درباره تهیه یک نرم‌افزار ضدویروس، داشتن لایسنس معتبر است. چون این محصول به عنوان یک نرم‌افزار امنیتی وظیفه محافظت از رایانه و تجهیزات شما را در برابر مخاطرات امنیتی به عهده داشته و به همه بخش های سیستم دسترسی دارد. بنابراین، درصورت استفاده از یک نرم‌افزار ضدویروس تقلبی یا بدون لایسنس معتبر، امکان سواستفاده از رایانه شما افزایش می‌یابد و اگر نرم‌افزار ضدویروس صحیح کار نکند، می‌تواند خساراتی را در پی داشته باشد. به عبارت دیگر، تهیه یک نرم‌افزار ضدویروس معتبر که این روزها خرید آن به سادگی از طریق خریدهای اینترنتی و غیرحضوری و با هزینه ای کم نیز امکانپذیر است، اطلاعات شما را در برابر مخاطرات امنیتی تا حد قابل توجهی محافظت می‌کند. بهتر است بدانید، با خرید محصولات ضدویروس چند کاربره با پرداخت هزینه ای نسبتاً کمتر، می توانید رایانه های مورد استفاده خود و خانواده و یا تلفن همراه را به صورت مدیریت شده از نفوذ بدافزار ها حفظ کنید.
به رغم همه اقداماتی که تاکنون برای محافظت در برابر بدافزارها گفته شد، در صورت آلودگی رایانه به بدافزار موارد ذیل را در نظر داشته باشید :

• اگر از اطلاعات خود قبلاً نسخه پشتیبان تهیه کرده اید، بهتر است تا زمانی که بدافزار به طور کامل از روی سیستم شما پاکسازی نشده، از بازیابی اطلاعات خودداری کنید. چون وجود بدافزار ممکن است موجب آلودگی مجدد شده و در بدترین حالت اطلاعات پشتیبان نیز از دست بروند.
• در صورت بُروز آلودگی، سیستم خود را خاموش کنید تا اطلاعات بیشتری آلوده نشوند. بعد از خاموش کردن سیستم آلوده از روشن کردن مجدد آن خودداری کنید و از یک متخصص برای رفع مشکل یاری بگیرید. چرا که احتمال آسیب بیشتر به اطلاعات و نرم‌افزارها و یا رمزگذاری چندباره فایل¬ها یا تکمیل عملیات خرابکاری روی فایل‌هایی که به هر دلیلی مصون مانده‌اند وجود دارد.
• از دستکاری سیستم آلوده تا حد امکان خودداری کنید و در صورت نیاز از یک متخصص کمک بگیرید.

تهیه نسخه پشتیبان

:

تهیه نسخه پشتیبان به این معنی است که کپی یا رونوشتی از اطلاعات در حافظه‌ای جداگانه ذخیره شود تا در هنگام بروز مشکل یا از بین رفتن اطلاعات اصلی از آن نسخه استفاده شود. هر فردی در طول زندگی‌اش ممکن است اطلاعات و دارایی‌هایی را خواسته و یا ناخواسته از دست بدهد. تصور کنید چندین ماه است که در حال کار کردن بر روی یک پروژه تحقیقاتی برای محل کار یا دانشگاه بر روی رایانه خود هستید، ناگهان رایانه شما دچار مشکل می‌شود و تمامی اطلاعات ذخیره شده در آن از بین می‌رود. این به معنی از بین رفتن همه زحمات چند ماهه شما و از دست دادن اطلاعات مهم دیگر خواهد بود. بدتر این که بدانید هیچ کپی دیجیتال یا نسخه چاپی از این اطلاعات ندارید. و یا در اتفاق دیگری ممکن است اطلاعات رایانه شما که محل ذخیره تصاویر و فیلم های خانواده، دوستان و سفرها است بر اثر آلوده شدن به یک بدافزار از نوع باج‌افزار، به حالت رمز شده درآیند. حال آنکه بسیاری از این اطلاعات را نمی توانید دوباره تهیه کنید و یا ارزشمند بوده یا این که در زمان کوتاه قابل جمع آوری نباشند. در چنین شرایطی اهمیت تهیه و نگهداری از یک نسخه پشتیبان درک می گردد.

بنابراین، لازم است همیشه از اطلاعات مهم و حساس خود نسخه پشتیبان داشته باشید تا در صورت وجود آلودگی و از بین رفتن اطلاعات بتوانید با بازیابی نسخه‌های پشتیبان، اطلاعات خود را برگردانید. برای تهیه نسخه پشتیبان باید یک استراتژی و روش مناسب داشته باشید تا در گذر زمان و با بالارفتن حجم اطلاعات، کارایی لازم را داشته باشد. از این جمله برای تهیه نسخه پشتیبان، برنامه زمانبندی داشته باشید برای مثال انتهای هر روز یا هر هفته با توجه به حجم و اهمیت اطلاعات تولید شده، از آن‌ها نسخه پشتیبان تهیه کنید. اطلاعات نسخه پشتیبان را بر روی یک تجهیز ثالث مثلاً حافظه های ذخیره سازی جانبی و در محلی امن به دور از آب و گرما و دسترسی افراد غیرمجاز نگهداری کنید. حتماً روی رسانه های ذخیره سازی حاوی اطلاعات پشتیبان برچسب گذاری کنید تا در صورت نیاز برای بازیابی اطلاعات، قابل شناسایی و تشخیص باشند. معمولاً سازمآن‌ها سیاست های تعریف شده ای برای نگهداری نسخه پشتیبان دارند که باید همه کارکنان از این سیاست ها در حیطه مسئولیت خود آگاه باشند و مورد توجه قرار دهند. مثلاً تجهیزات حاوی اطلاعات نسخه پشتیبان باید دارای برچسب اطلاعات شامل تاریخ و نوع و طبقه اطلاعاتی باشند و در محل امن نظیر گاوصندوق و کمدهای قفل دار نگهداری شوند. همینطور ممکن است مجوز و سطوح دسترسی مشخصی برای افراد برای استفاده از اطلاعات تعریف شود. علاوه براین، در سیاست های سازمانی معمولاً ابزار و امکانات تهیه و ذخیره سازی نسخه پشتیبان از اطلاعات هم مشخص می‌شود. مثلاً در سازمانی ممکن است زیرساخت های لازم برای نگهداری اطلاعات در بستر مبتنی بر شبکه با در نظر گرفتن ملاحظات امنیتی لازم ایجاد شده باشد.

یکی از مشکلات کاربران در تهیه نسخه پشتیبان این است که نمی‌دانند از چه اطلاعاتی پشتیبان تهیه کنند. پوشه My Document عمدتاً پوشه‌ای در رایانه است که به‌صورت پیش فرض هر فایلی که دانلود یا ذخیره می کنید، به این پوشه منتقل می‌شود. بسیاری از کاربران برای دسته‌بندی و مدیریت فایل‌ها از این پوشه استفاده می کنند، در نتیجه داشتن نسخه پشتیبان از این فایل ضروری است. فایل‌های ذخیره شده بر روی رایانه نیز اطلاعاتی هستند که شما ایجاد کرده و یا از جای دیگری به رایانه منتقل کرده‌اید. این فایل‌ها ممکن است تصویری، صوتی، کتاب الکترونیک یا اسناد و مکاتبات متنی باشند. در صورتی که آن‌ها را یک جا نگهداری کنید، تهیه نسخه پشتیبان از آن‌ها هم بسیار راحت خواهد بود و یا اگر از نرم‌افزارهای واسطی استفاده می کنید که به نحوی اطلاعاتی در آن‌ها ذخیره می‌شود، از فایل های اصلی و یا از روش‌های پیش بینی شده در خود نرم‌افزار یک کپی تهیه و در جای دیگری نگهداری کنید. به عنوان مثال نرم‌افزار

Outlook نرم‌افـزاری واسـط جهـت مدیریـت پسـت هـای الکترونیـک اسـت، کـه بایـد از اطلاعـات ذخیـره شـده آن نسـخه ای به عنوان پشتیبان تهیه و نگهداری شود.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- ضرورت حفظ امنیت رایانه ها و سامانه‌ها را دریافته اید.	
۲- با تعریف سیستم‌عامل و برنامه‌های کاربردی و اهمیت به‌روزرسانی آن‌ها آشنا شدید.	
۳- با راهکارهای محافظت در برابر انواع بدافزارها آشنا شدید.	
۴- اهمیت تهیه نسخه پشتیبان از اطلاعات را درک کرده اید.	

خودآزمایی جلسه هفتم :

۱. ..... نرم‌افزاری است که با استفاده مستقیم از منابع و قابلیت‌های رایانه، کاری را مستقیماً برای کاربر انجام می‌دهد.

الف) سخت‌افزار ب) سیستم عامل ج) برنامه کاربردی د) حافظه های جانبی

۲. کدامیک از تعاریف زیر درباره "ارتقای نرم‌افزار" صحیح است.

الف) به‌روزرسانی نرم‌افزار که باعث تغییر نسخه آن محصول می‌شود

ب) جایگزینی یک محصول با یک نوع جدید آن

ج) دریافت وصله‌های امنیتی

د) گزینه الف و ب

۳. کدامیک از جملات زیر در صورت آلوده شدن سیستم به بدافزارها، صحیح نمی‌باشد؟

الف) از دستکاری آن خودداری کنید و در صورت نیاز از متخصص کمک بگیرید.

ب) سیستم خود را خاموش و مجدداً روشن کنید، شاید بدافزار از بین برود.

ج) تا زمانی که بدافزار به طور کامل از روی سیستم شما پاکسازی نشده است، از بازیابی نسخ پشتیبان اطلاعات خودداری کنید.

د) هیچ کدام

۴. تهیه نسخه پشتیبان به معنی ..... در حافظه‌ای جداگانه برای استفاده در هنگام بروز مشکل یا از بین رفتن اطلاعات اصلی است.

الف) جابه‌جایی اطلاعات ب) تهیه کپی یا رونوشتی از اطلاعات ج) محافظت از اطلاعات د) امن‌سازی اطلاعات

پاسخ‌نامه تشریحی

خودآزمایی جلسه هفتم

:

۱. پاسخ صحیح، گزینه «ج»
برنامه کاربردی، نرم‌افزاری است که با استفاده مستقیم از منابع و قابلیت‌های رایانه، کاری را مستقیماً برای کاربر انجام می‌دهد.

۲. پاسخ صحیح، گزینه «د»
ارتقا یعنی به‌روزرسانی نرم‌افزار که باعث تغییر نسخه آن محصول می‌شود و مجموعه‌ای از تغییرات را در نرم‌افزار اعمال می‌کند و به عبارت دیگر ارتقا به معنای جایگزینی یک محصول با یک نوع جدید آن است.

۳. پاسخ صحیح، گزینه «ب»
در صورت آلودگی سیستم به بدافزارها انجام اقدامات زیر ضروری است:
- اگر از اطلاعات خود نسخه پشتیبان دارید، بهتر است تا زمانی که بدافزار به طور کامل از روی سیستم شما پاکسازی نشده، از بازیابی اطلاعات خودداری شود.
- در صورت بُروز آلودگی، سیستم خود را خاموش کنید تا اطلاعات بیشتری آلوده نشوند. بعد از خاموش کردن سیستم آلوده از روشن کردن مجدد آن خودداری کرده و از یک متخصص برای رفع مشکل یاری بگیرید. چرا که احتمال آسیب بیشتر به اطلاعات و نرم‌افزارهای سیستم یا رمزگذاری چندباره فایل¬ها یا تکمیل عملیات خرابکاری روی فایل‌هایی که به هر دلیلی مصون مانده‌اند وجود دارد.
- از دستکاری سیستم آلوده تا حد امکان خودداری کنید و در صورت نیاز از یک متخصص کمک بگیرید.

۴. پاسخ صحیح، گزینه «ب»
تهیه نسخه پشتیبان به معنی تهیه کپی یا رونوشتی از اطلاعات در حافظه‌ای جداگانه برای استفاده در هنگام بروز مشکل یا از بین رفتن اطلاعات اصلی است.

جلسه هشتم

ارتقای امنیت در استفاده از سامانه‌ها و اینترنت

۱۶۳	اهداف یادگیری
۱۶۴	پیش‌آزمون
۱۶۶	توجه به نکات امنیتی در استفاده از سامانه‌ها
۱۶۸	رمز عبور و مدیریت آن
۱۷۱	انتخاب رمز عبور مناسب
۱۷۶	راهکارهای محافظت از رمز عبور
۱۸۱	امنیت در هنگام استفاده از اینترنت
۱۸۲	ابزارهای اصالت سنجی
	پروتکل ارتباطی SSL
	میزان دستیابی به اهداف آموزشی
	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با نحوه انتخاب رمز عبور و ملاحظات نگهداری آن آشنا شود.
۲. ملاحظات امنیتی در هنگام استفاده از اینترنت را دریابد.
۳. با مفهوم ابزار (Token)، ابزارهای اصالت سنجی و پروتکل ارتباطی SSL آشنا شود.

پیش‌آزمون جلسه هشتم :

۱. کدامیک از موارد زیر در خصوص انتخاب و مدیریت رمز عبور، صحیح نمی‌باشد؟

الف) یک رمز عبور برای همه سامانه‌ها و کارت‌های اعتباری خود انتخاب کنیم تا به خاطر سپردن آن راحت‌تر باشد.

ب) رمزهای عبور و کدهای کاربری خود را در یک دفترچه یادداشت کنیم و در یک جای امن بگذاریم.

ج) برای جلوگیری از فراموشی رمز عبور خود، از کلمات و عبارات متداول استفاده کنیم.

د) همه موارد

۲. کدامیک از نکات زیر در هنگام استفاده از اینترنت صحیح می‌باشد؟

الف) استفاده از یک ضدویروس معتبر و به روز

ب) تهیه نسخه پشتیبان از اطلاعات مهم

ج) نصب برنامه‌های کاربردی متعدد بر روی سیستم خود

د) گزینه الف و ب

پاسخ‌نامه

پیش‌آزمون جلسه هشتم :

	الف	ب	ج	د
۱				
۲				

توجه به نکات امنیتی در استفاده از سامانه‌ها

:

همانطور که قبلاً گفته شد، حفظ و ارتقای امنیت اطلاعات نیازمند توجه به نکات امنیتی از جنبه های مختلف در فضای سایبری است. در بخش قبل در مورد ملاحظات و نکات قابل توجه در مورد استفاده از رایانه، تبلت و تلفن های هوشمند توضیح داده شد. اگرچه رعایت نکات مهمی نظیر به‌روزرسانی سیستم عامل و استفاده از نرم‌افزارهای ضدویروس به روز و معتبر در مصون ماندن از مخاطرات امنیتی نقش چشمگیری دارد، اما در نظر داشته باشید، روش‌های متفاوتی برای سوء استفاده از اطلاعات وجود دارد. روش‌های مهندسی اجتماعی، اشتباهات سهوی نظیر ترک رایانه بدون قفل نمودن صفحه ورود و...، اتفاقاتی است که امکان سوء استفاده از اطلاعات کاربران را ایجاد می کنند. پس ضرورت دارد، علاوه بر توجه به حفظ ارتقای امنیت تجهیزات مورد استفاده ، با رعایت نکات امنیتی ساده اما مهم مانند انتخاب کلمه عبور مناسب برای سامانه‌ها و نرم‌افزارهای مورد استفاده ، بهره گیری از ابزارهایی نظیر توکن و یکبار رمز در هنگام ورود به سامانه‌های مهم و یا توجه به ملاحظات امنیتی در هنگام استفاده از اینترنت، موجب محافظت و مصونیت دارایی‌های اطلاعاتی در مقابل رخدادهای احتمالی شوید. در ادامه به نکات و راهکارهای امنیتی که موجب ارتقای سطح امنیت در هنگام استفاده از سامانه‌ها و اینترنت اشاره می گردد.

رمز عبور و مدیریت آن

:

رمز عبور یا گذرواژه یک کلمه یا جمله و یا عبارتی است که به همراه حساب‌های کاربری جهت اصالت‌سنجی و احراز هویت برای ورود و دسترسی به یک سامانه، سیستم عامل رایانه، پست الکترونیک ، وب‌سایت ها ، تجهیزات امنیتی و ...، به کار می‌رود. داشتن یک رمز عبور مناسب قطعاً امنیت محرمانگی اطلاعات را بالا برده و گاهی یک رمز عبور نامناسب می تواند موجب دسترسی و سوء استفاده از کل یک شبکه ارتباطی گردد. پس آگاهی از نحوه انتخاب رمز عبور مناسب و راهکارهای محافظت از آن، گامی بزرگ و مهم در حفظ امنیت دارایی‌های اطلاعاتی شخصی و سازمانی است.

انتخاب رمز عبور مناسب

:

برای انتخاب کلمات عبور مناسب، بهتر است موارد ذیل را در نظر داشته باشید:

- رمز عبور ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص باشد.
- طول کلمه عبور حداقل هشت کاراکتر باشد.
- از رمزهای عبوری که با توالی کلیدهای صفحه کلید ساخته شده و امکان دیده شدن آن هنگام وارد کردن توسط افراد را میسر می‌کند، نظیر abc۱۲۳ یا ۱۲۳۴۵۶ یا qwerty ، اجتناب شود.
- بر پایه اطلاعات شخصی نظیر اسم، فامیل، تاریخ تولد، شماره تلفن، کد ملی و .... نباشد.
- از کلمات متداول و دارای معنی در فرهنگ لغات که قابل حدس زدن می باشند، استفاده نشده باشد.
- دارای الگویی باشد که به خاطر آوردن آن برای صاحب رمز عبور آسان و حدس زدن آن برای دیگران دشوار باشد.

راهکارهای محافظت از رمز عبور

:

علاوه بر انتخاب کلمه عبور مناسب، حفاظت از رمز عبور به عنوان یک دارایی اطلاعاتی محرمانه اهمیت بسیاری دارد. امروزه با توجه به اینکه بسیاری از کارهای روزمره شخصی و سازمانی از طریق دسترسی به خدمات و سامانه‌های مبتنی بر شبکه انجام می گردد، اکثرافراد با تعدد رمزهای عبور مواجه هستند، بنابراین توجه به نحوه انتخاب کلمات عبور و چگونگی نگهداری و دسترسی به آن‌ها، موضوع مهم و قابل توجهی است. لذا، در ذیل به نکات و ملاحظاتی که در حفظ محرمانگی رمزهای عبور انتخاب شده باید مورد توجه قرار گیرند، اشاره شده است :

• رمز عبور سامانه‌های مورد استفاده، سیستم عامل ، پست الکترونیک ، کارت های بانکی و .... ، را حداقل هر سه ماه یکبار تغییر دهید.

• از نوشتن رمزعبور در دفترچه یادداشت روزانه، تقویم رومیزی یا چسباندن آن بر روی مانیتور و میز کار خود، خودداری کنید.

• از ارائه نام کاربری و رمزعبور به اعضای خانواده و دوستان حتی افراد مورد اعتمادتان خودداری کنید.

• در صورتی‌که متوجه شدید کسی از نام کاربری و یا رمز عبور شما مطلع شده، یا احتمال می دهید که فاش شده باشد، فوراً آن را تغییر دهید.

• از رمز عبور مشابه برای تمامی سامانه‌ها و حساب‌های کاربری خود استفاده نکنید. برای به‌خاطر سپردن رمزهای عبور در سامانه‌ها و حساب‌های کاربری از الگوریتم مشخصی استفاده کنید. در این صورت به خاطر سپردن رمز عبور راحت تر خواهد بود.

• رمز عبور را ازطریق تلفن برای کسی بازگو نکرده و همچنین از طریق پست الکترونیک و سایر شکل های ارتباطی فاش نکنید.

• قالب و الگوریتم رمزهای عبور مورد استفاده را برای کسی بازگو نکنید.

• از ویژگی "Remember Password" یا ذخیره رمز عبور در مرورگر های وب ، استفاده نکنید.

• از ذخیره نام کاربری و کلمات عبور بر روی کاغذ و یا یک فایل در رایانه اجتناب کنید. در صورت نیاز به استفاده از ابزاری جهت مدیریت رمزهای عبور می توان از شرکت‌هایی که محصولات امنیتی تولید می‌کنند، نرم‌افزار مدیریت رمز عبور تهیه کرد. این نرم‌افزارها قادر به ایجاد، مدیریت و ذخیره رمزهای عبور منحصر به فرد با هر طول و پیچیدگی با روش‌های امنیتی مناسب می‌باشند.

معمولاً در سازمآن‌ها سیاست هایی برای انتخاب و استفاده از رمز عبور تعریف شده است که کارکنان می بایست در حیطه وظایف خود در مورد آن‌ها آگاه باشند. همچنین در مورد سامانه‌های مهم و دارای اطلاعات طبقه بندی شده، برخی از این سیاست ها به صورت اجباری اعمال می گردند. به طور مثال: الزام به تغییر رمزعبور در بازه زمانی ۴۵ روزه و یا اجبار به انتخاب رمز عبور پیچیده و متشکل از حرف و عدد و کاراکتر و یا جلوگیری از انتخاب کلمات عبوری که قبلاً استفاده شده اند، نمونه هایی از کنترل های تعبیه شده در سامانه‌های مورد استفاده توسط سازمآن‌ها و سرویس هایی است که در قالب خدمت به مشتریان ارائه می گردد.

امنیت در هنگام استفاده از اینترنت

:

در عصر حاضر ، نیازهای روزمره به نحوی افراد را به استفاده از اینترنت وابسته نموده و به عبارتی اینترنت به یکی از ارکان ارتباطی و نیازهای اصلی در فعالیت های روزمره تبدیل شده است. این در حالی است که به همین میزان، تهدیدات فضای سایبری و روش‌های سوء استفاده از طریق بستر اینترنت در حال افزایش است. پس میزان آگاهی کاربران این شبکه ارتباطی در محافظت در برابر مخاطرات موجود و افراد سودجو مؤثر و دارای اهمیت است. اگر چه بسیاری از نکات مهم و دارای اهمیت در فصول مختلف این مستند ودر قالب موضوعات مفتون اشاره شده اند، ولی به دلیل اهمیت این مقوله ، در اینجا به طور خاص به نکاتی که رعایت آن‌ها در هنگام استفاده از اینترنت، کاربران را مصون می نماید، اشاره می گردد.

• برای اتصال به اینترنت از رایانه و یا تجهیزاتی که دارای سیستم عامل و نرم‌افزار ضدویروس به روز و معتبر هستند، استفاده کنید.
• در هنگام استفاده از مرورگرهای وب ، تنظیمات امنیتی آن‌ها را فعال وبه صورت مستمر آن‌ها را بروزرسانی کنید.
• با استفاده از رسانه های ذخیره سازی جانبی از مهم ترین اطلاعات خود نسخه پشتیبان تهیه کنید.
• به پست الکترونیک و پیامک‌هایی با محتوای برنده شدن در قرعه‌کشی و یا حاوی لینک‌ها و پیوست‌های مشکوک توجهی نکنید.
• در هنگام استفاده از شبکه‌های اجتماعی، نکات زیر را مورد توجه قرار دهید:
o اتفاقاتی که برایتان می‌افتد، به ویژه رویدادهای خاص زندگی را سریعاً به اشتراک نگذارید.
o از تنظیمات حفظ حریم خصوصی در این شبکه ها حتماً استفاده کنید. به این ترتیب مانع دسترسی افراد غیر مجاز به اطلاعات خود می شوید.
o عکس‌ها و فیلم‌های خصوصی خود را در صفحاتی که نمی‌شناسید، منتشر نکنید.
• از کلیک کردن بر روی لینک‌های ناشناس در صفحات وب بپرهیزید.
• مراقب ترفندهای مهندسی اجتماعی باشید.
• برای دریافت برنامه ها و فایل های مورد نیاز از اینترنت، حتماً از سایت های معتبر استفاده کنید و از نصب انواع برنامه‌های ناشناس و غیرضروری بپرهیزید.
• جهت دسترسی به وب‌سایت های اینترنتی به ویژه به منظور انجام تراکنش های مالی از صحت نشانی وارد شده در مرورگر وب ، مطمئن شوید.
• قبل از ورود اطلاعات از اصالت درگاه‌های بانکی و از وجود نشانگرهای امنیتی (SSL و HTTPS) قبل از نشانی اینترنتی سایت مورد نظر اطمینان حاصل کنید. این نشانگرهای امنیتی به معنای رمز شدن اطلاعات و عدم امکان سرقت اطلاعات شما توسط دیگران می‌باشد.
• از انجام امور بانکداری اینترنتی و پرداخت اینترنتی و یا ورود به پست الکترونیک در کافی‌نت ها و مراکز عمومی پرهیز کنید. در صورتی که مجبور به انجام این کار شدید، پس از انجام این امور، از حساب کاربری خود خارج شوید و ترجیحاً در اولین فرصت نسبت به تغییر رمز عبور اقدام کنید.
• در صورت دریافت پست الکترونیک ناشناس ، هوشیارانه عمل کنید، در صورتی که فرستنده را نمی‌شناسید و یا موضوع به نظر مشکوک می آمد، بهتر است نامه را حذف کنید و یا پیوست های آن را قبل از بازکردن با استفاده از نرم‌افزار ضدویروس، پویش نمایید.
• از ابزارهای فیلتر شکن نظیر VPN در هنگام دسترسی به سامانه‌های نیازمند نام کاربری و رمز عبور به ویژه در هنگام انجام امور بانکداری اینترنتی اجتناب کنید.
سازمان‌ها برای استفاده از اینترنت معمولاً دارای سیاست های سازمانی خاصی هستند که کارکنان آن‌ها علاوه بر رعایت موارد یاد شده در فوق، می بایست به اجرای ملاحظات سازمانی توجه نمایند. به طور مثال الزام به استفاده از پست الکترونیک سازمان در تعاملات کاری و یا اجتناب از نصب و استفاده از نرم‌افزارهای
شبکه‌های اجتماعی، نمونه هایی از این سیاست ها هستند.

ابزارهای اصالت سنجی

:

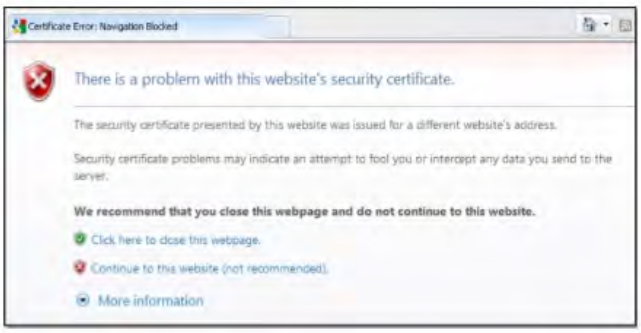
همان‌طور که گفته شد، نام کاربری و رمز عبور برای احراز هویت جهت ورود و دسترسی به سامانه‌ها و خدمات استفاده می‌شود. از آنجایی که احتمال فاش شدن و سوء استفاده از رمز عبور به تنهایی وجود دارد، در مورد سامانه‌های دارای اطلاعات حساس و همچنین سامانه‌های بانکی از ابزارهای احراز هویت و
اصالت سنجی دیگری به عنوان عامل دوم و با بهره گیری از مکانیزم های رمزنگاری استفاده می‌شود. در این صورت وجود ابزارهای احراز هویت دو عاملی که با نام عمومی توکن نام برده می شوند، احتمال دسترسی های غیرمجاز را تقریباً ناممکن می سازد. در این حالت ، برای ورود و استفاده از یک سامانه به رمز عبور اکتفا نشده و از کاربر عامل یا فاکتور دوم (توکن) را جهت شناسایی در خواست می نماید. توکن ها انواع مختلفی دارند اما نمونه های متداول آن‌ها به صورت سخت‌افزاری و ظاهری شبیه به یک حافظه فلش دارند. کاربردهای عمومی آن‌ها شامل احراز هویت،

امضای دیجیتال و رمز نگاری اطلاعات است. با توجه به اینکه هر توکن منحصراً برای یک نام کاربری خاص تعریف و قابل استفاده است، به نوعی ابزار اصالت سنجی محسوب می گردد. این نوع توکن ها در هنگام استفاده می بایست به رایانه متصل شده و رمز عبور (PIN) مربوطه برای شناسایی وارد شود.
نمونه دیگری از توکن ها، توکن یکبار رمز (OTP) است، که با تولید رمز عبور منحصر به فرد و دارای اعتبارِ زمانیِ مشخص به عنوان عامل دوم احراز هویت استفاده می‌شود. استفاده از یکبار رمز در هنگام استفاده از خدمات بانکداری اینترنتی متداول و گاهاً الزامی است. این توکن ها انواع مختلفی اعم از سخت‌افزاری، نرم‌افزاری و مبتنی بر تلفن همراه دارند.
باتوجه به اینکه توکن ها ابزار احراز هویت و اصالت سنجی می باشند ،در حفظ و نگهداری آنها باید دقت کرده و در صورت مفقود شدن در اولین فرصت مراتب به مراجع مرتب اعلام شود.

پروتکل ارتباطی SSL

:

همانطور که می دانید، نشانی وب‌سایت هایی که در آن‌ها تراکنش های مالی انجام می‌شود، نظیر وب‌سایت بانکداری اینترنتی و یا درگاه های پرداخت با عبارت HTTPS به جای HTTP آغاز می شوند. عبارت HTTPS حاکی از استفاده از پروتکل ارتباطی امن(SSL) جهت ایجاد ارتباط دو طرفه بین خدمات دهنده (نظیر بانک) و خدمات گیرنده (مشتری یا کاربر) در بستر شبکه ارتباطی می باشد. این ارتباط امن موجب جلوگیری از شنود، تغییر و سوء استفاده از اطلاعات در حال تبادل می گردد. این پروتکل های ارتباطی که گواهینامه دیجیتال SSL نیز نامیده می شوند، علاوه بر ایجاد یک ارتباط امن، به نحوی هویت وب‌سایت را نیز تأیید می‌کند. این گواهینامه ها دارای اعتبار زمانی هستند و چنانچه به هر دلیلی گواهینامه معتبر نبوده و یا تاریخ اعتبار آن به پایان رسیده باشد، در مرورگر وب پیغام خطایی، نمایش داده می‌شود. در این مواقع بهتر است از ورود به سایت و ورود اطلاعات خودداری شود. همچنین در محل نمایش نشانی سایت در مرورگر وب، علامت قفل بیانگر معتبر بودن گواهینامه دیجیتال SSL می باشد و با کلیک بر روی آن، جزئیات گواهینامه از جمله تاریخ اعتبار آن قابل مشاهده است.
استفاده از گواهینامه دیجیتال SSL، محدود به وب‌سایت های بانکی نبوده و برای هر وب‌سایتی که به نحوی در آن، اطلاعات مهم و محرمانه قابل دسترسی و تبادل باشد، استفاده می گردد. برای همین در بسیاری از وب‌سایت های اینترانتی و درون سازمانی هم از پروتکل ارتباطی(HTTPS SSL) استفاده می‌شود.



شکل ۱: نمونه پیغام خطا در صورت عدم اعتبار گواهینامه SSL

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید،
در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- با نحوه انتخاب رمز عبور و ملاحظات نگهداری آن آشنا شدید.	
۲- ملاحظات امنیتی در هنگام استفاده از اینترنت را درک کرده اید.	
۳-بامفهوم ابزار توکن، ابزارهای اصالت سنجی و پروتکل ارتباطی SSL آشنا شدید.	

خودآزمایی جلسه هشتم :

۱. کدامیک از نکات زیر در هنگام استفاده از شبکه‌های اجتماعی صحیح می‌باشد؟
الف) عدم به اشتراک گذاری تصاویر و فیلم‌های خانوادگی و اتفاقات روزمره
ب) عدم افشای نام‌های کاربری و رمز عبور و اطلاعات شخصی و خاطرات خود
ج) احتیاط و دقت در مقابل ترفندهای مهندسی اجتماعی
د) همه موارد

۲. یک رمزعبور مناسب باید ..... :
الف) ترکیبی از حروف کوچک و بزرگ ، اعداد و کاراکترهای خاص باشد.
ب) دارای طول حداقل هشت کاراکتر باشد.
ج) از کلمات متداول و عمومی در آن استفاده نشده باشد.
د) همه موارد

۳. کدامیک از موارد زیر از کاربردهای توکن نیست ؟
الف) احراز هویت ب) امضای دیجیتال ج) ذخیره اطلاعات د) رمزنگاری اطلاعات

۴. پروتکل ارتباطی SSL جهت ..... بین خدمات دهنده و خدمات گیرنده استفاده می‌شود.
الف) ایجاد ارتباط امن ب) ایجاد ارتباط سریع ج) رمزنگاری اطلاعات د) انتقال اطلاعات

پاسخ‌نامه تشریحی

خودآزمایی جلسه هشتم

:

۱. پاسخ صحیح، گزینه «د»

در هنگام استفاده از شبکه‌های اجتماعی، به نکات زیر توجه کنید:

- هر اتفاقی که برایتان می‌افتد را سریعاً به اشتراک نگذارید.
- تنظیمات حریم خصوصی در این شبکه‌ها را بهینه کنید.
- عکس‌ها و فیلم‌های خصوصی خود را در صفحاتی که نمی‌شناسید، منتشر نکنید.
- از افشای نام‌های کاربری و رمز عبور و اطلاعات شخصی و خاطرات خاص خود بپرهیزید.
- از کلیک کردن بر روی لینک‌های ناشناس بپرهیزید.
- مراقب ترفندهای مهندسی اجتماعی باشید.

۲. پاسخ صحیح، گزینه «د»

یک رمزعبور مناسب باید :

- ترکیبی از حروف کوچک و بزرگ ، اعداد و کاراکترهای خاص باشد.
- دارای طول حداقل هشت کاراکتر باشد.
- از کلمات متداول و عمومی در آن استفاده نشده باشد.
- بر پایه اطلاعات شخصی نظیر اسم ، فامیل، تاریخ تولد، شماره تلفن، کد ملی و ....، نباشد.

۳. پاسخ صحیح، گزینه «ج»

کاربردهای عمومی توکن ها شامل احراز هویت، امضای دیجیتال و رمز نگاری اطلاعات است.

۴. پاسخ صحیح، گزینه «الف»

پروتکل ارتباطی SSL جهت ایجاد ارتباط امن بین خدمت دهنده و خدمت گیرنده استفاده می‌شود.

جلسه نهم

سیاست میز و صفحه نمایش پاک

۱۸۷	اهداف یادگیری
۱۸۸	پیش‌آزمون
۱۹۰	سیاست میز کار پاک و صفحه نمایش پاک
۱۹۲	الزامات سیاست میز کار پاک و صفحه نمایش پاک
۱۹۲	میزان دستیابی به اهداف آموزشی
۱۹۷	خودآزمایی
۱۹۸	خلاصه فصل چهارم

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با سیاست میز پاک و صفحه نمایش پاک و الزامات آن آشنا شود.

پیش‌آزمون جلسه نهم :

۱. اجرای سیاست میزپاک و صفحه نمایش پاک باید توسط چه کسانی انجام شود؟

الف) واحد امنیت سازمان

ب) همهٔ پرسنل

ج) مدیران سازمان

د) واحد حراست سازمان

۲. در صورت ترک میز خود کدامیک از اقدامات زیر را بهتر است انجام دهیم؟

الف) با همکار مجاور هماهنگ نمود.

ب) سیستم را خاموش نمود.

ج) صفحه نمایش سیستم را قفل کرد.

د) گذرواژه را تغییر داد.

پاسخ‌نامه

پیش‌آزمون جلسه نهم

:

	الف	ب	ج	د
۱				
۲				

سیاست میز کار پاک و صفحه نمایش پاک

:

امروزه اطلاعات همانند سایر سرمایه های تجاری یک سازمان و شاید بیش از آن ها ارزشمند بوده و به همان میزان نیازمند مراقبت صحیح و مطمئن در برابر تهدیدات گسترده داخلی و خارجی است. برای درک بهتر این سیاست تصور کنید کارمند واحد مشتریان سازمانی در حال تهیه گزارش از سطوح مالی، میزان تراکنش ها و گزارش های تحلیلی مرتبط است. در آخرین لحظه، مدیر وی او را به یک جلسه فوری دعوت می کند و کارشناس مربوطه بدون در نظر گرفتن مخاطرات نسبت به دارایی ها و اسناد کاغذی روی میزش و اطلاعات محرمانه و مهم روی صفحه نمایش رایانه اش، اتاق را ترک می کند. در این زمان، در دسترس بودن دارایی های اطلاعاتی توسط کارمند مجاور یا هر یک از همکاران درون سازمانی یا شخصی که در آن نزدیکی قرار دارد، مخاطره مهمی تلقی می شود و دارایی های اطلاعاتی و محرمانه سازمان در معرض دسترسی افرادی که نباید دسترسی داشته باشند، قرار می گیرد. در سیاست میز کار پاک و صفحه نمایش پاک با رعایت نکات امنیتی تعریف شده با هدف محافظت از اطلاعات در فضای محیطی محل کار، از بروز چنین مشکلاتی جلوگیری خواهد شد.

شکل ۲: رعایت سیاست میز کار پاک و صفحه نمایش پاک

الزامات سیاست میز کار پاک و صفحه نمایش پاک

:

برای محافظت از اطلاعات پیرامون فضای محیطی محل کارتان ، به نکات ذیل همواره توجه داشته باشید :

• دارایی های اطلاعاتی همچون اسناد کاغذی و رسانه های ذخیره سازی مانند لپ تاپ، تلفن های هوشمند، فلش و غیره را زمانی که شخصی برای محافظت از آن ها وجود ندارد یا زمانی که مورد نیاز نمی باشند، در کمدها، قفسه ها یا کشوهای دارای قفل سالم و امن نگهداری کنید.

• از قرار دادن اسناد کاری و اطلاعات محرمانه بر روی میز کاری خود بدون مراقبت کاربرخودداری کنید.

• رایانه ها و تجهیزات مشابه را در زمان عدم استفاده یا زمانی که پشت میز خود نیستید، قفل یا Log off و در صورت ترک محل کار خود، خاموش کنید.

• لازم است رایانه تان به گونه ای قرار گیرد که صفحه نمایش شما قابل رویت توسط سایر افراد نباشد.

• سیستم های خود را به گونه ای تنظیم نمایید که در صورت عدم استفاده به مدت مثلاً ۱۰ دقیقه، صفحه نمایش آن ها به صورت خودکار قفل شود.

• استفاده از پرینتر، دستگاه کپی، دستگاه فکس، دوربین و سایر تجهیزات مشابه باید تحت کنترل و مراقبت کاربر باشد. این کنترل باعث کاهش نشت اطلاعات می شود و اطلاعات کمتری در معرض مشاهده دیگران خواهد بود.

• پس از چاپ اطلاعات مورد نیاز به ویژه اطلاعات طبقه بندی شده و حساس سازمان ، حتماً و سریعاً آن را از روی پرینتر بردارید.

• از قرار دادن و ذخیره کردن اطلاعات مهم و زیاد بر روی صفحه نمایش رایانه خود اجتناب کنید و صفحه نمایش خود را تمیز و خلوت نگه دارید.

• اطلاعات و اسناد کاغذی یا الکترونیک مهم و محرمانه را در صورتی که مورد نیاز نیستند، با استفاده از روش های ایمن مانند دستگاه کاغذ و سی دی خردکن، امحا کنید و از استفاده مجدد این اسناد کاغذی به عنوان اسناد باطله جداً پرهیز نمایید.

• از نوشتن اطلاعات مهم بر روی تقویم میز کار و یا چسباندن کاغذهای حاوی اطلاعات بر روی صفحه نمایش ، میز و یا دیوار خودداری کنید.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- با سیاست میز کار پاک و صفحه نمایش پاک و الزامات آن آشنا شدید.	

خودآزمایی جلسه نهم :

۱. پیش از ترک محل کار باید کدامیک از اقدامات زیر را انجام دهیم؟
الف) سیستم رایانه خود را خاموش کنیم.
ب) صفحه نمایش سیستم خود را قفل کنیم.
ج) خاموش کردن سیستم خود را به همکار بسپاریم.
د) صفحه نمایش سیستم خود را خاموش کنیم.

۲. کدامیک از موارد زیر درباره سیاست میز کار پاک و صفحه نمایش پاک صحیح است؟
الف) قابل رویت نبودن صفحه نمایش رایانه شما توسط دیگران
ب) عدم استفاده از پرینتر، دستگاه کپی و دستگاه فکس بدون مراقبت کاربر
ج) داشتن صفحه نمایش تمیز و خلوت
د) همه موارد

پاسخ‌نامه تشریحی

خودآزمایی جلسه نهم

:

۱. پاسخ صحیح، گزینه «الف»

رایانه‌ها و تجهیزات مشابه را در زمان عدم استفاده یا زمانی که پشت میز خود نیستید، قفل یا Log off و در صورت ترک محل کار خود خاموش کنید.

۲. پاسخ صحیح، گزینه «د»

در سیاست میز کار پاک و صفحه نمایش پاک :

- لازم است رایانه‌تان به گونه‌ای قرار گیرد که صفحه نمایش شما قابل رویت توسط سایر افراد نباشد.
- استفاده از پرینتر، دستگاه کپی، دستگاه فکس، دوربین و سایر تجهیزات مشابه باید تحت کنترل و مراقبت کاربر باشد.
- از قرار دادن و ذخیره کردن اطلاعات مهم و زیاد بر روی صفحه نمایش رایانه خود اجتناب کنید و صفحه نمایش خود را تمیز و خلوت نگه دارید.

خلاصه فصل چهارم

جلسه هفتم

سیستم‌عامل (OS)، نرم‌افزاری است که مدیریت منابع رایانه را بر عهده گرفته و بستری را برای اجرا و بهره‌گیری از برنامه‌های کاربردی فراهم می‌کند. منظور از برنامه کاربردی، نرم‌افزاری است که با استفاده مستقیم از منابع و قابلیت‌های رایانه، کاری را مستقیماً برای کاربر انجام می‌دهد. به‌روزرسانی زمان‌بندی‌شده و مستمر سیستم‌عامل و برنامه‌های کاربردی مورد استفاده در سیستم کاربر، جهت افزایش سطح امنیت، از اهمیت ویژه‌ای برخوردار است.

علاوه بر به‌روزرسانی سیستم‌عامل و برنامه‌های کاربردی، ارتقای آن‌ها نیز حائز اهمیت می‌باشد. ارتقا یعنی به‌روزرسانی نرم‌افزار که باعث تغییر نسخه آن محصول می‌شود و مجموعه‌ای از تغییرات را در نرم‌افزار اعمال می‌کند و به عبارت دیگر، ارتقا به معنای جایگزینی یک محصول با یک نوع جدید آن است. آلودگی رایانه ها به بدافزار از طرق مختلفی نظیر باز کردن پیوست ایمیل‌های ناشناس و مشکوک، کلیک روی لینک‌های ناشناس موجود در سایت‌های نامعتبر و شبکه‌های اجتماعی، انتقال از طریق رسانه‌های ذخیره‌سازی قابل حمل انجام می گردد. یکی از این راهکارهای مقابله با نفوذ بدافزارها، استفاده از نرم‌افزار ضدویروس یا ضد بدافزار است. این نرم‌افزار بعد از نصب بر روی رایانه، خودکار شروع به کار کرده و وظیفه آن جلوگیری از هر گونه فعالیت مشکوک توسط برنامه‌ها می‌باشد. علاوه بر اهمیت نصب ضدویروس بر روی سیستم رایانه‌ای، مطلب مهم دیگر، به‌روز بودن آن می‌باشد. نکته دیگر درباره تهیه یک ضدویروس، لایسنس‌دار (قانونی و معتبر) بودن آن است چرا که امکان به‌روزرسانی و تأمین امنیت بیشتری را دارا می باشد.

تهیه نسخه پشتیبان به معنی تهیه و ذخیره کپی یا رونوشتی از اطلاعات در حافظه‌ای جداگانه است تا در هنگام بروز مشکل یا از بین رفتن اطلاعات اصلی از نسخه پشتیبان استفاده شود. نسخه پشتیبان باید در فواصل زمانی مشخص تهیه و ضمن ذخیره بر روی رسانه های ذخیره سازی جانبی، در محلی امن دور از آب و گرما و دسترسی افراد غیرمجاز نگهداری شوند. نسخ پشتیبان سازمانی را داخل کمدهای قفل‌دار یا گاوصندوق بگذارید.

جلسه هشتم

یکی از راهکارهای دیگر برای محافظت از اطلاعات استفاده از رمزعبور مناسب و مدیریت آن است. رمز عبور یا گذرواژه یک کلمه یا جمله و یا عبارتی است که جهت اصالت‌سنجی و احراز هویت برای استفاده از یک سامانهٔ محافظت شده و حساب‌های کاربری به کار می‌رود. رمز عبور مناسب ویژگی های زیر را دارد:

- رمز عبور ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص باشد.
- طول کلمه عبور حداقل هشت کاراکتر باشد.
- از رمزهای عبوری که با توالی کلیدهای صفحه کلید ساخته شده و امکان دیده شدن آن هنگام وارد کردن توسط افراد را میسر می‌کند، نظیر abc۱۲۳ یا ۱۲۳۴۵۶ یا qwerty، اجتناب شود.

• بر پایه اطلاعات شخصی نظیر اسم ، فامیل، تاریخ تولد، شماره تلفن، کد ملی و .... نباشد.
• از کلمات متداول و دارای معنی در فرهنگ لغات که قابل حدس زدن می باشند، استفاده نشده باشد.
• دارای الگویی باشد که به خاطر آوردن آن برای صاحب رمز عبور آسان و حدس زدن آن برای دیگران دشوار باشد.

با توجه به نیاز روزمره به استفاده از اینترنت ، میزان آگاهی کاربران این شبکه ارتباطی در محافظت در برابر مخاطرات موجود و افراد سودجو مؤثر و دارای اهمیت است. برخی از نکات مورد توجه در هنگام استفاده از اینترنت به شرح است :

• برای اتصال به اینترنت از رایانه و یا تجهیزاتی که دارای سیستم عامل و نرم‌افزار ضدویروس به روز و معتبر هستند، استفاده کنید.
• در هنگام استفاده از مرورگرهای وب ، تنظیمات امنیتی آن‌ها را فعال وبه صورت مستمر آن‌ها را به‌روزرسانی کنید.
• به پست الکترونیک و پیامک‌هایی با محتوای برنده شدن در قرعه‌کشی و یا حاوی لینک‌ها و پیوست‌های مشکوک توجهی نکنید.
• از کلیک کردن بر روی لینک‌های ناشناس در صفحات وب بپرهیزید.
• برای دریافت برنامه ها و فایل های مورد نیاز از اینترنت، حتماً از سایت های معتبر استفاده کنید و از نصب انواع برنامه‌های ناشناس و غیرضروری بپرهیزید.
• جهت دسترسی به وب‌سایت های اینترنتی به ویژه به منظور انجام تراکنش های مالی از صحت نشانه وارد شده در مرورگر وب ، مطمئن شوید.
• قبل از ورود اطلاعات از اصالت درگاه‌های بانکی و از وجود نشانگرهای امنیتی (SSL و HTTPS) قبل از نشانه اینترنتی سایت مورد نظر اطمینان حاصل کنید. این نشانگرهای امنیتی به معنای رمز شدن اطلاعات و عدم امکان سرقت اطلاعات شما توسط دیگران می‌باشد.
• از ابزارهای فیلتر شکن نظیر VPN در هنگام دسترسی به سامانه‌های نیازمند «نام کاربری و رمز عبور» به ویژه در هنگام انجام امور بانکداری اینترنتی اجتناب کنید.

ابزار توکن برای احراز هویت دو عاملی و با بهره گیری از مکانیزم های رمزنگاری استفاده می‌شود. استفاده از عامل دوم احراز هویت، احتمال دسترسی های غیرمجاز را تقریباً ناممکن می سازد. در این حالت ، برای ورود و استفاده از یک سامانه به رمز عبور اکتفا نشده و از کاربر عامل یا فاکتور دوم (توکن) را جهت شناسایی در خواست می نماید. توکن ها انواع مختلفی دارند اما نمونه های متداول آن‌ها به صورت سخت‌افزاری و ظاهری شبیه به یک حافظه فلش دارند. کاربردهای عمومی آن‌ها شامل احراز هویت، امضای دیجیتال و رمز نگاری اطلاعات است. یکبار رمز نیز نمونه ای از ابزار احراز هویت دو عاملی است.

نشانی وب‌سایت هایی که در آن‌ها تراکنش های مالی انجام می‌شود ، نظیر وب‌سایت بانکداری اینترنتی و یا درگاه های پرداخت با عبارت HTTPS به جای HTTP آغاز می شوند. عبارت HTTPS حاکی از استفاده از پروتکل ارتباطی امن(SSL) جهت ایجاد ارتباط دو طرفه بین خدمت دهنده (نظیر بانک) و خدمت گیرنده (مشتری یا کاربر) در بستر شبکه ارتباطی می باشد. این ارتباط امن موجب جلوگیری از شنود ، تغییر و سوءاستفاده از اطلاعات در حال تبادل می گردد.

جلسه نهم

:

سیاست میز کار پاک و صفحه نمایش پاک، رعایت نکات امنیتی با هدف محافظت از اطلاعات در فضای محیطی محل کار را بیان می کند. الزامات سیاست میز کار پاک و صفحه نمایش پاک شامل موارد زیر است:

• دارایی‌های اطلاعاتی همچون اسناد کاغذی و رسانه‌های ذخیره‌سازی مانند لپ‌تاپ، تلفن‌های هوشمند ، فلش و غیره را زمانی که شخصی برای محافظت از آن‌ها وجود ندارد یا زمانی که مورد نیاز نمی‌باشند، در کمدها، قفسه‌ها یا کشوهای دارای قفل سالم و امن نگهداری کنید.
• از قرار دادن اسناد کاری و اطلاعات محرمانه بر روی میز کاری خود بدون مراقبت کاربر خودداری کنید.
• رایانه‌ها و تجهیزات مشابه را در زمان عدم استفاده یا زمانی که پشت میز خود نیستید، قفل یا Log off و در صورت ترک محل کار خود خاموش کنید.

• لازم است رایانه‌تان به گونه‌ای قرار گیرد که صفحه نمایش شما قابل رویت توسط سایر افراد نباشد.
• سیستم‌های خود را به گونه‌ای تنظیم نمایید که در صورت عدم استفاده به مدت مثلاً ۱۰ دقیقه، صفحه نمایش آن‌ها خودکار قفل شود.
• استفاده از پرینتر، دستگاه کپی، دستگاه فکس، دوربین و سایر تجهیزات مشابه باید تحت کنترل و مراقبت کاربر باشد. این کنترل باعث کاهش نشت اطلاعات می‌شود و اطلاعات کمتری در معرض مشاهده دیگران خواهد بود.
• پس از چاپ اطلاعات مورد نیاز به ویژه اطلاعات طبقه بندی شده و حساس سازمان، حتماً و سریعاً آن را از روی پرینتر بردارید.
• از قرار دادن و ذخیره کردن اطلاعات مهم و زیاد بر روی صفحه نمایش رایانه خود اجتناب کنید و صفحه نمایش خود را تمیز و خلوت نگه دارید.
• اطلاعات و اسناد کاغذی یا الکترونیک مهم و محرمانه را در صورتی که مورد نیاز نیستند، با استفاده از روش‌های ایمن مانند دستگاه کاغذ و سی‌دی خردکن، امحا کنید و از استفاده مجدد این اسناد کاغذی به عنوان اسناد باطله جداً پرهیز نمایید.
• از نوشتن اطلاعات مهم بر روی تقویم میز کار و یا چسباندن کاغذهای حاوی اطلاعات بر روی صفحه نمایش ، میز و یا دیوار خودداری کنید.

فصل اول: آشنایی با مفاهیم امنیت اطلاعات

فصل دوم: امنیت فیزیکی و محیطی

فصل سوم: تهدیدات امنیتی در شبکه های رایانه‌ای

فصل چهارم: امنیت در مقابله با تهدیدات فضای سایبری

فصل پنجم

امنیت تجهیزات قابل حمل

جلسه دهم:
امنیت در رسانه های ذخیره‌سازی و رایانه های قابل حمل

جلسه یازدم:
امنیت در تلفن های هوشمند

فصل ششم:
توصیه های امنیتی در خدمات بانکی

فصل هفتم:
جرایم رایانه‌ای و تعهدنامه عدم افشای اطلاعات

فصل هشتم:
پیاده سازی امنیت در سازمان ها

جلسه دهم

امنیت در رسانه های ذخیره‌سازی و رایانه های قابل حمل

۱۴۱	اهداف یادگیری
۱۴۲	پیش‌آزمون
۱۴۴	رسانه ذخیره‌سازی قابل حمل
۱۴۸	نکات امنیتی در بکارگیری رسانه‌های ذخیره‌سازی قابل حمل
۱۴۹	اهمیت امنیت در رایانه های قابل حمل
۱۴۹	نکات امنیتی در رایانه های قابل حمل
۱۵۰	میزان دستیابی به اهداف آموزشی
۱۵۱	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با رسانه‌های ذخیره‌سازی قابل حمل آشنا شود.
۲. اهمیت برقراری امنیت در رایانه‌های قابل حمل را درک کند.
۳. با نکات امنیتی در هنگام استفاده از رسانه‌های ذخیره‌سازی و رایانه های قابل حمل آشنا شود.

پیش‌آزمون جلسه دهم :

۱. ..... ابـزاری دارای حافظـه اسـت کـه بـرای ذخیره‌سـازی داده‌هـا و اطلاعـات از آن‌هـا اسـتفاده می‌شـود.

الف) فضای رایانه‌ای ب) رسانه ذخیره سازی ج) مانیتور د) کیبورد

۲. کدامیک از جملات زیر در خصوص رسانه‌های ذخیره سازی صحیح نمی‌باشد؟

الف) اطلاعات سازمانی و شخصی خود را بر روی رسانه‌های ذخیره سازی قابل حمل نگهداری کنید.

ب) از نگهداری این رسانه‌ها در مکان‌های عمومی و قابل دسترس همگان پرهیز نمایید.

ج) قبل از استفاده از رسانه، آن را با نرم افزار ضد ویروس به‌روز و قانونی پایش کنید.

د) از رسانه‌های قابل حملی که دارای کد اموال هستند و توسط سازمان احراز شده‌اند، استفاده کنید.

۳. کدامیک از جملات زیر درباره رایانه‌های قابل حمل صحیح نمی‌باشد؟

الف) برای انجام امور سازمانی فقط از لپ‌تاپ های مشخص و سازمانی و دارای کد اموال استفاده کنید.

ب) برای لپ‌تاپ رمز عبور انتخاب کنید و نکات مربوط به انتخاب رمز عبور مناسب را در نظر بگیرید.

ج) یک نرم افزار ضد ویروس به‌روز و مورد تأیید روی آن نصب کنید.

د) هیچ کدام

پاسخ‌نامه

پیش‌آزمون جلسه دهم

:

	الف	ب	ج	د
۱		■		
۲	■			
۳				■

رسانه ذخیره‌سازی قابل حمل

:

رسـانه ذخیره‌سـازی ابـزاری دارای حافظـه اسـت کـه بـرای ذخیره‌سـازی داده‌هـا و اطلاعـات از آن‌هـا اسـتفاده می‌شـود. رسـانه‌های ذخیره‌سـازی قابـل حمـل یـا جداشـدنی می‌تواننـد بـه راحتـی بـه رایانـه متصـل و جـدا شـوند و اغلـب بـرای نگهـداری و انتقـال داده میـان رایانه‌هـا بـه کار می‌رونـد.
فلـش ، حافظـه ذخیـره سـازی جانبـی ، کارت حافظـه میکـرو (SD)، لـوح فـشرده(CD)، دی‌وی‌دی (DVD)، تبلـت، تلفن‌هـای همـراه هوشـمند و ... نمونه‌هایـی از رسـانه‌های ذخیره‌سـازی قابـل حمـل می‌باشـند.

نکات امنیتی در بکارگیری رسانه‌های ذخیره‌سازی قابل حمل

:

از آنجایـی کـه کاربـرد اصلـی رسـانه‌های ذخیره‌سـازی قابـل حمـل، انتقـال اطلاعـات می‌باشـد، بنابرایـن، عـدم توجـه بـه مقولـه امنیـت اطلاعـات می‌توانـد ایـن رسـانه را بـه ابـزاری بـرای نشـت اطلاعـات و انتقـال بدافزارهـا تبدیـل کنـد.
بنابـر ایـن، در زمـان اسـتفاده از ایـن رسـانه‌ها ضروری اسـت نـکات امنیتـی لازم مـورد توجـه قـرار بگیرنـد. در حـد امـکان از ذخیـره کـردن اطلاعـات مهـم و محرمانـه شـخصی و سـازمانی در انـواع رسـانه‌های ذخیره‌سـازی قابـل حمـل اجتنـاب نماییـد.
در صـورت نیـاز بـه ذخیـره کـردن اطلاعـات سـازمانی در رسـانه‌های ذخیره‌سـازی لازم اسـت بـه نـکات زیـر توجـه کنیـد :
o حتی الامکان از رسانه‌های قابل حملی که دارای کد اموال هستند و یا توسط سازمان احراز شده‌اند، استفاده کنید.
o از نگهـداری ایـن رسـانه‌ها در مکان‌هـای عمومـی و قابـل دسـترس همـگان پرهیـز کـرده و آن هـا را در مکانـی امـن نگهـداری کنیـد.
o قبل از استفاده از رسانه، آن را با نرم افزار ضدویروس به‌روز و مورد تأیید سازمان پایش کنید.
o پس از استفاده از رسانه، حتماً اطلاعات روی آن را به‌صورت کامل و امن پاک کنید.
o در صـورت گـم شـدن یـا سرقـت رسـانه‌ها و یـا حتـی اسـتفاده توسـط افـراد غیرمجـاز، موضـوع را بـه اطـلاع مدیـر یـا مسـئول مربوطـه برسـانید.
رایانـه ای کـه رسـانه ذخیره‌سـازی را بـه آن متصـل می‌کنیـد، بایـد دارای آخریـن به‌روزرسـانی‌های امنیتـی سیسـتم عامـل و نـرم افـزار ضدویـروس بـه‌روز، فعـال و مـورد تاییـد باشـد. همچنیـن ترجیحـاً دارای فایـروال فعـال بـوده و حتـی المقـدور بـه اینترنـت متصـل نباشـد.

اهمیت امنیت در رایانه های قابل حمل

:

اگرچـه اسـتفاده از رایانـه هـای قابـل حمـل بـه عنـوان ابـزاری جهـت سـهولت دسترسـی بـه اطلاعـات در هـر زمـان و هـر مـکان مـی باشـد، امّـا ویژگـی هایـی نظیـر قابـل حمـل بـودن و وزن و ابعـاد کـم، تهدیداتـی را در پـی دارد کـه اسـتفاده از ایـن تجهیـزات را مسـتلزم رعایـت نـکات امنیتـی مـی نمایـد. اگـر مقـداری پـول نقـد داشـته باشـید و در مـکان عمومـی نشسـته باشـید، آیـا حتـی بـرای یـک لحظـه روی خـود را از آن برمی‌گردانیـد؟ آیـا موقـع سـفر، آن‌را در چمـدان خـود قـرار می‌دهیـد؟ آیـا آن‌را در صندلـی عقـب ماشـین رهـا می‌کنیـد؟ البتـه کـه چنیـن کارهایـی نخواهیـد کـرد. هـمان مراقبتـی کـه از پـول نقـد خـود می‌کنیـد، از رایانـه قابـل حمـل (Laptop) خـود نیـز بایـد انجـام دهیـد. کوچک‌تریـن بی‌احتیاطـی و عـدم رعایـت نـکات امنیتـی می‌توانـد بـه از دسـت دادن رایانـه قابـل حمـل شـخصی یـا سـازمانی منجـر شـود. اگـر ایـن تجهیـزات گـم شـوند، ممکـن اسـت تمـام اطلاعـات بـا ارزش ذخیره‌شـده در آن‌هـا بـه دسـت افـراد غیرمجـاز بیفتـد. بنابرایـن، بـرای جلوگیـری از نابـودی یـا سوءاسـتفاده از اطلاعـات داخـل آن‌هـا بایـد یـک رشـته راهکارهـای امنیتـی اولیـه را رعایـت نمـود.

نکات امنیتی در رایانه های قابل حمل

:

هنگامی که همراه با رایانه قابل حمل (Laptop) شخصی از منزل خارج می‌شوید و یا همراه رایانه قابل حمل (Laptop) سازمانی در محیط بیرون از محل کار هستید، با آن مثل کیف پول‌تان برخورد کنید. اطلاعات داخل آن مانند پول داخل کیف دارای ارزش می‌باشند.

برای انجام امور سازمانی فقط از رایانه قابل حمل (Laptop) مشخص و سازمانی و دارای کد اموال استفاده کنید. و از اطلاعات حیاتی و مهم روی آن، نسخه پشتیبان تهیه کنید. همچنین برای دسترسی به سیستم عامل آن رمز عبور انتخاب کنید و نکات مربوط به انتخاب رمز عبور مناسب را مورد توجه داشته باشید.

حتماً سیستم‌عامل آن را به‌روز نگه دارید و آخرین وصله‌های امنیتی را بر روی آن نصب کنید. برای این منظور در مورد رایانه های سازمانی و برای مطابقت با سیاست های سازمان، لازم است ضمن مشورت با مسئول امور انفورماتیک، آن را دربازه های زمانی مشخص مثلاً به صورت ماهانه به شبکه داخلی سازمان برای دریافت نسخ به روزرسانی مرتبط متصل کنید. علاوه بر آن ضروری است بر روی آن یک نرم افزار ضدویروس مورد تأیید نصب و همواره آن را به روز کنید. بدیهی است برای رایانه های سازمانی باید نرم افزار ضدویروس مورد تأیید سازمان را نصب کرده و حداقل به صورت هفتگی آن را جهت دریافت نسخ به روزرسانی به شبکه داخلی سازمان متصل کنید.

در صورت عدم استفاده، میکروفون و دوربین آن را غیرفعال کنید. به یاد داشته باشید هنگام ترک محل (عدم استفاده برای مدتی کوتاه و موقت) آن را قفل یا Log off و هنگام ترک سازمان آن‌را خاموش کنید و در جای مناسب و امن قرار دهید.

در فرودگاه‌ها و هتل‌ها و اماکن عمومی بسیار مراقب رایانه قابل حمل(Laptop) شخصی یا سازمانی خود باشید و آن را حتی لحظه‌ای در اختیار سایر همکاران و افراد ناشناس قرار ندهید. از اتصال رایانه قابل حمل (Laptop) به شبکه‌های بی‌سیم ناشناخته و عمومی پرهیز کنید و در صورت اتصال، صرفاً به جستجوی اینترنتی عادی بپردازید و از خرید اینترنتی، ارسال پست الکترونیک و سایر امور جداً بپرهیزید.

حتماً از وارد شدن به سایت‌های ناشناخته و مشکوک و کلیک بر روی لینک‌های ارسالی و تبلیغات پرهیز کنید. و از اتصال رسانه‌های ذخیره‌سازی نظیر (فلش و حافظ های ذخیره سازی جانبی و غیره) به رایانه قابل حمل (Laptop) به ویژه موارد ناشناخته و غیر قابل اعتماد پرهیز کنید. در صورت نیاز به اتصال این رسانه‌ها، حتماً قبل از استفاده آن‌ها را توسط نرم افزار ضدویروس پویش کنید.

از نگهداری اطلاعات شخصی مهم و یا اطلاعات مهم و محرمانه سازمانی بر روی رایانه قابل حمل (Laptop) تا حد ممکن اجتناب نمایید و در صورت ضرورت، پس از استفاده، اطلاعات را از روی رایانه حذف کنید. و اطلاعات مهم و محرمانه ذخیره شده روی رایانه قابل حمل (Laptop) را حتی المقدور به صورت رمزنگاری شده نگهداری نمایید. رمزنگاری اطلاعات موجب جلوگیری از دسترسی افراد غیرمجاز به اطلاعات در صورت دسترسی های غیرمجاز و یا سرقت رایانه می گردد.

با توجه به اینکه رایانه های قابل حمل (Laptop) به دلیل ابعاد کوچک و ارزش بالا، هدف جذابی برای سارقان می باشند، از اینرو در مکان های شلوغ، هنگام عبور از خیابان و معابر عمومی، در اتومبیل و....،ملاحظات امنیتی لازم را مدّنظر داشته باشید.

اتصال رایانه قابل حمل (Laptop) به شبکه در سازمان ها عموماً تابع سیاست های ویژه ای است، پس در محل کار نسبت به اتصال رایانه های شخصی همکاران، پیمانکاران و سایرین به شبکه حساس باشید و در صورت مشاهده هر گونه نا امنی به مسئول مافوق اطلاع رسانی کنید.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید،
در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱-با رسانه‌های ذخیره‌سازی قابل حمل آشنا شدید.	
۲-اهمیت برقراری امنیت در رایانه‌های قابل حمل را درک کند.	
۳-با نکات امنیتی در هنگام استفاده از رسانه‌های ذخیره‌سازی و رایانه های قابل حمل آشنا شدید.	

خودآزمایی جلسه دهم :

۱. کدامیک از جملات زیر در خصوص رسانه‌های ذخیره‌سازی، صحیح نمی‌باشد؟
الف) سیستمی که رسانه به آن متصل می‌شود، دارای آخرین به‌روزرسانی‌های امنیتی باشد.
ب) سیستمی که رسانه به آن متصل می‌شود، دارای فایروال فعال باشد.
ج) در صورت گم شدن رسانه ذخیره‌سازی حاوی اطلاعات محرمانه سازمان، از یک رسانه دیگر استفاده کنید.
د) پس از استفاده از رسانه، اطلاعات روی آن را به‌صورت کامل و امن پاک کنید.

۲. کدامیک از جملات زیر درباره رایانه‌های قابل حمل صحیح می‌باشد؟
الف) در فرودگاه‌ها و هتل‌ها و اماکن عمومی بسیار مراقب رایانه های قابل حمل (Laptop) شخصی یا سازمانی خود باشید.
ب) اتصال رایانه های قابل حمل (Laptop) به شبکه های بی‌سیم عمومی بلامانع است.
ج) اتصال رسانه‌های ذخیره‌سازی اقوام و دوستان که آن ها را می‌شناسیم به رایانه های قابل حمل (Laptop)، بدون اسکن شدن توسط نرم افزار ضد ویروس بلامانع است.
د) همه موارد

۳. اتصال رایانه قابل حمل (Laptop) به شبکه در سازمان ها عموماً .....؟
الف) تابع سیاست های داخلی سازمان است.
ب) نیازمند قاعده خاصی نیست.
ج) نباید انجام گردد.
د) در صورت رعایت ملاحظات امنیتی بلامانع می باشد.

۴. کدام گزینه راهکار مناسبی برای افزایش امنیت رایانه های قابل حمل نیست؟
الف) یک نسخه نرم افزار ضدویروس بر روی آن نصب و آن را مستمراً به روزرسانی کنیم.
ب) از اطلاعات موجود بر روی آن نسخه پشتیبان تهیه کنیم.
ج) میکروفون و دوربین آن را غیرفعال کنیم.
د) هنگام ترک سازمان آن‌را خاموش کنیم.

پاسخ‌نامه تشریحی

خودآزمایی جلسه دهم

۱. پاسخ صحیح، گزینه «ج»

• پس از استفاده از رسانه، حتماً اطلاعات روی آن را به‌صورت کامل و ایمن پاک کنید.

• در صورت گم شدن یا سرقت رسانه‌ها و یا حتی استفاده توسط افراد غیرمجاز، موضوع را به اطلاع مدیریت یا مسئول مربوطه برسانید.

• سیستمی که رسانه ذخیره‌سازی را به آن متصل می‌کنید، باید دارای آخرین به‌روزرسانی‌های امنیتی و دارای فایروال فعال باشد.

۲. پاسخ صحیح، گزینه «الف»

• در فرودگاه‌ها و هتل‌ها و اماکن عمومی بسیار مراقب لپ‌تاپ شخصی یا سازمانی خود باشید و آن را حتی لحظه‌ای در اختیار سایر همکاران و افراد ناشناس قرار ندهید.

• از اتصال لپ‌تاپ به شبکه‌های بی‌سیم ناشناخته و عمومی پرهیز کنید.

• از اتصال رسانه‌های ذخیره‌سازی ناشناخته همچون (فلش و هاردهای قابل حمل و غیره) به لپ‌تاپ پرهیز کنید .

• در صورت نیاز به اتصال این رسانه‌ها، حتماً قبل از استفاده، آن‌ها را توسط نرم افزار ضدویروس پویش کنید.

۳. پاسخ صحیح، گزینه «الف»

اتصال رایانه قابل حمل (Laptop) به شبکه در سازمان ها عموماً تابع سیاست های ویژه ای است، پس، در محل کار نسبت به اتصال رایانه های شخصی همکاران، پیمانکاران و سایرین به شبکه، حساس باشید و در صورت مشاهده هرگونه نا امنی به مسئول مافوق اطلاع رسانی کنید.

۴. پاسخ صحیح، گزینه «د»

برای حفظ امنیت رایانه قابل حمل، در هنگام ترک سازمان، ضروری است علاوه بر خاموش کردن رایانه، آن را در جای مناسب و امن قرار دهیم.

جلسه یازدهم

امنیت در تلفن های هوشمند

۱۶۳	اهداف یادگیری
۱۶۴	پیش‌آزمون
۱۶۶	اهمیت امنیت در تلفن های هوشمند
۱۶۸	نکات امنیتی در استفاده از تلفن های هوشمند
۱۷۱	میزان دستیابی به اهداف یادگیری
۱۷۶	خودآزمایی
۱۸۱	خلاصه فصل پنجم

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. اهمیت برقراری امنیت در تلفن های هوشمند را درک کند.
۲. با نکات امنیتی در استفاده از تلفن های هوشمند آشنا شود.

پیش‌آزمون جلسه یازدهم :

۱. بکارگیری کدامیک از راهکارهای زیر برای قفل کردن صفحه تلفن‌های هوشمند می‌تواند امنیت بیشتری را ایجاد کند؟

الف) استفاده از رمز عبور ب) استفاده از اثر انگشت ج) استفاده از الگوهای امنیتی د) همه موارد

۲. کدامیک از جملات زیر درباره رایانه‌های قابل حمل صحیح نمی‌باشد؟

الف) برای انجام معاملات بانکی از برنامه موبایل‌بانک به جای مرورگر وب استفاده کنید.

ب) برنامه‌های کاربردی تلفن هوشمند خود را از فروشگاه‌های معتبر همچون فروشگاه اپل خرید کنید.

ج) برای اینکه بتوانید محدودیت‌های تحریم را دور بزنید و برنامه‌های رایگان زیادی را بر روی تلفن خود نصب کنید، قفل تلفن هوشمند خود را بشکنید.

د) هنگام نصب برنامه‌های کاربردی بر روی تلفن هوشمند، قبل از تأیید دسترسی این برنامه‌ها به بخش‌های مختلف تلفن، آن را بررسی کنید.

پاسخ‌نامه

پیش‌آزمون جلسه یازدهم

:

	الف	ب	ج	د
۱				
۲				

اهمیت امنیت در تلفن‌های هوشمند

:

در سال های اخیر داشتن یک تلفن همراه، صرفاً به منظور برقراری ارتباط با سایرین نیست، بلکه قابلیت های تعبیه شده بر روی گوشی،آن را تبدیل به یک رایانه همراه کرده است و قابلیت های آن سبب شده تولید نرم افزارهای کاربردی در حوزه های مختلف با ویژگی های مناسب استفاده در صفحه چند اینچی تلفن همراه تبدیل به یک حرفه شود و بازارهای متعددی را جهت ارائه محصولات مختلف ایجاد کرده است. با کمی جستجو می بینیم که نرم افزارهای خاص پیش بینی آب و هوا، کالری شمار، تایپ و انواع بازی ها گرفته تا انواع نرم افزارهای تخصصی مالی، صنعتی، هتری و ....، سازگار با انواع سیستم عامل های تلفن های هوشمند تولید و ارائه شده اند. ویژگی خاص این نرم افزارها که عموماً با واژه اپلیکیشن نام برده می شوند، سهولت در استفاده و سادگی و نداشتن پیچیدگی در ظواهر و کاربری آن هاست، لذا، امروزه خیلی افراد ممکن است با دانش و توانایی کار با رایانه آشنا نباشند اما به خوبی می توانند با اپلیکیشن های منصوب در گوشی تلفن همراه خود بسیاری از فعالیت های حرفه ای از ویرایش یک تصویر تا فعالیت در رسانه های اجتماعی و یا کار با سامانه های مختلف را انجام دهند. حتی سهولت بکارگیری و حمل و نقل آن ها سبب شده، گوشی تلفن و یا تبلت، ابزار و کانال ارتباطی راه دور مدیران و کارکنان سازمان ها با سامانه های مورد استفاده نظیر کارتابل مکاتبات اداری و پست الکترونیک، سازمانی گردد. نفوذ این ابزارها در زندگی هر روزه و نیاز و تمایل اکثر افراد به دسترسی گوشی تلفن همراه به اینترنت باعث شده، گوشی تلفن همراه که روزی صرفاً یک ابزار ارتباط صوتی و متنی بود، مانند یک رایانه مورد توجه هکرها قرار بگیرد و به همین ترتیب حفظ امنیت اطلاعات موجود در آن برای کاربران آن ضروری است. پس، بسیاری از ملاحظاتی که در مورد رایانه خود نظیر به روزرسانی سیستم عامل، نصب نرم افزارهای معتبر، عدم دانلود فایل های ناشناس و ... را مورد توجه قرار می دهید، لازم است در مورد گوشی تلفن همراه هم رعایت کنید.

اکنون با گسترش استفاده از تلفن‌های هوشمند و تبلت‌ها، کاربران حجم بیشتری از اطلاعات و تصاویر شخصی و مهم خود و در بعضی موارد، دارایی‌های اطلاعاتی سازمان‌شان را روی گوشی‌های هوشمند ذخیره می‌کنند. هنگامی که با این تلفن‌های هوشمند و تبلت‌ها در حال گشت و گذار در اینترنت هستید، مهاجمان و هکرها از به‌دست آوردن اطلاعات شما، خوشنود می‌شوند. بنابراین، توجه به نکات امنیتی در استفاده این تجهیزات حائز اهمیت است. اگرچه خوشبختانه با تغییر تکنولوژی توسط سازندگان این گوشی‌ها و تبلت‌ها امنیت به حد قابل قبولی رسیده است امّا با توجه بیشتر و انجام چند اقدام ساده می‌توانید امنیت گوشی‌های هوشمند و تبلت خود را در مقابل نفوذ هکرها افزایش دهید.

نکات امنیتی در استفاده از تلفن‌های هوشمند

:

هنگام استفاده از تلفن‌های هوشمند و تبلت‌ها، با استفاده از رمزعبور یا یک الگوی امنیتی یا اثر انگشت، صفحه اصلی تلفن هوشمند/تبلت خود را قفل کنید و با این کار از دسترسی سایر افراد به تلفن خود جلوگیری نمایید. همچنین می‌توانید برای استفاده از برنامه‌های کاربردی خاص نصب شده بر روی تلفن خود مانند برنامه‌های پیام‌رسان، برنامه‌های پست الکترونیک، برنامه‌های مالی، برنامه‌های ذخیره تصاویر و فیلم‌ها و غیره که حاوی اطلاعات مهم هستند، به طور جداگانه رمز عبور انتخاب کنید.

تا حد امکان برای افزایش ضریب امنیت حساب‌های کاربری خود همچون پست الکترونیک یا برنامه‌های کاربردی تحت وب که بر روی تلفن هوشمند شما فعال هستند، از رمز عبور با تأیید دو مرحله‌ای استفاده کنید. تأیید دو مرحله‌ای، کاربر را ملزم می‌کند تا علاوه بر وارد کردن رمز عبور خود، کد امنیتی ارسال شده به تلفن همراه خود را نیز تایید کند. بنابراین، در صورت مفقود شدن یا سرقت تلفن همراه، با غیرفعال سازی سیم کارت، احتمال سوء استفاده از حساب های کاربری دشوار و ناممکن می گردد. همچنین از شکستن قفل تلفن هوشمند/تبلت خود برای سرگرمی یا رهایی از محدودیت‌های ناشی از تحریم و دلایل دیگر، پرهیز کنید. این کار باعث می‌شود که نتوانید جدیدترین به روزرسانی ها و وصله‌های امنیتی منتشر شده برای سیستم‌عامل تلفن هوشمند/تبلت خود را دریافت و نصب کنید

و ایـن یعنـی سـطح آسـیب‌پذیری و احتـمال نفـوذ بـه تلفـن هوشـمند خـود را افزایـش مـی دهیـد.
قبـل از دریافـت و نصـب برنامه‌هـای کاربـردی بـر روی تلفـن هوشـمند/تبلت خـود، از معتـبر بـودن آن اطمینـان حاصـل کنیـد و ایـن برنامه‌هـا را از منابـع معتـبر و قابـل اطمینـان همچـون فروشـگاه‌های اینترنتـی اپـل (App Store) و اندرویـد (Google Play) دریافـت نمایید.هنـگام نصـب برنامه‌هـای کاربـردی بـه پیغام‌هایـی کـه حیـن نصـب مبنـی بـر دسترسـی آن برنامـه بـه بخش‌هـای مختلـف تلفـن هوشـمندتان نمایـش داده می‌شـود، دقـت کنیـد. ایـن دسترسـی‌ها می‌توانـد شـامل دسترسـی بـه تصاویـر، موقعیت‌هـای جغرافیایـی، دفترچـه مخاطبـان و سـایر بخش‌هـای تلفـن شـما باشـند. بهـتر اسـت قبـل از تأییـد دسترسـی ایـن برنامه‌هـا بـه بخش‌هـای مختلـف تلفـن، آن را بررسـی کنیـد. اگرچـه اغلـب ایـن پیغام‌هـا مربـوط بـه درخواسـت‌های متعـارف و قانونـی هسـتند و آسـیبی ایجـاد نخواهنـد کـرد امـا بهـتر اسـت جانـب احتیـاط را رعایـت کنیـد.
بـرای انجـام امـور مهـم نظیـر معاملات بانکـی و امـوری کـه نیازمنـد تبـادل اطلاعـات خصوصـی و حسـاس بیـن تلفـن هوشـمند و اینترنـت می‌باشـد، بـه جـای اسـتفاده از مرورگـر از برنامـه کاربـردی موثـق و رسـمی مرتبـط بـا آن اسـتفاده کنیـد. بـرای مثـال بـه جـای وارد شـدن بـه صفحـه اینترنـت بانـک خـود به‌وسـیله مرورگـر تلفـن هوشـمند، می‌توانیـد از برنامـه کاربـردی همـراه بانـک کـه بانـک مبـدأ تهیـه کـرده اسـت ، اسـتفاده کنیـد. اسـتفاده از ایـن برنامه‌هـا، امنیـت بیشـتری نسـبت بـه مرورگرهـا دارد.
از اطلاعـات روی تلفن‌هـای هوشـمند و تبلـت خـود نسـخه پشـتیبان تهیـه کنیـد. ایجـاد نسـخه پشـتیبان از دارایی‌هـای اطلاعاتـی و نظیـمات تلفن‌هـای هوشـمند در مواقعـی کـه آن را جـا گذاشـته‌اید یـا در مـواردی کـه تلفـن هوشـمند شـما بـه سرقـت رفتـه و مجبـور هسـتید اطلاعـات آن را از راه دور پـاک کنیـد، بـه شـما کمـک خواهـد کـرد.
سیسـتم‌عامل تلفـن هوشـمند و تبلـت خـود را از طریـق نصـب نسـخ بـه روزرسـانی ارائـه شـده توسـط شرکـت سـازنده آن بـه‌روز نمایید و بـر روی تلفـن هوشـمند و تبلـت خـود نـرم افـزار ضدویـروس معتـبر نصـب کنیـد و آن را بـه‌روز نگـه داریـد. وقتـی کـه در خانـه یـا محیطـی امـن نیسـتید، بهـتر اسـت کـه وایرلـس و بلوتـوث تلفـن هوشـمند خـود را خامـوش کنیـد. هـر زمـان کـه بـه یـک شـبکه بی‌سـیم نامطمـئن متصـل شـوید، بـه هکرهـا اجـازه داده‌ایـد تـا بـه راحتـی بتواننـد از طریـق آن شـبکه، بـه اطلاعـات شـما دسترسـی پیـدا کننـد. امـروزه اسـتفاده از تجهیـزات جانبـی مختلـف همچـون هِدسِـت، سـاعت، ابزارهـای تناسـب انـدام و غیـره کـه از طریـق بلوتـوث بـه تلفـن هوشـمند شـما متصـل می‌شـوند، رواج بسـیاری پیـدا کـرده اسـت، آگاه باشـید کـه اگـر بلوتـوث تلفـن شـما روشـن و قابـل مشـاهده بـرای همـگان باشـد، احتـمال نفـوذ هکرهـا و شـنود داده‌هـای در حـال مبادلـه بیـن تجهیـز بلوتوثـی و تلفـن هوشـمند شـما وجـود دارد.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- اهمیت برقراری امنیت در تلفن های هوشمند را درک کردید.	
۲- با نکات امنیتی در استفاده از تلفن های هوشمند آشنا شدید.	

خودآزمایی جلسه یازدهم :

۱. برای افزایش ضریب امنیت حساب‌های کاربری خود همچون پست الکترونیک یا برنامه‌های کاربردی تحت وب که بر روی تلفن هوشمند شما فعال هستند، از رمز عبور ..... استفاده کنید.

الف) تک مرحله‌ای ب) دو مرحله‌ای ج) یکسان د) ساده برای یادآوری آسان

۲. کدامیک از موارد زیر می‌تواند راهی برای نفوذ و آلودگی تلفن‌های هوشمند باشد؟

الف) روشن بودن وایرلس در اماکن عمومی

ب) روشن بودن بلوتوث در اماکن عمومی

ج) عدم استفاده از نرم افزار ضدویروس

د) همه موارد

۳. برنامه‌های کاربردی شناخته‌شده را ..... تهیه کنید.

الف) از حراجی‌ها ب) از منابع قابل اطمینان ج) رایگان د) از داخل کشور

۴. کدام گزینه ویژگی کاربردی تلفن های هوشمند و تبلت است ؟

الف) قابلاستفاده برای دسترسی به سامانه های اداری کارکنان

ب) محل ذخیره کردن اطلاعات وتصاویر شخصی

ج) قابل اتصال به اینترنت

د) همه موارد

پاسخ‌نامه تشریحی

خودآزمایی جلسه یازدهم

:

۱. پاسخ صحیح، گزینه «ب»

برای افزایش ضریب امنیت حساب‌های کاربری خود همچون ایمیل یا برنامه‌های کاربردی تحت وب که بر روی تلفن هوشمند شما فعال هستند، از رمز عبور با تأیید دو مرحله‌ای استفاده کنید.

۲. پاسخ صحیح، گزینه «د»

- بر روی تلفن هوشمند و تبلت خود نرم افزار ضدویروس قانونی نصب کنید و آن را به‌روز نگه دارید.
- وقتی که در خانه یا محیطی امن نیستید، بهتر است که وایرلس و بلوتوث تلفن هوشمند خود را خاموش کنید. هر زمان که به یک شبکه بی‌سیم نامطمئن متصل شوید، به هکرها اجازه داده‌اید تا به راحتی بتوانند از طریق آن شبکه، به اطلاعات شما دسترسی پیدا کنند.

۳. پاسخ صحیح، گزینه «ب»

قبل از دریافت و نصب برنامه‌های کاربردی بر روی تلفن هوشمند خود، از معتبر بودن آن اطمینان حاصل کنید و این برنامه‌ها را از منابع معتبر و قابل اطمینان همچون فروشگاه‌های اینترنتی اپل و اندروید دریافت نمایید.

۴. پاسخ صحیح، گزینه «د»

تلفن‌های هوشمند و تبلت‌ها کاربرد دسترسی به سامانه‌های اداری برای مدیران و کارکنان داشته و ضمن اینکه محلی برای ذخیره کردن اطلاعات وتصاویر شخصی هستند، قابلیت اتصال به اینترنت را نیز دارند.

خلاصه فصل پنجم

جلسه دهم

رسانه ذخیره‌سازی ابزاری است دارای حافظه که برای ذخیره‌سازی داده‌ها و اطلاعات از آن‌ها استفاده می‌شود. از آنجایی که کاربرد اصلی رسانه‌های ذخیره‌سازی قابل حمل، انتقال اطلاعات می‌باشد، بنابراین، نبود توجه به مقوله امنیت اطلاعات می‌تواند این رسانه را به ابزاری برای نشت اطلاعات و انتقال بدافزارها تبدیل کند. پس در حد امکان از ذخیره کردن اطلاعات مهم و محرمانه شخصی و سازمانی در انواع رسانه‌های ذخیره‌سازی قابل حمل اجتناب نمایید.

در هنگام استفاده از رایانه قابل حمل به موارد امنیتی نظیر موارد ذیل توجه کنید:

- برای انجام امور سازمانی فقط از رایانه قابل حمل (Laptop) مشخص و سازمانی و دارای کد اموال استفاده کنید.
- در فرودگاه‌ها و هتل‌ها و اماکن عمومی بسیار مراقب رایانه قابل حمل (Laptop) شخصی یا سازمانی خود باشید و آن را حتی لحظه‌ای در اختیار سایر همکاران و افراد ناشناس قرار ندهید.
- از اتصال رایانه قابل حمل(Laptop) به شبکه‌های بی‌سیم ناشناخته و عمومی پرهیز کنید و در صورت اتصال، صرفاً به جستجوی اینترنتی عادی بپردازید و از خرید اینترنتی، ارسال پست الکترونیک و سایر امور جداً بپرهیزید.
- از نگهداری اطلاعات شخصی مهم و یا اطلاعات مهم و محرمانه سازمانی بر روی رایانه قابل حمل (Laptop) تا حد ممکن اجتناب نمایید و در صورت ضرورت، پس از استفاده، اطلاعات را از روی رایانه حذف کنید.

جلسه یازدهم

امروزه تلفن همراه، صرفاً به منظور برقراری ارتباط با سایرین نیست، بلکه قابلیت های تعبیه شده بر روی گوشی،آن را تبدیل به یک رایانه همراه کرده است و قابلیت های آن سبب شده تولید نرم افزارهای کاربردی در حوزه های مختلف با ویژگی های مناسب استفاده در صفحه چند اینچی تلفن همراه تبدیل به یک حرفه شده و بازارهای متعددی جهت ارائه محصولات مختلف را ایجاد کرده است. همینطور سهولت بکارگیری و حمل و نقل آن ها سبب شده، گوشی تلفن و یا تبلت، ابزار و کانال ارتباطی راه دور مدیران و کارکنان سازمان‌ها با سامانه های مورد استفاده نظیر کارتابل مکاتبات اداری و پست الکترونیک سازمانی گردد. نفوذ این ابزارها در زندگی هر روزه و نیاز و تمایل اکثر افراد به دسترسی گوشی تلفن همراه به اینترنت باعث شده است گوشی تلفن همراه که روزی صرفاً یک ابزار ارتباط صوتی و متنی بود، مانند یک رایانه مورد توجه هکرها قرار بگیرد و به همین ترتیب، حفظ امنیت اطلاعات موجود در آن برای کاربران آن ضروری است. پس، بسیاری از ملاحظاتی را که در مورد رایانه خود نظیر به روزرسانی سیستم عامل، نصب نرم افزارهای معتبر، عدم دانلود فایل های ناشناس و ...، مورد توجه قرار می دهید، لازم است در مورد گوشی تلفن همراه هم رعایت کنید.

فصل اول: آشنایی با مفاهیم امنیت اطلاعات
فصل دوم: امنیت فیزیکی و محیطی
فصل سوم: تهدیدات امنیتی در شبکه های رایانه‌ای
فصل چهارم: امنیت در مقابله با تهدیدات فضای سایبری
فصل پنجم: امنیت تجهیزات قابل حمل

فصل ششم

توصیه های امنیتی در خدمات بانکی

جلسه دوازدهم:
امنیت در کاربرد کارت های بانکی و خریدهای اینترنتی

جلسه سیزدهم:
امنیت بانکداری اینترنتی و همراه بانک

فصل هفتم:
جرایم رایانه‌ای و تعهدنامه عدم افشای اطلاعات
فصل هشتم:
پیاده سازی امنیت در سازمان ها

جلسه دوازدهم

امنیت در کاربرد کارت های بانکی و خرید های اینترنتی

۱۸۷	اهداف یادگیری
۱۸۸	پیش آزمون
۱۹۰	امنیت در کاربرد کارت های بانکی و خرید های اینترنتی
۱۹۲	ملاحظات امنیتی در کاربرد کارت های بانکی
۱۹۲	ملاحظات امنیتی در استفاده از دستگاه های خودپرداز (ATM) و پایانه های فروش (POS)
۱۹۷	ملاحظات امنیتی در درگاه های پرداخت اینترنتی و خرید اینترنتی
۱۹۸	میزان دستیابی به اهداف یادگیری
	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با ملاحظات امنیتی در کاربرد کارت‌های بانکی آشنا شود.
۲. با ملاحظات امنیتی در استفاده از دستگاه‌های خودپرداز (ATM) و پایانه‌های فروش (POS) آشنا شود.
۳. با ملاحظات امنیتی در درگاه پرداخت اینترنتی و خرید اینترنتی آشنا شود.

پیش‌آزمون جلسه دوازدهم :

۱. کدامیک از جملات زیر صحیح نمی‌باشد؟

الف) هرگز رمز اول و دوم کارت بانکی خود را بر روی کاغذ یا رسید چاپی بانک یادداشت نکنید.

ب) از در اختیار گذاشتن کارت بانکی خود به دیگران اجتناب نمایید.

ج) از انتخاب رمز قابل حدس نظیر سال تولد، سال ازدواج، شماره شناسنامه و ...، برای رمز اول و دوم کارت بانکی خود اجتناب نمایید.

د) می‌توانید برای راحتی خود، رمزهای مشابه برای کارت‌ها و سامانه‌های بانکی انتخاب نمایید.

۲. کدامیک از جملات زیر صحیح نمی‌باشد؟

الف) جهت انتقال وجه صرفاً اعلام شماره حساب ویا شماره کارت به فرد واریز کننده وجه کفایت می‌کند و نیازی به ارائه رمز اول و دوم، CVV۲ یا تاریخ انقضای کارت نمی‌باشد.

ب) هنگام خرید از طریق پایانه های فروش، رمز کارت بانکی خود را فقط در اختیار فروشنده قرار دهید.

ج) از پذیرش درخواست افراد ناشناس جهت استفاده از کارت بانکی شما به‌عنوان واسط (نظیر انتقال وجه) اجتناب نمایید.

د) در صورت صدور آنی کارت، شخصاً نسبت به ثبت رمز خود از طریق کارتخوان‌های شعبه‌ای اقدام نمایید.

پاسخ‌نامه

پیش‌آزمون جلسه دوازدهم

:

	الف	ب	ج	د
۱				
۲				

امنیت در کاربرد کارت‌های بانکی و خریدهای اینترنتی

:

در دنیـای کنونـی بـا افزایـش تعـداد کاربـران اینترنـت، اکـثر مـردم بـرای انجـام امـور گوناگـون، از امـور آموزشـی و تفریـح و سرگرمـی گرفتـه تـا امـور اداری و تجـاری، از بسـتراینترنت اسـتفاده می‌کننـد و همـه چیـز رنـگ و بـوی اینترنتـی بـه خـود گرفتـه اسـت و افـراد زیـادی بـرای رفـع نیازهـای روزمـره خـود و خریدهـای روزانـه از طریـق خریـد اینترنتـی اقـدام کـرده و در وقـت و هزینـه خـود نیـز صرفـه جویـی مـی کننـد.

امـروزه افـراد می‌تواننـد بـه راحتـی و بـدون تـرک محـل سـکونت خـود بـه هـزاران فروشـگاه اینترنتـی دسترسـی داشـته باشـند و هـر محصولـی کـه مـورد نیازشـان اسـت را فقـط بـا اطلاعـات یـک کارت بانکـی و بـا بـاز کـردن صفحـه وب سـایت فروشـگاه اینترنتـی مـورد نظـر خریـداری نماینـد و یـا بـدون نیـاز بـه همـراه داشـتن مقـدار زیـادی وجـه نقـد و خطـرات احتمالـی جابـه جایـی آن، فقـط بـا در دسـت داشـتن یـک کارت بانکـی، از طریـق پایانه‌هـای فـروش (POS) خریدهـای خـود را انجـام دهنـد.

بـا توجـه بـه گسـترش اسـتفاده از ایـن گونـه کاربردهـای کارت هـای بانکـی و بسـترهای خریدهـای اینترنتـی، یکـی از مشـکلات مهـم در ایـن مقولـه بـی اطـلاع کاربـران از نـکات سـاده و در عیـن حـال مهمـی اسـت کـه سـبب می‌شـود خریـد اینترنتـی یـا خریـد از طریـق پایانـه هـای فـروش (POS) بـه منبعـی بـرای سـودجویان جهـت سـوء اسـتفاده از حسـاب هـای بانکـی کاربـران تبدیـل شـود. لـذا، توجـه بـه ملاحظـات امنیتـی در هنـگام خریدهـای اینترنتـی و اسـتفاده از کارت‌هـای بانکـی امـری ضروری جهـت پیشـگیری از وقـوع سـوء اسـتفاده هـای احتمالـی اسـت .

ملاحظات امنیتی در کاربرد کارت‌های بانکی

:

بـا توجـه بـه اینکـه کارت‌هـای بانکـی، مـورد اسـتفاده خیلـی از افـراد در سرتاسـر دنیـا قـرار دارد واین کارت هـا توانسـته‌اند بـه خوبـی جـای پـول نقـد را بگیرنـد، بنابرایـن، رعایـت نـکات امنیتـی در اسـتفاده از ایـن کارت‌هـا بسـیار حائـز اهمیـت می‌باشـد. در ایـن زمینـه بانـک هـا در راسـتای آگاهـی رسـانی بـه مشـتریان خـود، عمومـاً از روش هـای متـداول نظیـر انتشـار بروشـورهای کاربـری و امنیتـی تـا حـد ممکـن سـعی مـی کننـد ، دانـش و آگاهـی مشـتریان خـود را در ایـن حـوزه افزایـش دهنـد. لـذا توجـه بـه ایـن پیـام هـا و توصیـه هایـی کـه از سـوی بانـک هـا ارائـه مـی شـوند ، ضمـن افزایـش سـطح آگاهـی افـراد ، در اسـتفاده امـن از خدمـات کارت هـا و خریدهـای غیرحضـوری تأثیـر بـه سـزایی دارد.

شـما به‌عنـوان یکـی از اسـتفاده‌کنندگان ایـن کارت‌هـا، زمانـی کـه بـه بانـک خـود درخواسـت دریافـت کارت بانکـی می‌دهیـد، بایـد هنـگام دریافـت پاکـت محتـوی رمـز کارت بانکـی خـود، از بـاز و مخـدوش نبـودن آن اطمینـان حاصـل نمـوده و در صـورت مخـدوش بـودن مسـئول شـعبه دریافـت کننـده کارت را مطلـع نماییـد. در صورتـی کـه صـدور کارت شـما به‌صـورت آنـی توسـط بانـک صـورت می‌گیـرد، شـخصاً نسـبت بـه ثبـت رمـز خـود از طریـق کارتخوان‌هـای شـعبه صـادر کننـده بانـک اقـدام نماییـد.

بلافاصلـه پـس از دریافـت کارت ، شـماره کارت خـود را در جایـی یادداشـت نماییـد تـا در صـورت مفقـودی یـا سرقـت آن بتوانیـد بـا مراجعـه بـه شـعب بانـک صادرکننـده کارت و یـا از طریـق سـامانه بانکـداری اینترنتـی آن را غیرفعـال کنیـد. همچنیـن بعـد از دریافـت کارت خـود، رمـز اول و دوم آن را از طریـق دسـتگاه خودپـرداز (ATM) تغییـر دهیـد و هرگـز رمزهـای کارت بانکـی خـود را در اختیـار دیگـران قـرار ندهیـد و آن را در فواصـل زمانـی (حداقـل هـر سـه مـاه) و بنـا بـه ضرورت تغییـر دهیـد. هرگـز رمزهـای کارت بانکـی خـود را بـر روی کارت خـود یـا بـر روی رسـیدهای چاپـی خودپـرداز یادداشـت نکنیـد.

اطلاعـات کارت بانکـی را اگرچـه بنـا بـه ضرورت و بـرای انتقـال پـول ممکـن اسـت در اختیـار دیگـران قـرار دهیـد امّـا همـواره بـه ایـن نکتـه توجـه داشـته باشـید کـه اطلاعـات کارت بانکـی در زمـره اطلاعـات شـخصی و مهـم مـی باشـد، پـس اطلاعـات کارت بانکـی خـود را در اختیـار افـراد غیـر و ناشـناس قـرار ندهیـد و از پذیـرش درخواسـت افـراد ناشـناس جهـت اسـتفاده از کارت بانکـی شـما به‌عنـوان واسـط (نظیـر انتقـال وجـه) اجتنـاب کنیـد.

هرگـز اطلاعـات مهـم خـود را ماننـد رمزهـای کارت‌هـای بانکـی، کلمـه عبـور سـامانه‌های بانکـی، کـد اعتبارسـنجی (CVV۲) و تاریـخ انقضـای کارت بانکـی، بـر روی گوشـی تلفـن همـراه ذخیـره نکـرده یـا اطلاعـات خـود را از طریـق پیامـک، ایمیـل و سـایر سـامانه‌های ارتباطـی مشـابه و شـبکه هـای اجتماعـی، متصـل بـه لینـک هـای ارتباطـی اینترنتـی را بـرای سـایرین ارسـال

و بازگـو نکنیـد.

شکل۱: نمایی از صفحات پشت و روی کارت بانکی بانک ملت

سـعی کنیـد از انتخـاب رمزهـای قابـل حـدس نظیـر سـال تولـد، سـال ازدواج، شـماره شناسـنامه و غیـره و همچنیـن از انتخـاب رمزهـای مشـابه بـرای کارت‌هـا و سـامانه‌های بانکـی مختلـف خـود اجتنـاب کنیـد.

بـه ایـن نکتـه توجـه داشـته باشـید کـه بانـک هرگـز اطلاعـات محرمانـه شـما (نظیـر مشـخصات شناسـنامه‌ای، کدملـی، اطلاعـات مربـوط بـه کارت و حسـاب بانکـی و ...) را از طریـق تلفـن، ایمیـل یـا پیامـک و شـبکه هـای اجتماعـی، پیشـنهاد اتصـال بـه لینـک هـای ارتباطـی اینترنتـی و... از شـما درخواسـت نمی‌کنـد پـس، درصـورت مواجـه شـدن بـا ایـن مـورد، ضمـن عـدم پاسـخگویی بـه چنیـن درخواسـت‌هایی، بانـک را از موضـوع مطلـع کنیـد.. همچنیـن در نظـر داشـته باشـید کـه جهـت انتقـال وجـه صرفاً اعـلام شـماره حسـاب ویـا شـماره کارت بـه فـرد واریـز کننـده وجـه، کفایـت می‌کنـد و نیـازی بـه ارائـه رمـز اول و دوم، CVV۲ یـا تاریـخ انقضـای کارت شـما نمی‌باشـد.

همچنیـن بانـک هـا بـا ایجـاد امکانـات غیـر حضـوری سـعی در تسـهیل درخواسـت هـای مشـتریان خـود دارنـد، مثـلاً می‌توانیـد بـا مراجعـه بـه سـامانه بانکـداری اینترنتـی بانـک خـود، نسـبت بـه مدیریـت کارت هـای بانکـی و دریافـت خدماتـی نظیـر غیرفعـال نمـودن کارت، اتصـال یـا قطـع حسـاب‌های فرعـی، دریافـت رمـز دوم و ...، اقـدام کنیـد.

ملاحظات امنیتی در استفاده از دستگاه‌های خودپرداز(ATM) و پایانه‌های فروش(POS)

:

هنـگام اسـتفاده از دسـتگاه خودپـرداز یـا پایانه‌هـای فـروش نیـز لازم اسـت نـکات امنیتـی را رعایـت کنیـم. بـه ایـن نکتـه توجـه داشـته باشـید کـه در هنـگام اسـتفاده از دسـتگاه خـود پـرداز حداقـل فاصلـه سـایرین بـا شـما (حـدود یـک مـتر) رعایـت شـود و همچنیـن شـما نیـز ایـن فاصلـه را هنـگام اسـتفاده دیگـران، رعایـت کنیـد. سـعی کنیـد هنـگام خریـد از طریـق پایانـه هـای فـروش، شـخصاً نسـبت بـه ورود رمـز کارت بانکـی خـود اقـدام نماییـد و رمـز خـود را بلنـد و بـه دیگـران اعـلام نکنیـد.

تـا حـد امـکان در هنـگام اسـتفاده از دسـتگاه خودپـرداز یـا پایانه‌هـای فـروش، از عـدم نصـب تجهیـزات اضافـی بـر روی آن هـا و نبـود دوربین‌هـای غیرمجـاز در اطـراف آن‌هـا، اطمینـان حاصـل کنیـد، چـون ممکـن اسـت ایـن تجهیـزات قصـد ثبـت و ضبـط اطلاعـات رمـز شـما را حیـن وارد کـردن داشـته باشـند تـا بتواننـد از کارت شـما سوءاسـتفاده کننـد.

در صورتـی کـه کارت بانکـی شـما توسـط دسـتگاه خودپـرداز ضبـط شـود، شـما بـا پیغـام "خـارج ازسرویـس شـدن خودپـرداز" یـا "ارائـه رسـید توسـط خودپـرداز مبنـی بـر ضبـط کارت" مواجـه می‌شـوید، در غیـر ایـن صـورت تـا حصـول اطمینـان از ضبـط

کارت و یـا بیـرون آمـدن کارت از دسـتگاه، محـل خودپـرداز را تـرک نکنیـد.
دقـت داشـته باشـید کـه بـرای انتقـال وجـه از طریـق خودپـرداز، نیـازی بـه اسـتفاده از زبـان انگلیسـی نیسـت، بنابرایـن، مراقـب ترفندهـای مهندسـی اجتماعـی کلاهـبرداران بـا اسـتفاده از ایـن قابلیـت باشـید. همچنیـن تـا حـد امـکان سـعی کنیـد شـب‌ها بـه خودپردازهایـی کـه در محل‌هـای کـم رفـت وآمـد و تاریـک هسـتند، مراجعـه نکنیـد.

ملاحظات امنیتی در درگاه های پرداخت اینترنتی و خرید اینترنتی

:

درگاه پرداخـت اینترنتـی درگاهـی اسـت کـه عملکـرد آن مشـابه بـا پایانـه هـای فـروش (POS) امـا از بسـتر اینترنـت مـی باشـد، یعنـی امـکان انجـام عملیـات پرداخـت را بـدون حضـور کارت و از طریـق اینترنـت، فراهـم مـي نمایـد و از طریـق آن دارنـدگان همـهٔ کارت‌هـای بانکـی می‌تواننـد بـا اسـتفاده از مشـخصات کارت بانکـی خـود شـامل شـماره کارت، رمـز دوم، تاریـخ انقضـا و کـد اعتبـار سـنجی (CVV۲) نسـبت بـه خریـد کالا یـا خدمـات به‌صـورت الکترونیـک از طریـق درگاه‌هـای پرداخـت اینترنتـی قابـل دسـترس از طریـق وب سـایت هـای فـروش کالا یـا خدمـات اقـدام نماینـد. همانطـور کـه در فصـول قبلـی مطـرح شـد، امـکان سـوء اسـتفاده هـای احتمالـی از بسـتر اینترنـت بـا روش هـای مختلـف مـورد توجـه هکرهـا قـراردارد. پـس، اسـتفاده از درگاه هـای پرداخـت اینترنتـی هـم نظیـر سـایر حـوزه هـای بانکـی ، ضرورتـاً نیازمنـد توجـه بـه نـکات امنیتـی در هنـگام اسـتفاده از آن می‌باشـد.

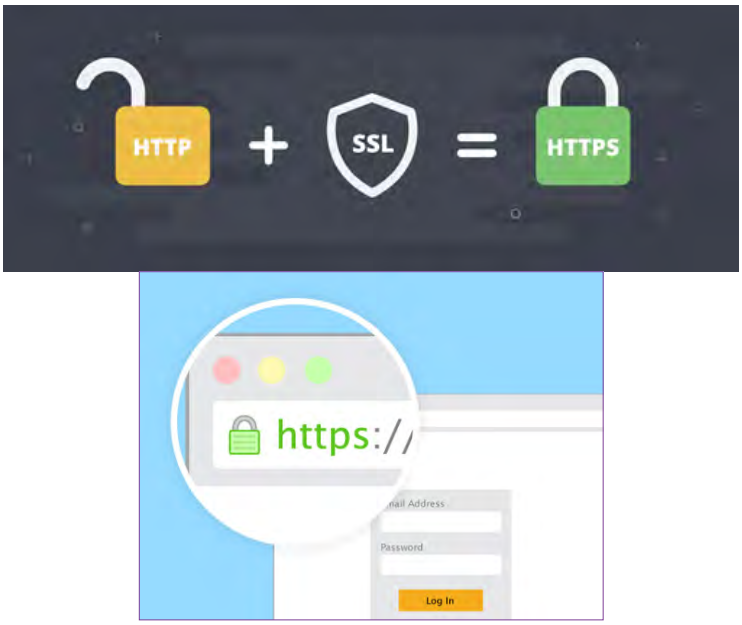
شکل ۲: نمایی از درگاه پرداخت اینترنتی بانک ملت

بهـتر اسـت تـا حـد ممکـن از رایانـه هـای موجـود در مـکان هـای عمومـی (مثـل کافـی نـت هـا)، رایانـه هـای ناشـناس و شـبکه هـای بـی سـیم عمومـی دسترسـی بـه اینترنـت بـرای خریدهـای اینترنتـی اسـتفاده نکنیـد. بـه عبـارت دیگـر، سـعی کنیـد، تـا آنجـا کـه امـکان دارد خریـد هـای اینترنتـی خـود را از طریـق رایانـه شـخصی خـود انجـام دهیـد و پیـش از اقـدام بـه خریـد اینترنتـی، همـواره از عـدم نصـب ابزارهـای کلیدنـگار در نقـش سرقـت کلمـه(key logger) سـخت‌افزاری و نرم‌افـزاری بـر روی رایانـه اطمینـان حاصـل نماییـد.. همچنیـن از بـه روزرسـانی مسـتمر سیسـتم‌عامل، مرورگـر وب و سـایر نرم‌افزارهـای نصـب شـده روی رایانـه، تبلـت و گوشـی تلفـن همـراه خـود مطمئـن شـوید. رایانـه، تبلـت و گوشـی تلفـن همـراه خـود را بـه ضدویـروس معتـبر مجهـز کـرده و آن را بـه صـورت مسـتمر بـه روزرسـانی نماییـد. از دریافـت(Download) و اجـرای نرم‌افـزار و فایل‌هـای ناشـناس و متفرقـه روی رایانـه، تبلـت و گوشـی تلفـن همـراه خـود اجتنـاب نماییـد.
بـه ایمیل‌هـا و پیام‌هـاي ناشـناس و مشـکوک مبنـي بـر ورود بـه حسـاب اینترنتـي خـود توجـه نکنیـد و توجـه داشـته باشـید کـه صفحاتـی کـه ناخواسـته در صفحـات وب در برابـر شـما بـاز می‌شـوند (Pop-up) و حـاوی تبلیغـات فـروش کالاهـا و ارائـه خدمـات هسـتند، ممکـن اسـت تقلّبـی بـوده و قصـد کلاهـبرداری داشـته باشـند، پـس ترجیحـاً از ایـن صفحـات خریـد اینترنتـی انجـام ندهیـد.
ایـن نکتـه را بدانیـد کـه مرکـز توسـعه تجـارت الکترونیـک وزارت بازرگانـی، بـا همـکاری نیـروی انتظامـی جمهـوری اسـلامی

ایـران در جهـت افزایـش امنیـت خدمـات تجـارت الکترونیـک، اقـدام بـه اعطـای نمـاد اعتـماد الکترونیکـی (e-namad) بـه فروشـگاه‌های اینترنتـی نمـوده اسـت تـا خریـداران بـه راحتـی و بـا آسـودگی خاطـر، خریـد خـود را انجـام دهنـد. پـس ترجیحـاً از وب سـایت فروشـگاه‌هایی کـه دارای ایـن نمـاد هسـتند، خریـد کنیـد.

شکل ۳: نماد اعتماد الکترونیکی

تمامـی سـایت‌های معتـبر و مهـم کـه تراکنش‌هـای مالـی انجـام می‌دهنـد، دارای نشـانگرهای امنیتـی (SSL و HTTPS) می‌باشـند. لـذا جهـت انجـام خریـد اینترنتـی، قبـل از ورود اطلاعـات در وب‌سـایت درگاه پرداخـت اینترنتـی، از وجـود ایـن نشـانگرهای امنیتـی و معتـبر بـودن وب‌سـایت مذکـور اطمینـان حاصـل نماییـد و دقـت کنیـد کـه حتـماً آدرس صفحـه درگاه پرداخـت الکترونیـک، متعلـق بـه هـمان بانکـی باشـد کـه آرم و لوگـوی آن را در صفحـه مشـاهده می‌کنیـد. همانطـور کـه در فصـل هـای قبلـی اشـاره شـد ، در بعضـی مواقـع، کلاهـبرداران بـا جعـل صفحـات درگاه پرداخـت الکترونیـک بانک‌هـا ، شـما را بـه صفحاتـی هدایـت می‌کننـد کـه آدرسـی بسـیار شـبیه بـه آدرس بانـک اصلـی دارنـد. در صـورت بـی دقتـی خریـدار و ورود اطلاعـات کارت بانکـی وی، اطلاعـات خریـدار را در سیسـتم خـود ثبـت کـرده و عمـلاً امـکان هرگونـه اقـدام وسـوء اسـتفاده ازحسـاب و موجـودی او را خواهنـد داشـت.



شکل ۴ : درگاه پرداخت اینترنتی

جهـت ورود مشـخصات کارت بانکـی خـود در درگاه پرداخـت اینترنتـی ، ترجیحـاً از صفحـه کلیـد مجـازی تعبیـه شـده در سـایت مربوطـه اسـتفاده نماییـد.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- با ملاحظات امنیتی در کاربرد کارت‌های بانکی آشنا شدید.	
۲- با ملاحظات امنیتی در استفاده از دستگاه‌های خودپرداز (ATM) و پایانه‌های فروش (POS) آشنا شدید.	
۳- با ملاحظات امنیتی در درگاه پرداخت اینترنتی و خرید اینترنتی آشنا شدید.	

خودآزمایی جلسه دوازدهم :

۱. کدامیک از جملات زیر صحیح نمی‌باشد؟

الف) از بـه روزرسـانی مسـتمر سیسـتم عامـل، مرورگـر وب و سـایر نرم‌افزارهـای منصـوب روی رایانـه، تبلـت و گوشـی تلفـن همـراه خـود اطمینـان حاصـل نماییـد.

ب) رایانـه، تبلـت و گوشـی تلفـن همـراه خـود را بـه ضدویـروس معتـبر مجهـز نمـوده و آن را بـه صـورت مسـتمر بـه روزرسـانی نماییـد.

ج) جهـت ورود مشـخصات کارت بانکـی خـود در درگاه پرداخـت اینترنتـی، ترجیحـاً از صفحـه کلیـد کیبـورد اسـتفاده نماییـد.

د) به ایمیل‌ها و پیام‌هاي ناشناس و مشکوک مبني بر ورود به حساب اینترنتي خود توجه نکنید.

۲. کدامیک از جملات زیر صحیح نمی‌باشد؟

الـف) در صورتـی کـه بـرای انجـام امـور بانکـی از طریـق خودپـرداز مشـکلی داشـتید، از افـراد ناشـناس نزدیـک خودپـرداز کمـک بگیریـد.

ب) ترجیحاً از فروشگاه‌هایی که دارای نماد اعتماد الکترونیکی یا e-namad هستند، خرید کنید.

ج) مادامـي کـه از سـامانه بانکـداری اینترنتـی خـود خـارج نشـده ایـد، رایانـه خـود را تـرک نکنیـد و بعـد از پایـان کار خـود حتـماً بـا اسـتفاده از گزینـه خـروج از سـامانه خـارج شـوید.

د) در هنـگام خریـد اینترنتـی دقـت کنیـد کـه حتـماً آدرس صفحـه درگاه پرداخـت الکترونیـک، متعلـق بـه هـمان بانکـی باشـد کـه آرم و لوگـوی آن را در صفحـه مشـاهده می‌کنیـد.

۳. کدام مورد جزو پارامترهای کنترلی امنیتی کارت بانک محسوب نمی شود؟

الف) رمز اول کارت

ب) کد اعتبار ستجی (CVV۲)

ج) تاریخ انقضای کارت

د) شماره ۱۶ رقمی کارت

۴. کدام گزینه در مورد رمز کارت های بانکی باید بیشتر مورد توجه قرار گیرد؟

الف) پاکت محتوی رمز کارت بانکی ، نباید باز و یا مخدوش باشد.

ب) از انتخاب رمزهای قابل حدس نظیر سال تولد، سال ازدواج، شماره شناسنامه اجتناب شود.

ج) از انتخاب رمزهای مشابه برای کارت‌ها و سامانه‌های بانکی اجتناب شود.

د) همه موارد به یک اندازه دارای اهمیت می باشند.

پاسخ‌نامه تشریحی

خودآزمایی جلسه دوازدهم

:

۱. پاسخ صحیح، گزینه «ج»
برای ورود مشخصات کارت بانکی خود در درگاه پرداخت الکترونیک، ترجیحاً از صفحه کلید مجازی تعبیه شده در سایت مربوطه استفاده نمایید.

۲. پاسخ صحیح، گزینه «الف»
از در اختیار گذاشتن کارت بانکی خود به دیگران اجتناب نمایید.
از پذیرش درخواست افراد ناشناس جهت استفاده از کارت بانکی شما به‌عنوان واسط (نظیر انتقال وجه) اجتناب نمایید.

۳. پاسخ صحیح، گزینه «د»
شماره ۱۶ رقمی کارت جزو دارایی های اطلاعاتی است اما جزو پارامترهای کنترلی امنیتی نیست.

۴. پاسخ صحیح، گزینه «د»
توجه به تمامی نکات مربوط به رمز کارت و سامانه های بانکی، دارای اهمیت یکسان می باشند.

جلسه سیزدهم

امنیت بانکداری اینترنتی و همراه بانک

۱۸۷	اهداف یادگیری
۱۸۸	پیش آزمون
۱۹۰	امنیت در کاربرد کارت های بانکی و خرید های اینترنتی
۱۹۲	ملاحظات امنیتی در کاربرد کارت های بانکی
۱۹۲	ملاحظات امنیتی در استفاده از دستگاه های خودپرداز (ATM) و پایانه های فروش (POS)
۱۹۷	ملاحظات امنیتی در درگاه های پرداخت اینترنتی و خرید اینترنتی
۱۹۸	میزان دستیابی به اهداف یادگیری
	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با نکات امنیتی در استفاده از خدمات بانکداری اینترنتی آشنا شود.
۲. با توصیه های امنیتی در استفاده از سامانه همراه بانک آشنا شود.
۳. با توصیه های امنیتی در استفاده از سامانه تلفن¬بانک آشنا شود.

پیش‌آزمون جلسه سیزدهم :

۱. کدامیک از جملات زیر صحیح می‌باشد؟

الف) توصیه می‌گردد برای کلمه عبور سامانه بانکداری اینترنتی، یک کلمه ساده و قابل حدس انتخاب کنید.

ب) کلمه عبور سامانه بانکداری اینترنتی خود را برای همیشه ثابت نگه دارید و آن را تحت هیچ شرایطی تغییر ندهید.

ج) هنگام ورود شناسه مشتری و کلمه عبور سامانه بانکداری اینترنتی، از دیده نشدن آن توسط دیگران اطمینان حاصل نمایید.

د) شناسه مشتری و کلمه عبور خود را برای اینکه فراموش نکنید، در جایی یادداشت و نگهداری کنید.

۲. کدامیک از جملات زیر صحیح نمی‌باشد؟

الف) از باز کردن ایمیل‌های ناشناس و پاسخ به نامه‌ای که در آن درخواست اطلاعات شخصی، مشخصات و جزئیات حساب بانکی، کارت بانکی و ...، را می‌نماید، اجتناب کنید.

ب) از ورود به وب‌سایت‌های متفرقه و بازنمودن لینک‌های مربوطه اجتناب نمایید.

ج) رایانه، تبلت و گوشی تلفن همراه خود را طوری تنظیم نمایید که در فواصل زمانی کوتاه با استفاده از روش های امنیتی نظیر (pattern,pin,password و...) قفل گردد.

د) در صورت نا توانایی در ورود به سامانه بانکداری اینترنتی از ابزارهای فیلتر شکن نظیر VPN استفاده نمایید.

۳. کدامیک از جملات زیر صحیح نمی‌باشد؟

الف) نرم‌افزار سامانه همراه بانک را می‌توانید از طریق مراجعه حضوری به شعب بانک و یا مراجعه مستقیم به وب‌سایت بانک به کمک روش‌هایی نظیر بلوتوث، ایمیل، وب‌سایت‌های متفرقه، فروشگاه‌های اینترنتی و وب‌سایت‌های ارائه‌دهنده نرم‌افزار، دریافت و نصب نمایید.

ب) رمز ورود سامانه همراه بانک خود را فقط در اختیار افراد درجه یک خانواده خود قرار دهید و هرگز آن را در اختیار دیگران قرار ندهید.

ج) رمز ورود سامانه همراه بانک ارائه شده توسط شعبه را پس از نصب کامل نرم‌افزار آن، در اولین فرصت تغییر دهید.

د) گزینه الف و ب

پاسخ‌نامه

پیش آزمون جلسه دوازدهم

:

	الف	ب	ج	د
۱				
۲				
۳				

نکات امنیتی در استفاده از سامانه بانکداری اینترنتی

:

هم زمان با سایر حوزه های مالی و کاربردی مبتنی بر اینترنت که در حال توسعه و مورد توجه افراد قرار دارند ، خدمات بانکداری اینترنتی هم به عنوان خدمت غیر حضوری ارائه دهنده بسیاری از خدمات بانکی، مورد توجه مشتریان بانکها وگسترش استفاده قراردارد و این امکان را برای افراد فراهم می‌آورد تا در وقت و هزینه خود صرفه جویی نمایند و بسیاری از امور بانکی خود را به صورت غیرحضوری از طریق این سرویس انجام دهند. با توجه به بستر مبتنی بر وب این خدمت، اکثر تهدیدات و آسیب پذیری های مطرح شده در فصول قبلی در این حوزه نیز مورد توجه و سوء استفاده مهاجمان و هکرها قرار دارد. پس، باید ملاحظات امنیتی لازم مورد توجه مشتریان و استفاده کنندگان آن قرار گیرد. علاوه بر این، ماهیت سامانه بانکداری اینترنتی به عنوان کانال ارائه دهنده اکثر خدمات بانکی مهم و مورد استفاده مشتریان، عملکردی در نقش یک شعبه مجازی دارد و توجه به جنبه های امنیتی آن را دو چندان می نماید. برای همین منظور، بانک ها اقدامات امنیتی ویژه ای را برای این خدمت عملیاتی نموده اند.

در اولین گام برای فعال‌سازی خدمات بانکداری اینترنتی با مراجعه به شعبه بانک مورد نظر، پاکتی حاوی شناسه مشتری و کلمه عبور سامانه بانکداری اینترنتی به شما تحویل داده می‌شود، در هنگام تحویل گرفتن این پاکت، از باز و مخدوش نبودن آن اطمینان حاصل نموده و در صورت مخدوش بودن، مسئول شعبه را مطلع نمایید. توصیه می شود به رغم الزام در تغییر رمز دریافتی از شعبه در نخستین ورود به سامانه بانکداری اینترنتی، شناسه مشتري خود را نیز به منظور افزایش ضریب امنیتی تغییر دهید. سعی کنید در انتخاب و بکارگیری رمز عبور از رمزهای قابل حدس و مشابه با سایر سامانه ها استفاده نکنید و همچنین به نکات امنیتی که قبلاً در مورد انتخاب رمز گفته شد نیز توجه کنید. اگر چه در برخی از بانک ها برای این سامانه حداقل های امنیتی انتخاب رمز عبور (طول کلمه عبور و میزان پیچیدگی آن) به عنوان پارامترهای اجباری در نظر گرفته شده است. همینطور رمز عبور سامانه بانکداری اینترنتی را در اختیار دیگران حتی کارکنان ونمایندگان بانک قرار ندهید.

صفحه کلید مجازی تعبیه شده در بخش های ورود اطلاعات (شناسه مشتری و کلمه عبور) این امکان را ایجاد می کند که احتمال سوء استفاده از طریق نصب ابزارهای کلیدنگار در نقش سرقت کلمه (KeyLogger) کاهش یابد، پس هنگام وارد نمودن شناسه مشتری و رمز عبور سامانه بانکداری اینترنتی خود، ترجیحاً از صفحه کلید مجازی تعبیه شده در سایت مربوطه استفاده کنید. همچنین هنگام ورود اطلاعات از دیده نشدن آن توسط دیگران مطمئن شوید. از یادداشت و ذخیره شناسه مشتری و رمز عبور سامانه بانکداری اینترنتی خود در جایی که امکان سوءاستفاده‌های آتی از حساب بانکی شما را برای یابنده آن فراهم می‌نماید، خودداری کنید.

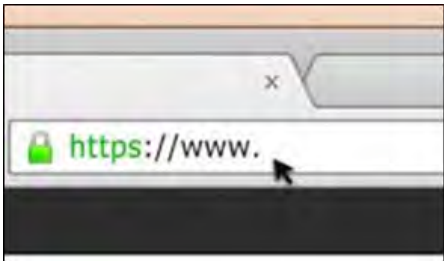
یکی از پارامترهای خاص پیش بینی شده برای خدمت بانکداری اینترنتی استفاده از یکبار رمز (OTP) است که بسته به سیاست های امنیتی مورد توجه بانک ها ممکن است به صورت اجباری و یا اختیاری به مشتریان ارائه شود. به عنوان مثال: استفاده از یکبار رمز در هنگام ورود به سامانه بانکداری اینترنتی برای مشتریان بانک ملت در خارج از کشور به صورت اجباری است درحالی که این امر در داخل کشور اختیاری است. در حال حاضر دریافت و استفاده از یکبار رمز از سه طریق توکن یکبار رمز ، یکبار رمز همراه (استفاده از تلفن همراه و بستر UUSD) و ارسال پیامک به تلفن همراه قابل انجام می باشد. با استفاده از یکبار رمز ، در واقع از روش احراز هویت دو عاملی استفاده می شود و راهکاری برای مقابله با سوء استفاده های احتمالی ناشی از سرقت شناسه مشتری و کلمه عبور می باشد. یکبار رمز ،کلمه عبوری است که با روش های رمزنگاری تولید و اعتبار آن برای مدتی کوتاه است (مثلاً یک دقیقه) و فقط یکبار استفاده می شود. پس توصیه می شود جهت افزایش امنیت سامانه بانکداری اینترنتی خود، جهت ورود به سامانه و انجام تراکنش‌های مالی از یکبار رمز استفاده کنید. استفاده از یکبار رمز در هنگام ورود به سامانه احتمال سوء استفاده از طریق حمله فیشینگ را تقریباً نا ممکن می سازد.

شکل ۵: نمایی از دستگاه تولید یکبار رمز (OTP)

بهتر است تا حد ممکن، رایانه های موجود در مکان های عمومی (مثل کافی نت ها)، رایانه های ناشناس و شبکه های بی سیم عمومی دسترسی به اینترنت را برای استفاده از سامانه بانکداری اینترنتی بکار نگیرید و در صورت استفاده، حتماً در اولین فرصت ممکن رمزعبور خود را تغییر دهید. به عبارت دیگر، سعی کنید، در صورت امکان، ورود به سامانه بانکداری اینترنتی را از طریق رایانه شخصی خود انجام دهید و در زمان دسترسی به سامانه بانکداری اینترنتی مطمئن شوید که از ابزارهای فیلتر شکن نظیر VPN استفاده نمی کنید. همینطور از ذخیره رمز عبور در مرورگر وب خوداری کنید، اگرچه این ویژگی برای سهولت کاربری و عدم تکرار درج اطلاعات پیش بینی شده است امّا ذخیره اطلاعات شخصی از جمله اطلاعات شناسه کاربری و رمز عبور سامانه های مالی و سایر سامانه های مهم به لحاظ نقض پارامترهای امنیتی، هرگز توصیه نمی شود. علاوه براین از عدم نصب ابزارهای کلید نگار در نقش سرقت کلمه(key logger) سخت افزاری و نرم افزاری بر روی رایانه اطمینان حاصل نمایید. همچنین از به روزرسانی مستمر سیستم عامل، مرورگر وب و سایر نرم افزارهای نصب شده روی رایانه، تبلت و گوشی تلفن همراه خود مطمئن شوید. رایانه، تبلت و گوشی تلفن همراه خود را به نرم افزار ضدویروس معتبر مجهز نموده و آن را به صورت مستمر به روزرسانی نمایید. از دریافت(Download) و اجرای نرم افزار و فایل های ناشناس و متفرقه روی رایانه، تبلت و گوشی تلفن همراه خود اجتناب کنید.

به یاد داشته باشید که بانک از کانال هایی نظیر پست الکترونیک و پیامک شما را ترقیب به ورود به سامانه بانکداری اینترنتی نمی کند، پس، در صورت مواجه شدن با چنین موضوعاتی هوشیار باشید و ترجیحاً بانک مرجع را از موضوع مطلع کنید. همینطور از باز کردن پست الکترونیک ناشناس و پاسخ به نامه‌ای که در آن درخواست اطلاعات شخصی، مشخصات و جزئیات حساب بانکی، کارت بانکی و ...، را می نماید، امتناع کنید.

جهت کاهش اشتباه و مصون ماندن از سوء استفاده، برای استفاده از سامانه بانکداری اینترنتی صرفاً از طریق مراجعه مستقیم به وب‌سایت بانک مورد نظر اقدام کنید. همچنین توصیه می‌شود برای امنیت بیشتر، وب‌سایت بانک را با تایپ نمودن نشانی اینترنتی (URL) آن در نوار آدرس (Address bar) مرورگر وب، مشاهده نمایید.



شکل۶: نوار آدرس مرور گر وب

از باز کردن ایمیل‌های ناشناس و پاسخ به نامه‌ای که در آن درخواست اطلاعات شخصی، مشخصات و جزئیات حساب بانکی، کارت بانکی و ...، را می نماید، امتناع کنید.

رایانه، تبلت و گوشی تلفن همراه خود را طوری تنظیم نمایید که در فواصل زمانی کوتاه با استفاده از روش‌های امنیتی (PIN, Pattern, Password و ...) قفل شوند. همینطور در زمان کار با سامانه بانکداری اینترنتی چنانچه برای مدت کوتاهی نیز رایانه خود را ترک می کنید پنجره ورود به سیستم را قفل کرده و هنگام پایان کار با سامانه بانکداری اینترنتی، حتماً با استفاده از کلید خروج تعبیه شده در صفحه، از سامانه خارج شوید.

ارسال پیامک و ایمیل جهت ورود به سامانه بانکداری اینترنتی و یا انجام تراکنش‌های مالی، امکانی است که توسط بانکها دراختیار مشتریان قرار می گیرد تا سبب آگاهی مشتری از سوءاستفاده احتمالی و جلوگیری از سوءاستفاده های بیشتر شود. پس، به محض دریافت چنین پیامک‌ها و ایمیل‌هایی، در صورتی که عمل مذکور از سوی خودتان انجام نشده، نسبت به تغییر رمزعبور خود اقدام و مراتب را در اسرع وقت به مرکز ارتباط بانک اطلاع‌رسانی کنید. همچنین از صحت اطلاعات تماس خود (شماره تلفن همراه و آدرس پست الکترونیک) در سامانه بانکداری اینترنتی مطمئن شوید و در صورت تغییر اطلاعات مزبور به ویژه تغییر شماره تلفن همراه، حتماً در اولین فرصت ممکن به کمک روشهای غیرحضوری که بانک در اختیار مشتریانش گذاشته است یا مراجعه به شعبه نسبت به، به روزرسانی آن‌ها اقدام نمایید. همینطور به این نکته توجه داشته باشید که نباید اطلاعات مربوط به حساب و کارت بانکی خود را در شبکه‌های اجتماعی قرار دهید.

ملاحظات امنیتي غیرفعال سازي خدمات بانکداري اینترنتي: درصورت بروز سوء استفاده اینترنتی بر روی حساب های

شما یا ورود غیرمجاز به سامانه بانکداری اینترنتی یکی از اقدامات ذیل را در اسرع وقت انجام دهید :

۱. اطلاع موضوع به مرکزارتباط ملت ودرخواست غیرفعال سازی سامانه

۲. مراجعه حضوری به یکی از شعب بانک ملت و درخواست غیرفعال سازی سامانه

۳. استفاده نمودن از قابلیت "فعال/غیرفعال نمودن خدمات الکترونیک"موجود در سایت بانکداری اینترنتی به منظور غیرفعال نمودن خدمات سامانه نظیر مشاهده گردش حساب، انواع حواله و...

نکات امنیتی در استفاده از سامانه همراه بانک

:

امروزه داشتن یک تلفن همراه ، صرفاً به منظور برقراری ارتباط با سایرین نیست، بلکه قابلیت های تعبیه شده بر روی گوشی،آن را تبدیل به یک رایانه همراه کرده است و قابلیت های آن سبب شده تولید نرم افزارهای کاربردی در حوزه های مختلف با ویژگی های مناسب استفاده در صفحه چند اینچی تلفن همراه تبدیل به یک حرفه شود و بازارهای متعددی جهت ارائه محصولات مختلف را ایجاد کرده است. با کمی جستجو می بینیم که از نرم افزارهای خاص پیش بینی آب و هوا ، کالری شمار ، تایپ و انواع بازی ها گرفته تا انواع نرم افزارهای تخصصی مالی ، صنعتی ، هنری و .... ، سازگار با انواع سیستم عامل های تلفن های هوشمند تولید وارائه شده اند. ویژگی خاص این نرم افزارها که عموماً با واژه اپلیکیشن نام برده می شود ، سهولت در استفاده و سادگی و نداشتن پیچیدگی در ظواهر و کاربری آنهاست ، لذا، امروزه خیلی افراد ممکن است با دانش و توانایی کار با رایانه آشنا نباشند امّا به خوبی می توانند با اپلیکیشن های منصوب در گوشی تلفن همراه خود بسیاری از فعالیت های حرفه ای از ویرایش یک تصویر تا فعالیت در رسانه های اجتماعی و یا کار با سامانه های مختلف را انجام دهند. نفوذ این ابزارها در زندگی روزمره و نیاز و تمایل اکثر افراد به دسترسی گوشی تلفن همراه به اینترنت باعث شده است گوشی تلفن همراه که روزی صرفاً یک ابزار ارتباط صوتی و متنی بود، مانند یک رایانه مورد توجه هکرها قرار بگیرد و به همین ترتیب حفظ امنیت اطلاعات موجود در آن برای کاربران آن ضروری باشد. پس، بسیاری از ملاحظاتی را که در مورد رایانه خود نظیر بروزرسانی سیستم عامل ، نصب نرم افزارهای معتبر ، عدم دانلود فایل های ناشناس و ... ، مورد توجه قرار می دهید، لازم است در مورد گوشی تلفن همراه هم رعایت کنید.

با توصیفی که از کاربردهای اپلیکیشن های تلفن همراه گفته شد، بانک ها نیز با تولید نرم افزار سازگار با تلفن های هوشمند، دسترسی و استفاده از خدمات غیر حضوری بانکی را میسر و تسهیل نموده اند که با واژه "همراه بانک" نامبرده می شود. با داشتن تنها یک گوشی تلفن همراه هوشمند و نصب و راه اندازی نرم افزار "همراه بانک" می توانید در هر زمان از شبانه روز به اطلاعات حساب بانکی خود دسترسی یافته و بسیاری از خدمات بانکی را از طریق آن انجام دهید.با آنچه که پیش از این در مورد اهمیت تلفن همراه بخاطر کاربردهای آن گفته شد از یک سو و از سوی دیگر چنانچه قصد دارید از سامانه همراه بانک استفاده کنید یا از آن استفاده می کنید، برای مصون ماندن از سوءاستفاده های احتمالی همهٔ ملاحظات امنیتی را می بایست هوشیارانه مدنظر قرار داد.

جهت فعال سازی سامانه همراه بانک، با مراجعه به شعبه بانک مورد نظر، پاکتی حاوی رمز ورود به سامانه همراه بانک به شما تحویل داده می شود، در هنگام تحویل گرفتن این پاکت، از باز و مخدوش نبودن آن اطمینان حاصل نموده و در صورت مخدوش بودن مسئول شعبه را مطلع نمایید. جهت نصب سامانه همراه بانک، صرفاً از طریق مراجعه حضوری به شعب بانک مورد نظر و یا مراجعه مستقیم به وب سایت بانک، نرم افزار همراه بانک را دریافت و بر روی تلفن همراه خود نصب نمایید و هرگز از طریق روش های غیرمعتبر نظیر بلوتوث (به غیر از سامانه بلوتوث شعب بانک)، پست الکترونیک، وب سایت های متفرقه، فروشگاه های اینترنتی متفرقه ارائه دهنده نرم افزارهای موبایل اقدام به دریافت و نصب آن ننمایید. قطعاً بانک مرجع نحوه دریافت نسخه سامانه همراه بانک را بر اساس نوع سیستم عامل گوشی های تلفن (مثلاً IOS ، Android و یا Windows) ، از طریق راهنماهای منتشر شده مرتبط در وب سایت بانک، افراد آگاه مستقر در شعبه و یا مرکز ارتباط بانک را در اختیار مشتریان خود قرار می دهد ، پس، دریافت ، نصب و به روزرسانی نسخه سامانه همراه بانک را مطابق منبع دریافت نرم افزار و نحوه نصبی که بانک به شما اعلام می کند انجام دهید. همچنین در صورت ارائه نسخه جدید نرم افزار سامانه همراه بانک، در اولین فرصت نرم افزار مزبور را بر روی گوشی تلفن همراه خود ارتقای دهید.

رمز ورود به سامانه همراه بانک ارائه شده توسط بانک را پس از نصب کامل نرم افزار ، در اولین فرصت تغییر دهید.

در انتخاب و بکارگیری رمز ورود جدید به نکات امنیتی که پیش از این به آن اشاره شد، توجه داشته باشید ضمن اینکه رمز سامانه را در اختیار دیگران نمی گذارید، سعی کنید از انتخاب رمز ورود قابل حدس مشتمل بر سال تولد، سال ازدواج،شماره شناسنامه و...، براي ورود به سامانه همراه بانك خود، اجتناب کنید و در فواصل زمانی مناسب مثلاً حداقل هر سه ماه رمز عبور را تغییر دهید. نام کاربری خود را نیز به منظور افزایش ضریب امنیتی پس از نصب کامل نرم افزار، در اولین فرصت تغییرداده و در محل امن نگهداری نمایید. از آنجایی که تکنولوژی تلفن های همراه رو به تغییر و افزایش قابلیت های امنیتی هستند، بانک ها نیز سعی در سازگاری و بهره گیری از این قابلیت های جدید دارند. به طور مثال: قابلیت استفاده از اسکن اثر انگشت بر روی گوش های تلفن به جای رمز ورود، در حال حاضر توسط اکثر بانک ها بکار گرفته می شود: بنابر این، درصورتی که تلفن همراه شما این ویژگی را داشته باشید، بجای ورود رمز از طریق صفحه کلید، می توانید شناسایی و احراز هویت ورود به سامانه را از طریق اسکن اثرانگشت روی گوشی انجام دهید.بدیهی است این ویژگی تأثیر بسیاری در افزایش امنیت سامانه و جلوگیری از سوء استفاده از حساب های بانکی شما از طریق سامانه همراه بانک را خواهد داشت. توصیه می شود در صورت امکان هنگام اتصال به شبکه های بیسیم رایگان و عمومی، از نرم افزار همراه بانک استفاده ننمایید.

شکل۷: اپلیکیشن اثر انگشت همراه بانک

گوشی تلفن همراه به دلیل کوچکی و در عین حال دارا بودن ارزش مالی تقریباً بالا از یک سو و نحوه استفاده از آن که سبب می گردد در هر مکانی آن را به همراه داشته باشند از سوی دیگر، ریسک سرقت و یا گم شدن را دارد، بنابر این در صورت سرقت یا مفقودی تلفن همراه خود، برای غیرفعال سازی سامانه همراه بانک منصوب در گوشی مفقود شده در اسرع وقت به یکی از شعب بانک مراجعه کرده یا به صورت تلفنی با مرکز ارتباط بانک تماس گرفته و درخواست غیرفعال سازی آن را کنید یا با استفاده از قابلیت "فعال/غیرفعال نمودن خدمات الکترونیک" موجود در سایت بانکداری اینترنتی خدمات سامانه همراه بانک نظیر حواله، مانده، سه گردش و...، را غیر فعال نمائید. همچنین در صورت تغییر در شماره تلفن همراه و یا واگذاری سیم کارت فعلی خود، اطلاعات مربوط به شماره تلفن همراه خود را در بانک به روزرسانی کنید. به این نکته توجه داشته باشید که پیش از فروش یا واگذاری گوشی تلفن همراه خود، نرم‌افزار سامانه همراه بانک را از روی آن حذف کنید.

در صورت نصب سامانه همراه بانک بر روی گوشی تلفن همراه خود، به منظور پیشگیری از بروز مخاطرات امنیتی، بر روی تلفن همراه خود نرم افزار ضدویروس معتبر نصب نموده و آن را به صورت مستمر به روزرسانی نمایید. گوشی تلفن همراه خود را طوری تنظیم نمایید که در فواصل زمانی کوتاه با استفاده از روش‌های امنیتی (PIN, Pattern, Password) قفل گردد. همچنین از اعمال تغییرات و دستکاری هایی که موجب کاهش سطح امنیت و قابلیت اعتماد سخت افزار و نرم افزار تلفن همراه می شود (روش های شکستن قفل سیستم عامل آن جهت نصب نرم افزارهای رایگان و ...) اجتناب کنید و در صورت مشاهده هرگونه اختلال در عملکرد گوشی تلفن همراه و یا نیاز به خدمات سخت‌افزاری و نرم‌افزاری، به نمایندگی‌های معتبر مراجعه نمایید

سعی کنید اطلاعات مهم بانکی و شخصی خود نظیر رمز اول و دوم کارت ها،کلمه عبور سامانه های بانکی، اطلاعات CVV۲ و تاریخ انقضای کارت ها و یا نام و رمز عبور پست الکترونیک و سایر حساب های کاربری خود را بر روی گوشی تلفن همراه ذخیره نکنید و یا از طریق پیامک، پست الکترونیک و شبکه های اجتماعی،اتصال به لینک های ارتباطی را ارسال نکرده و یا از طریق تلفن برای دیگران بازگو نکنید.

همچنین از اعمال تغییرات و دستکاري هاي منجر به کاهش سطح امنیت و قابلیت اعتماد سخت افزار و نرم افزار تلفن همراه (نظیر شکستن قفل درگوشی های دارای سیستم عامل IOS (Jailbreak) و گوشی های دارای سیستم عامل اندروید(Root) و...) اجتناب نمایید. و در صورت مشاهده هرگونه اختلال در عملکرد گوشي تلفن همراه یا نیاز به سرویس سخت افزاري و نرم افزاري، به نمایندگي هاي معتبر مراجعه نمایید.

نکات امنیتی در استفاده از تلفنبانک

:

ملاحظات فعالسازي سامانه تلفن بانک و ملاحظات امنیتی درخواستی به شرح ذیل می باشد:
هنـگام دریافـت پاکـت محتـوي کلمـه عبـور سـامانه تلفنبانـک، از بـاز و مخـدوش نبـودن پاکـت اطمینـان حاصـل نمـوده و در صـورت مخـدوش بـودن، مسـئول شـعبه را مطلـع نماییـد. توصیـه مـی شـود رمـز ورود بـه سـامانه تلفـن بانـك ارائـه شـده توسـط شـعبه را در اولـین فرصـت تغییردهیـد. از انتخـاب رمزهـای مشـابه بـا رمـز کارت‌هـا و سـامانه‌های بانکـی بـرای سـامانه تلفنبانـک خـودداری فرمائیـد. از انتخـاب کلمـه عبـور قابـل حـدس نظیـر سـال تولـد، سـال ازدواج، شـماره شناسـنامه و ...، بـرای ورود بـه سـامانه تلفـن بانـک، اجتنـاب نماییـد. همچنیـن کلمـه عبـور تلفـن بانـک خـود را در اختیـار دیگـران قـرار ندهیـد و آن را در فواصـل زمـاني (حداقـل هـر سـه مـاه) و همچنیـن بنـا بـه ضرورت، تغییـر دهیـد.
توجـه داشـته باشـید هنـگام ورود شـماره حسـاب و کلمـه عبورسـامانه تلفنبانـک، از دیـده نشـدن آن توسـط دیگـران اطمینـان حاصـل نمـوده و از یادداشـت و ذخیـره نمـودن شـماره حسـاب و کلمـه عبـور خـود در جایـي کـه امـکان سوءاسـتفاده هـاي آتي از حسـاب بانـکي شـما را بـراي یابنـده آن فراهـم مـي نمایـد، خـوددارې نماییـد. در صـورت امـکان از یکبـار رمـز (OTP) اسـتفاده گـردد. نکتـه مهـم در اسـتفاده از OTP ایـن اسـت کـه، امـکان سـوء اسـتفاده از حسـاب هـای بانکـی شـما را کاهـش مـی دهـد. پـس، توصیـه مـی شـود جهـت ورود بـه سـامانه تلفنبانـک نیـز، از یکبـار رمـز اسـتفاده گـردد.
درخصـوص ملاحظـات امنیتـی غیرفعـال سـازی سـامانه تلفنبانـک نـکات ذکـر شـده ذیـل را مدنظـر قـرار دهیـد. درصـورت سرقـت رمـز کاربـری سـامانه تلفنبانـک، یکـی از اقدامـات ذیـل را انجـام دهیـد:
• مراجعه حضوري به يكي از شعب بانك ملت و درخواست غيرفعال سازي سامانه و دريافت رمز جديد
• اسـتفاده نمـودن از قابلیـت "فعال/غیرفعـال نمـودن خدمـات الکترونیـک" موجـود در سـایت بانکـداری اینترنتـی بـه منظـور غیرفعـال نمـودن خدمـات سـامانه تلفـن بانـک نظیـر مانـده، سـه گـردش و صورتحسـاب.
جهـت عملیـات بانکـی خـود اعـم از ورود بـه سیسـتم تلفـن بانـک یـا انجـام هرگونـه تراکنـش بانکـی، از تلفن‌هـای عمومـی و تلفن‌هایـی کـه دارای کاربـران زیـادی مـی باشـند، اسـتفاده ننماییـد. تلفنبانـک در مکان‌هایـی کـه از طریـق دوربیـن مداربسـته مانیتـور می‌شـوند، مـورد اسـتفاده قـرار نگیـرد یـا در صـورت بـروز شرایـط اجتنـاب ناپذیـر، دقـت کافـی درخصـوص عـدم رویـت رمـز و عملیـات درخواسـتی بـه عمـل آیـد. در صـورت امـکان سـامانه تلفنبانـک در حضـور دیگـران مـورد اسـتفاده قـرار نگیـرد و در صـورت ضرورت اجتنـاب ناپذیـر، از دیـده نشـدن رمـز و عملیـات درخواسـتی توسـط دیگـران اطمینـان حاصـل نماییـد.

شکل ۸: خدمات تلفنبانک ملت

در صـورت بـروز اشـکال در فراینـد اسـتفاده از سـامانه تلفنبانـک و عملیـات درخواسـتی، از یـاری جسـتن از افـراد ناشـناس جـداً خـودداری نماینـد. توجـه داشـته باشـید کـه اگـر در حیـن اسـتفاده از سـامانه تلفنبانـک، عملیـات درخواسـتی قطـع گردیـد، هیـچ تماسـی از سـوی بانـک جهـت ادامـه انجـام عملیـات، بـا شـما برقـرار نمـی گـردد. در صـورت بـروز چنیـن اتفاقـی، تمـاس دریافتـی را قطـع نمـوده و از خـط تلفـن دیگـری بـه منظـور تمـاس بـا سـامانه تلفنبانـک و انجـام عملیـات مـورد نظـر اسـتفاده نماییـد. از سـمت بانـک هیـچ گونـه تماسـی مبنـی بـر انجـام عملیـات تلفنبانـک بـا شـما برقـرار نمـی گـردد.
چنانچـه دسـتگاه تلفـن مـورد اسـتفاده شـما دارای صفحـه نمایـش مـی باشـد، پـس از اتمـام کار بـا سـامانه تلفنبانـک، از حـذف عملیـات خـود از حافظـه آن اطمینـان حاصـل نماییـد. در صـورت پیـش بینـی احتـمال شـنود یـا ردیابـی دسـتگاه تلفـن، از اسـتفاده از آن جهـت دسترسـی بـه سـامانه تلفنبانـک پرهیـز نماییـد.
هرگـز اطلاعـات مهـم خـود ماننـد رمـز اول و دوم کارت هـا، کلمـه عبـور سـامانه هـاي بانـکي نظیـر تلفنبانـک، CVV۲ و تاریـخ

انقضاي كارت را بـر روی كاغـذ، تلفـن همـراه و سـایر مكان‌هـا و تجهیزاتـی كـه امـكان دسترسـی بـه آن هـا وجـود دارد، ذخیـره ننمـوده و یـا از طریـق پیامـك، ایمیـل و سـایر سـامانه هـاي ارتباطـي نظـیر تلفـن، شـبكه هـای اجتماعـی و... بـراي سـایرین ارسـال و بازگـو ننماییـد. بانـك هرگـز اطلاعـات محرمانـه شـما (نظـیر مشـخصات شناسـنامه اي، كدمـلي، اطلاعـات مربـوط بـه كارت و حسـاب بانـكي و ...) را از طریـق تلفـن، ایمیـل، پیامـك، شـبكه هـای اجتماعـی، پیشـنهاد اتصـال بـه لینـک هـای ارتباطـی اینترنتـی و...، درخواسـت نمـي كنـد. در صـورت رخـداد ایـن مـورد، ضمـن عـدم پاسـخگویي بـه چنـین درخواسـت هایـي مراتـب را سریعـاً بـه بانـك اطـلاع دهیـد.

جهـت انجـام تراكنـش هـای بانكـی در سـامانه تلفنبانـک، صرفـاً از شـماره تلفن‌هـای اعـلام شـده در هنـگام ثبت‌نـام اسـتفاده نماییـد. در صـورت سرقـت و یـا مفقـود شـدن كارت بانكـی، امـكان مسـدود و غیرفعـال نمـودن كارت بـا اسـتفاده از سـامانه تلفنبانـک فراهـم مـی باشـد. بنابرایـن در صـورت بـروز هرگونـه مشـكل و یـا مشـاهده شـواهد مشـكوك در حسـاب خـود یـا دریافـت ایمیل/پیامـک غیرقابـل اطمینـان كـه صحـت آن هـا از سـوی شـما مـورد تأییـد نمـي باشـند، حتـماً بانـك را از طریـق شـماره تلفـن ۱۵۵۶ (تهـران) یـا ۸۲۴۸۸- ۰۲۱ (شهرسـتان) مطلـع نماییـد.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید،
در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱-باتوصیه های امنیتی در استفاده از خدمات بانکداری اینترنتی آشنا شدید.	
۲- با توصیه های امنیتی در استفاده از سامانه همراه بانک آشنا شدید.	
۳- با توصیه های امنیتی در استفاده از سامانه تلفنبانک آشنا شدید.	

خودآزمایی جلسه سیزدهم :

۱. کدامیک از جملات زیر صحیح می‌باشد؟
الف) در صورت ورود به سامانه بانکداری اینترنتی از محیط‌های عمومی (نظیر کافی‌نت) حتماً در اولین فرصت ممکن کلمه عبور خود را تغییر دهید.
ب) به محض دریافت پیامک ورود به سامانه بانکداری اینترنتی و یا انجام تراکنش‌های مالی، در صورتی که عمل مذکور از سوی خودتان صورت نگرفته، نسبت به تغییر کلمه عبور خود اقدام و مراتب را در اسرع وقت به مرکز ارتباط بانک اطلاع‌رسانی نمایید.
ج) هرگز اطلاعات مربوط به حساب و کارت بانکی خود را در شبکه‌های اجتماعی قرار ندهید.
د) همه موارد

۲. در صورتی که از طریق پست الکترونیک، نامه دریافت کردید که در آن لینک تغییر رمز ورود به سامانه بانکداری اینترنتی قرار داشته باشد، کدام گزینه اقدام مناسبی است؟
الف) از طریق لینک دریافت شده، در اسرع وقت رمز ورود به سامانه را تغییر دهیم.
ب) هیچ اقدامی روی لینک انجام ندهیم.
ج) بانک را از دریافت چنین نامه ای مطلع کنیم.
د) گزینه های ب و ج

۳. کدامیک از جملات زیر در صورت سرقت یا مفقودی تلفن همراه، صحیح می‌باشد؟
الف) اطلاع موضوع به مرکز ارتباط بانک و درخواست غیرفعال سازی سامانه همراه بانک
ب) مراجعه حضوری به یکی از شعب بانک و درخواست غیرفعال سازی سامانه همراه بانک
ج) استفاده نمودن از قابلیت "فعال/غیرفعال نمودن خدمات اکترونیک"موجود در سایت بانکداری اینترنتی به منظور غیرفعال نمودن خدمات سامانه
د) همه موارد

۴. کدام گزینه راهکار مناسبی برای حفظ امنیت سامانه "همراه بانک" نیست؟
الف) نسخه نرم افزار همراه بانک را با مراجعه به شعبه یا با مراجعه مستقیم به وب سایت بانک ملت دریافت و نصب نماییم.
ب) از به روزرسانی نسخه نرم افزار همراه بانک اجتناب کنیم.
ج) پس از فعال سازی سامانه همراه بانک، رمز عبور آن را عوض کنیم.
د) در صورت واگذاری گوشی تلفن همراه به غیر، نسخه نرم افزار همراه بانک منصوب روی آن را حذف نماییم.

پاسخ‌نامه تشریحی

خودآزمایی جلسه سیزدهم

۱. پاسخ صحیح، گزینه «د»

• تا حد امکان از محیط‌های عمومی (نظیر کافی‌نت) رایانه‌های ناشناس و شبکه‌های بی‌سیم عمومی برای دسترسی به سامانه بانکداری اینترنتی اجتناب نمایید و در صورت استفاده، حتماً در اولین فرصت ممکن کلمه عبور خود را تغییر دهید.

• درخواست ارسال پیامک جهت ورود به سامانه بانکداری اینترنتی و یا انجام تراکنش‌های مالی، سبب آگاهی مشتری از سوءاستفاده‌های احتمالی و جلوگیری از سوءاستفاده بیشتر می‌شود. به محض دریافت چنین پیامک‌هایی در صورتی که عمل مذکور از سوی خودتان صورت نگرفته است، نسبت به تغییر کلمه عبور خود اقدام و مراتب را در اسرع وقت به مرکز ارتباط بانک اطلاع‌رسانی نمایید.

• هرگز اطلاعات مربوط به حساب و کارت بانکی خود را در شبکه‌های اجتماعی قرار ندهید.

۲. پاسخ صحیح، گزینه «د»

در مواجه با دریافت چنین ایمیلی، باید هوشیارانه عمل کرد و ضمن اینکه هیچ اقدامی از طریق لینک انجام نمی‌دهیم، بهتر است بانک را نیز از موضوع مطلع نماییم.

۳. پاسخ صحیح، گزینه «د»

• در صورت سرقت یا مفقودی تلفن همراه، اقدامات ذیل را در اسرع وقت انجام دهید:

o اطلاع موضوع به مرکز ارتباط و درخواست غیرفعال سازی سامانه همراه بانک

o مراجعه حضوری به یکی از شعب بانک و درخواست غیرفعال سازی سامانه همراه بانک

o استفاده نمودن از قابلیت "فعال/غیرفعال نمودن خدمات اکترونیک" موجود در سایت بانکداری اینترنتی به منظور غیرفعال نمودن خدمات سامانه

۴. پاسخ صحیح، گزینه «ب»

برای حفظ امنیت سامانه همراه بانک، علاوه بر دریافت و نصب نسخه از مراجع معتبر نظیر شعبه و یا وب سایت بانک، در صورت ارائه نسخه جدید نرم افزار، آن را به روزرسانی کنیم. همچنین پس از فعال سازی سامانه همراه بانک، رمز عبور آن را عوض کرده و در صورت واگذاری گوشی تلفن همراه به غیر، نسخه نرم افزار همراه بانک منصوب روی آن را حذف نماییم. در صورت تغییر در شماره تلفن همراه یا واگذاري سیم کارت فعلي، اطلاعات مربوط به شماره تلفن همراه خود را در بانك به روزرساني نماييم. پیش از فروش یا واگذاري گوشي تلفن همراه خود، نرم افزار سامانه همراه بانك را از روي آن حذف (Uninstall) نماييم.

خلاصه فصل ششم

جلسه دوازدهم

اطلاعات کارت بانکی را اگرچه بنا به ضرورت و برای انتقال پول ممکن است در اختیار دیگران قرار دهید امّا همواره به این نکته توجه داشته باشید که اطلاعات کارت بانکی در زمره اطلاعات شخصی و مهم می باشد، پس اطلاعات کارت بانکی خود را در اختیار افراد غیر و ناشناس قرار ندهید و از پذیرش درخواست افراد ناشناس جهت استفاده از کارت بانکی شما به‌عنوان واسط (نظیر انتقال وجه) اجتناب کنید.

هرگز اطلاعات مهم خود مانند رمز کارت‌های بانکی، کلمه عبور سامانه‌های بانکی، کد اعتبارسنجی (CVV۲) و تاریخ انقضای کارت بانکی را بر روی گوشی تلفن همراه ذخیره نکرده و یا از طریق پیامک، ایمیل و سایر سامانه‌های ارتباطی نظیر تلفن برای سایرین ارسال و بازگو نکنید.

هنگام استفاده از دستگاه خودپرداز یا پایانه‌های فروش نیز لازم است نکات امنیتی نظیر حفظ حریم شخصی، هوشیاری نسبت به ترفندهای مهندسی اجتماعی را رعایت کنیم.

برای خرید های اینترنتی از رایانه های ناشناس و عمومی استفاده نکنید و از به روزرسانی مستمر سیستم‌عامل، مرورگر وب و سایر نرم‌افزارهای نصب شده روی رایانه، تبلت و گوشی تلفن همراه خود مطمئن شوید. رایانه، تبلت و گوشی تلفن همراه خود را به نرم افزار ضدویروس معتبر مجهز کنید و آن را به صورت مستمر به روزرسانی نمایید.

تمامی سایت‌های معتبر و مهم که تراکنش‌های مالی انجام می‌دهند، دارای نشانگرهای امنیتی (SSL و HTTPS) می‌باشند. لذا جهت انجام خرید اینترنتی، قبل از ورود اطلاعات در وب‌سایت درگاه پرداخت اینترنتی، از وجود این نشانگرهای امنیتی و معتبر بودن وب‌سایت مذکور اطمینان حاصل نمایید.

جلسه سیزدهم

پس از فعال سازی سامانه بانکداری اینترنتی یا همراه بانک یا تلفنبانک، رمز عبور ورود به سامانه را در اولین فرصت تغییر دهید.

یکی از پارامترهای خاص پیش بینی شده برای خدمت بانکداری اینترنتی استفاده از یکبار رمز (OTP) است . یکبار رمز ،کلمه عبوری است که با روش های رمزنگاری تولید و اعتبار آن برای مدت کوتاه (مثلاً یک دقیقه) و فقط یکبار استفاده می باشد. پس، توصیه می شود جهت افزایش امنیت سامانه بانکداری اینترنتی خود، جهت ورود به سامانه و انجام تراکنش‌های مالی از یکبار رمز استفاده کنید. در حد امکان ورود به سامانه بانکداری اینترنتی را از طریق رایانه شخصی خود انجام دهید و در زمان دسترسی به سامانه بانکداری اینترنتی مطمئن شوید که از ابزارهای فیلتر شکن نظیر VPN استفاده نمی کنید. همینطور از ذخیره رمز عبور در مرورگر وب خودداری کنید.

بانک از کانال هایی نظیر پست الکترونیک و پیامک و شبکه های اجتماعی، پیشنهاد اتصال به لینک های ارتباطی شما را ترغیب به ورود به سامانه بانکداری اینترنتی نمی کند، پس، در صورت مواجه شدن با چنین موضوعاتی هوشیار باشید و ترجیحاً بانک مرجع را از موضوع مطلع کنید. برای استفاده از سامانه بانکداری اینترنتی صرفاً از طریق مراجعه مستقیم به وب‌سایت بانک مورد نظر اقدام کنید. همچنین توصیه می‌شود برای امنیت بیشتر، وب‌سایت بانک را با تایپ نمودن نشانی اینترنتی (URL) آن در نوار آدرس (Address bar) مرورگر وب مشاهده نمایید.

در صورت نصب سامانه همراه بانک بر روی گوشی تلفن همراه خود، به منظور پیشگیری از بروز مخاطرات امنیتی، بر روی تلفن همراه خود، نرم افزار ضدویروس معتبر نصب نموده و آن را به صورت مستمر به روزرسانی نمایید. گوشی تلفن همراه خود را طوری تنظیم نمایید که در فواصل زمانی کوتاه با استفاده از روش‌های امنیتی (PIN, Pattern, Password) قفل گردد. همچنین از اعمال تغییرات و دستکاری هایی که موجب کاهش سطح امنیت و قابلیت اعتماد سخت افزار و نرم افزار تلفن همراه می شود اجتناب کنید.

سعی کنید اطلاعات مهم بانکی و شخصی خود نظیر رمز اول و دوم کارت ها ،کلمه عبور سامانه های بانکی، اطلاعات CVV۲ و تاریخ انقضای کارت ها و یا نام و رمز عبور پست الکترونیک و سایر حساب های کاربری خود را بر روی گوشی تلفن همراه ذخیره نکنید.

فصل اول: آشنایی با مفاهیم امنیت اطلاعات
فصل دوم: امنیت فیزیکی و محیطی
فصل سوم: تهدیدات امنیتی در شبکه های رایانه‌ای
فصل چهارم: امنیت در مقابله با تهدیدات فضای سایبری
فصل پنجم: امنیت تجهیزات قابل حمل
فصل ششم: توصیه های امنیتی در خدمات بانکی

فصل هفتم

جرایم رایانه ای و تعهدنامه عدم افشاء اطلاعات

جلسه چهاردهم:
جرایم رایانه‌ای و قوانین آن در ایران

جلسه پانزدهم:
تعهدنامه عدم افشای اطلاعات (NDA)

فصل هشتم:
پیاده سازی امنیت در سازمان ها

جلسه چهاردهم

جرایم رایانه‌ای و قوانین آن در ایران

۱۸۷	اهداف یادگیری
۱۸۸	پیش آزمون
۱۹۰	تعریف جرایم رایانه‌ای
۱۹۲	تاریخچه وقوع جرایم رایانه ای در ایران
۱۹۳	قانون جرایم رایانه‌ای در ایران
۱۹۷	تعریف تخلفات الکترونیک حوزهٔ فناوری اطلاعات بانک ملت
۱۹۸	میزان دستیابی به اهداف یادگیری
	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با جرایم رایانه‌ای و انواع آن آشنا شود.
۲. با قوانین جرایم رایانه‌ای در ایران آشنا شود.
۳. با انواع تخلفات الکترونیک بانک ملت آشنا شود.

پیش‌آزمون جلسه چهاردهم :

۱. .....به مجموعه‌ای از تخلفات و بزهکاری‌ها گفته می‌شود که از طریق رایانه و ابزارهای الکترونیک یا مؤثر بر رایانه واقع می‌شود.

الف) جرایم رایانه‌ای ب) جرایم سایبری ج) جرایم اینترنتی د) همه موارد

۲. به نظر شما کدامیک از موارد زیر جرم محسوب می‌شود؟

الف) شنود غیرمجاز

ب) دسترسی به داده ها

ج) انتشار صوت یا تصویر یا فیلم خصوصي یا خانوادگي یا اسرار دیگري بدون رضایت

د) همه موارد

پاسخ‌نامه

پیش‌آزمون جلسه چهاردهم

:

	الف	ب	ج	د
۱				
۲				

تعریف جرایم رایانه‌ای

:

با گسترش استفاده از رایانه، اینترنت، تلفن‌های هوشمند و انواع ابزارهای الکترونیک در دنیای امروزه و تغییر در سبک زندگی افراد، نوع بزهکاری و تخلفات نیز تغییر یافته و سارقان به‌جای استفاده از روش های سنتی و بالارفتن از دیوار و ورود به منازل، از روش‌های متفاوت دیگری نظیر روش‌های اینترنتی، مهندسی اجتماعی، سرقت اطلاعات مهم و بانکی برای دزدی استفاده می‌کنند. بنابراین، وجود قوانینی برای جلوگیری از وقوع این جرایم و یا رسیدگی به آن‌ها امری ضروری می‌باشد.

آنچه امروز تحت عنوان جرائم رایانه‌ای (جرایم اینترنتی، جرایم فضای سایبری) نام برده می‌شود، مجموعه‌ای از همین تخلفات و بزهکاری‌ها می‌باشد که از طریق رایانه و ابزارهای الکترونیک واقع می‌شود و مصادیق متعددی از آن نیز در ذهن ما نقش بسته است.

بر طبق تعاریف قانونی، سوءاستفاده از رایانه‌ها شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار و انتقال داده را جرم رایانه‌ای می‌نامند. به‌عبارت دیگر، هر عمل مثبت یا منفی غیرقانونی که رایانه در آن ابزار یا موضوع جرم باشد، جرم رایانه‌ای خوانده می‌شود.

جرایم رایانه‌ای را می‌توان به سه دسته تقسیم نمود:

۱. جرایمی که در آن ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شود، مانند: سرقت و تخریب

۲. جرایمی که در آن ها رایانه به عنوان ابزار ارتکاب جرم بکار گرفته می‌شود که معمولاً از طریق شبکه‌های رایانه‌ای و اینترنت رخ می‌دهند، مانند: کلاهبرداری، جعل و سرقت رایانه‌ای

۳. جرایمی که در فضای مجازی به وقوع می پیوندد اما آثار آن ها در دنیای واقعی ظاهر می‌شود، مانند: نفوذ غیرمجاز، شنود غیرمجاز، انتشار ویروس و کرم‌های رایانه‌ای

تاریخچه وقوع جرایم رایانه ای در ایران

:

در خصوص تاریخ وقوع جرم رایانه‌ای در ایران، به دلیل نبود قانون مدون و آمار دقیق از جرائم و سوءاستفاده از رایانه همزمان با ورود آن در کشور در سال ۱۳۴۱، نمی‌توان تاریخچه‌ای مشخص برای آن بیان نمود.

امّا براساس اطلاعات موجود، اولین جرم اینترنتی در ایران در سال ۱۳۷۸ به وقوع پیوست، که در آن یک کارگر چاپخانه و یک دانشجوی رشته کامپیوتر در کرمان اقدام به جعل چک‌های تضمینی مسافرتی کردند و عمل آن ها به عنوان جرم رایانه‌ای محسوب گردید. بعد از این بود که گروه‌های هکر، جرم‌های دیگری را مرتکب شدند، مواردی چون کلاهبرداري‌هاي الکترونيك، جازدن خود به جاي شخص ديگر (جعل هويت)، استفاده غیرمجاز از اطلاعات، هک و نفوذهای غیرمجاز به سیستم‌ها نمونه‌هایی از این جرایم هستند.

قانون جرایم رایانه‌ای در ایران

:

تصویب قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای درسال ۱۳۷۹ را می‌توان به عنوان اولین واکنش قانونی در قالب یک قانون مستقل در قبال جرایم رایانه‌ای در ایران نام برد.

همچنین در سال ۱۳۸۲ قانون مجازات جرایم نیروهای مسلح، سوءاستفاده‌های مالی نظامی را با استفاده از رایانه (کلاهبرداری و اختلاس) به عنوان جرم در نظر گرفت و در نهایت قانون جرایم رایانه‌ای، مشتمل بر ۵۶ ماده و ۲۵ تبصره در جلسه علنی در سال ۱۳۸۸ در مجلس شورای اسلامی تصویب و به تأیید شورای نگهبان رسید.

در حال حاضر دادسرای رسیدگی به جرایم رایانه‌ای، مسئول رسیدگی به این جرایم در ایران می‌باشد که با توجه به قوانین وضع شده، به بررسی این جرایم و رسیدگی به شکایات افراد پرداخته می‌شود.
اهم محتوای قانون جرایم رایانه ای کشور، مشتمل بر عناوین جرایم تعریف شده و شماره ماده قانون مرتبط در قالب جدول ذیل قابل مطالعه و بررسی است.

ردیف	عناوین جرایم رایانه‌ای		شماره ماده قانون مجازات اسلامی
	دسترسی غیرمجاز به داده ها و سامانه‌های رایانه ای		۷۲۹
	شنود غیرمجاز		۷۳۰
	جاسوسی رایانه ای (دسترسی به داده های سری)		۷۳۱
	جاسوسی رایانه ای (دسترسی به داده های سری و قرار دادن در اختیار اشخاص فاقد صلاحیت)		۷۳۱
	جاسوسی رایانه ای (دسترسی به داده های سری و افشای آن ها برای دولت‌ها و عوامل بیگانه)		۷۳۱
	نقض تدابیر امنیتی به قصد دسترسی به داده‌های سری		۷۳۲
	سهل انگاری مأموران دولت منجر به جاسوسی		۷۳۳
	جعل رایانه ای و استفاده از مجعول		۷۳۴ و ۷۳۵
	تخریب و اخلال در داده ها		۷۳۶
	از کار انداختن سامانه‌ها		۷۳۷
	ممانعت از دسترسی		۷۳۸
	تخریب و اخلال در داده‌ها و از کار انداختن سامانه‌ها و ممانعت از دسترسی علیه سامانه های بکار رفته در خدمات عمومی با قصد به خطر انداختن امنیت عمومی		۷۳۹
	ربودن داده های دیگری	با وجود عین داده در اختیار صاحب آن	۷۴۰
		بدون وجود عین داده در اختیار صاحب آن	۷۴۰
	کلاهبرداری مرتبط با رایانه		۷۴۱
	انتشار، توزیع یا معامله محتویات مستهجن یا نگهداری و تولید و ذخیره به انگیزه تجارت یا فساد		۷۴۲
	انتشار، توزیع یا معامله محتویات مبتذل یا نگهداری و تولید و ذخیره به انگیزه تجارت یا فساد		۷۴۲
	تحریک، ترغیب، تهدید یا تطمیع یا فریب افراد برای دسترسی به محتویات مستهجن یا تسهیل یا آموزش شیوه دسترسی		۷۴۳
	تحریک، ترغیب، تهدید یا تطمیع یا فریب افراد برای دسترسی به محتویات مبتذل یا تسهیل یا آموزش شیوه دسترسی		۷۴۳
	ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روانگردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز		۷۴۳
	هتک حیثیت با تغییر یا تحریف فیلم یا صوت یا تصویر دیگری و انتشار آن یا صرف انتشار با علم به تغییر یا تحریف (تغییر و تحریف مستهجن حداکثر هردو مجازات)		۷۴۴
	انتشار صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری بدون رضایت		۷۴۵
	نشر اکاذیب به قصد تشویش اذهان عمومی یا مقامات رسمی		۷۴۶
	تولید یا انتشار یا توزیع داده‌ها یا نرم‌افزارهایی که صرفاً برای ارتکاب جرم کاربرد دارند		۷۵۳
	فروش یا انتشار گذرواژه هایی که امکان دسترسی به داده یا سامانه های دیگری را فراهم کند		۷۵۳
	انتشار یا در دسترس قرار دادن آموزش ارتکاب جرایم رایانه ای		۷۵۳
	برقراری ارتباطات مخابراتی با استفاده از پهنای باند بین المللی از داخل به خارج از کشور و برعکس		۷۵۲
	عدم پالایش (فیلتر) محتوای مجرمانه از ناحیه ارائه دهندگان خدمات دسترسی و میزبانی	ناشی ازعمد	۷۴۹ و ۷۵۱
		ناشی از سهل‌انگاری	
	خودداری از اجرای دستور حفاظت از داده ها یا افشای داده‌های حفاظت شده یا آگاه نمودن اشخاصی که داده‌های مزبور به آن ها مربوط می‌شود		۷۶۲
	خودداری از اجرای دستور قضایی ارائه داده ها		۷۶۳

تعریف تخلفات الکترونیک حوزه فناوری اطلاعات بانک ملت

:

با توجه به اهمیت حوزه بانکی از منظر نوع و اهمیت اطلاعات مورد استفاده و مخاطرات احتمالی پیش‌رو، بانک ملت نیز با رویکرد دستیابی به اهداف ذیل و مبتنی بر مفاد قانون جرایم رایانه‌ای کشور و براساس آئین‌نامه انضباطی خود، جرایمی را تحت عنوان تخلفات الکترونیک حوزه فناوری اطلاعات تدوین نموده است:

- ایجاد بستر ضمانت‌های اجرایی در راستای توجه و اجرای سیاست‌های امنیتی مرتبط با حوزه فناوری اطلاعات
- پوشش ضرورت‌های مورد نیاز سیستم مدیریت امنیت اطلاعات (ISMS)
- ایجاد فضای بازدارنده از وقوع تخلف در حوزه فناوری اطلاعات در بانک

تخلفات الکترونیک تعریف شده، در قالب شانزده تخلف با درجه اهمیت‌های متفاوت براساس طبقه‌بندی تخلفات آیین‌نامه انضباطی بانک دسته‌بندی و از سال ۱۳۹۳ در محتوای تخلفات آیین‌نامه انضباطی درج گردیده‌اند و در صورت محرز شدن ارتکاب هر یک از این تخلفات توسط کارکنان، مطابق با طبقه تخلفاتی مربوطه و تنبیهات تعریف شده متناظر در آئین‌نامه انضباطی بانک، با فرد خاطی برخورد خواهد شد.

تخلفات الکترونیکی بانک ملت و دسته‌بندی متناظر آن‌ها به شرح جدول ذیل می‌باشد:

ردیف	عنوان تخلفات الکترونیکی	طبقه تخلفاتی
	سهل انگاری در حفظ هویت الکترونیک، دسترسی انحصاری و یا امنیت سامانه های الکترونیک تحت اختیار	طبقه یک
	نصب نرم افزارهای غیرمرتبط با وظایف محوله	طبقه یک
	سهل انگاری منجر به اخلال در دسترسی به داده ها و سیستم های رایانه ای	طبقه یک
	دریافت و ذخیره سازی محتوای غیرمجاز بر روی سیستم رایانه ای و یا شبکه تبادل داده	طبقه یک
	ورود به سیستم و یا سامانه های الکترونیک با هویت الکترونیک متعلق به غیر	طبقه دو
	اتصال هرگونه سخت افزار غیرمجاز بر روی سیستم های رایانه ای و یا شبکه تبادل داده	طبقه دو
	بهره برداری غیرمجاز از داده ها و سیستم های رایانه ای	طبقه دو
	ممانعت و یا اخلال عامدانه در دسترسی افراد مجاز به سیستم و یا اطلاعات تحت اختیار	طبقه دو
	نقض حریم خصوصی کارکنان و دسترسی به اطلاعات ایشان از طریق واسط‌های الکترونیکی	طبقه دو
	انتشار، مبادله و به اشتراک گذاری داده های غیراخلاقی و غیرمجاز از طریق سیستم رایانه ای و یا شبکه تبادل داده	طبقه دو
	افشای هویت الکترونیک خود	طبقه دو
	سوء استفاده از کد کاربری متعلق به غیر	طبقه سه
	دسترسی غیرمجاز به داده ها و سیستم های رایانه ای، افشا و یا در دسترس قراردادن آن ها	طبقه سه
	انتشار بدافزار یا نرم افزارهای مخرب	طبقه سه
	اخلال عامدانه در داده ها و سیستم های رایانه ای	طبقه سه
	جعل الکترونیک در داده و یا تراشه الکترونیک و یا استفاده عالمانه از داده های مجعول	طبقه سه

جدول ۲: تخلفات الکترونیک حوزه فناوری اطلاعات بانک ملت

جهت آشنایی با تعاریف تخلفات الکترونیک به بخش مربوطه در پیوست کتاب مراجعه نمایید.

میزان دستیابی به اهداف یادگیری

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
با جرایم رایانه‌ای و انواع آن آشنا شدید.	
با قوانین جرایم رایانه‌ای در ایران آشنا شدید.	
با انواع تخلفات الکترونیک بانک ملت آشنا شدید.	

خودآزمایی جلسه چهاردهم :

۱. کدامیک از موارد زیر از انواع جرایم رایانه‌ای محسوب می‌شود.
الف) جرایمی که در آن ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شود.
ب) جرایمی که در آن ها رایانه به عنوان ابزار ارتکاب جرم بکار گرفته می‌شود که معمولاً از طریق شبکه‌های رایانه‌ای و اینترنت رخ می‌دهد.
ج) جرایمی که در فضای مجازی به وقوع می پیوندد اما آثار آن ها در دنیای واقعی ظاهر می‌شود.
د) همه موارد

۲. کدامیک از تخلفات زیر جزو تخلفات الکترونیک طبقه سوم در بانک ملت محسوب نمی‌شود؟
الف) انتشار بدافزار یا نرم افزارهاي مخرب
ب) اخلال عامدانه در داده ها و سیستم هاي رایانه اي
ج) سهل انگاري منجر به اخلال در دسترسي به داده ها و سیستم هاي رایانه اي
د) سوء استفاده از کد کاربری متعلق به غیر

۳. سناریوی زیر کدامیک از جرایم رایانه‌ای را شامل می‌شود؟
"فردی با هک کردن سایت سازمان سنجش، اطلاعات مربوط به داوطلبان کنکور را ربوده و سایت سازمان سنجش را از کار انداخته است."
الف) دسترسی غیرمجاز به داده ها و سامانه‌های رایانه ای
ب) کلاهبرداری مرتبط با رایانه
ج) از کار انداختن سامانه‌ها
د) گزینه الف و ج

۴. سناریوی زیر کدامیک از جرایم رایانه‌ای را شامل می‌شود؟
"هکری، صفحه‌ای متقلبانه مشابه با سایت بانکی را ساخته و اطلاعات مشتریانی که اطلاعات حساب و رمز ورود خود را در این صفحه متقلبانه وارد می کنند؛ ربوده و سپس اقدام به سوءاستفاده از این اطلاعات نموده و از حساب بانکی آنها برداشت می‌نماید."
الف) شنود غیرمجاز
ب) کلاهبرداری مرتبط با رایانه
ج) تخریب و اخلال در داده ها
د) جاسوسی رایانه ای (دسترسی به داده های سری)

پاسخ‌نامه تشریحی

خودآزمایی جلسه چهاردهم

:

۱. پاسخ صحیح، گزینه «د»

جرایم رایانه‌ای را می‌توان به سه دسته تقسیم نمود:

- جرایمی که در آن ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شود، مانند: سرقت، تخریب و ...
- جرایمی که در آن ها رایانه به عنوان ابزار ارتکاب جرم بکار گرفته می‌شود که معمولاً از طریق شبکه‌های رایانه‌ای و اینترنت رخ می‌دهد، مانند: کلاهبرداری، جعل و سرقت رایانه‌ای و ...
- جرایمی که در فضای مجازی به وقوع می پیوندد اما آثار آن ها در دنیای واقعی ظاهر می‌شود، مانند: نفوذ غیرمجاز، شنود غیرمجاز، انتشار ویروس و کرم‌های رایانه‌ای و ...

۲. پاسخ صحیح، گزینه «ج»

سهل انگاری منجر به اخلال در دسترسی به داده ها و سیستم های رایانه ای

۳. پاسخ صحیح، گزینه «د»

دسترسی غیرمجاز به داده ها و سامانه‌های رایانه ای (دسترسی غیرمجاز به سایت سازمان سنجش و اطلاعات داوطلبان کنکور) و از کار انداختن سامانه‌ها (از کار انداختن سایت سازمان سنجش)

۴. پاسخ صحیح، گزینه «ب»

کلاهبرداری مرتبط با رایانه

جلسه پانزدهم

تعهدنامه عدم افشای اطلاعات (NDA)

۱۸۷	اهداف یادگیری
۱۸۸	پیش آزمون
۱۹۰	تعهدنامه عدم افشای اطلاعات (NDA)
۱۹۲	تعهدات عمدهٔ طرفین قرارداد در تعهدنامه عدم افشای اطلاعات (NDA)
۱۹۲	میزان دستیابی به اهداف یادگیری
۱۹۷	خودآزمایی
۱۹۸	خلاصه فصل هفتم

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با مفهوم تعهدنامه عدم افشای اطلاعات آشنا شود.
۲. با کاربردهای تعهدنامه عدم افشای اطلاعات آشنا شود.

پیش‌آزمون جلسه پانزدهم :

۱. ..... یک توافق‌نامه است که بین حداقل دو طرف حاصل می‌شود و براساس آن طرفین توافق می‌کنند که یک سری اطلاعات محرمانه شامل دانش و اطلاعات که طرفین به منظور خاصی به یکدیگر عرضه می‌کنند، بازنشر نداشته باشد و صرفاً در همان منظور خاص مورد استفاده قرارگیرد.

الف) قرارداد ب) تفاهم نامه عدم افشا ج) تفاهم نامه سطح سرویس د) هیچ کدام

۲. NDA یا تفاهم نامه عدم افشای اطلاعات باید میان سازمان و چه اشخاصی منعقد گردد؟

الف) کارکنان ب) اشخاص ثالث ج) پیمانکاران د) همه موارد

پاسخ‌نامه

پیش‌آزمون جلسه پانزدهم

:

	الف	ب	ج	د
۱				
۲				

تعهدنامه عدم افشای اطلاعات (NDA)

:

تعهدنامه عدم افشای اطلاعات (NDA) یک توافق‌نامه است که بین حداقل دو طرف حاصل می‌شود و براساس آن یکی از طرفین و یا هر دو توافق می‌کنند که یک رشته اطلاعات محرمانه شامل دانش و اطلاعات که به منظور خاصی به طرف مقابل عرضه می‌گردد، بازنشر نداشته باشد و صرفاً در همان منظور خاص مورد استفاده قرار گیرد. منظور از اطلاعات محرمانه، اطلاعاتی است که افشای آنها امنیت سیستم را به خطر می‌اندازد، ممکن است ضرر مالی به طرفین وارد نماید و یا اسرار و مزیت‌های رقابتی هر یک از طرفین را افشا نماید. اطلاعات محرمانه می‌تواند شامل اطلاعات دارایی‌ها، برنامه‌ها، فرایند انجام کارها، اهداف یک سازمان و یا اطلاعات در مورد نقاط ضعف آن سازمان باشد.

در واقع این نوع توافق، اطمینان دو طرفه‌ای برای به اشتراک گذاری اطلاعات، دانش و اسرار تجاری در قراردادهای همکاری فیمابین، بدون نگرانی از افشای آن ها نزد شخص سوم ایجاد می‌نماید.

افشای اطلاعات به معنای استفاده غیرمجاز و یا دراختیار قرار دادن آن به افراد غیرمجاز است. پس، باید محافظت لازم در قبال جلوگیری از افشای اطلاعات انجام شود تا از دسترسی افراد غیرمجاز محفوظ باشد. استفاده غیرمجاز به معنای استفاده در اموری غیر از قرارداد و یا توافق همکاری مربوطه است.

تعهدنامه عدم افشای اطلاعات (NDA) عمدتاً میان سازمان و پرسنل، پیمانکاران و سایر افراد حقیقی یا حقوقی (اشخاص ثالث) که به نوعی به اطلاعات محرمانه و حساس سازمان دسترسی دارند، منعقد می‌گردد. تعهدنامه عدم افشای اطلاعات می‌تواند در قالب یک ماده در داخل قرارداد اصلی و یا در قالب یک سند توافق‌نامه مجزا به امضای طرفین قرارداد و یا همکاری برسد.

تعهدات عمده طرفین قرارداد در تعهدنامه عدم افشای اطلاعات (NDA)

:

در تعهدنامه عدم افشای اطلاعات، طرفین قرارداد متعهد به پایبندی به مفاد زیر می‌باشند:

- حفظ و حراست از اطلاعات محرمانه و طبقه بندی شده و مستندات فنی و غیرفنی طرفین در برابر تهدیدات احتمالی همچون افشا و انتشار و آسیب رساندن به صحت اطلاعات دریافت شده
- حفظ همهٔ حقوق معنوی طرفین در خصوص اطلاعات و اسناد کسب شده

در ادامه به نکات کلیدی اطلاعیه بانک ملت در خصوص دریافت تعهدنامه عدم افشای اطلاعات اشاره می‌شود:

۱. در زمان عقد قرارداد میان بانک و سایر شرکت‌ها باید ماده‌ای با عنوان "تعهدات عدم افشای اطلاعات" وجود داشته باشد و در طول زمان همکاری با شرکت‌ها و همچنین پس از خاتمه تعهدات موضوع قرارداد، نسبت به اجرای مفاد این ماده، دقت و نظارت کافی معمول گردد.

۲. در صورت نیاز به ارائه دسترسی و یا انتقال اطلاعات طبقه‌بندی شده بانک به اشخاص حقیقی و حقوقی در قالب هر نوع تعامل و ارتباط فیمابین (برگزاری جلسات، مذاکرات تلفنی، مکاتبات الکترونیک یا چاپی، نامه‌های الکترونیک و ...) لازم است پیش از اعطای دسترسی، نسبت به تکمیل، امضا و نگهداری "تعهدنامه عدم افشای اطلاعات (اشخاص حقیقی و حقوقی)" اقدام شود.

یک نمونه از تعهدنامه عدم افشای اطلاعات (NDA) مورد استفاده در بانک، در ذیل درج شده است.

تعهدنامه عدم افشای اطلاعات (اشخاص حقیقی و حقوقی)

۱. شرکت/ فرد متعهد گردید، هرگونه اطلاعات طبقه بندی شده شامل همهٔ اطلاعات اعم از فنی، اداری، مالی، بازرگانی، شناسه و رمز دسترسی به سامانههای الکترونیک بانک که به صورت الکترونیک، مکتوب یا شفاهی و حسب ضرورت غیرقابل اجتناب در اختیار شرکت/ فرد قرار می گیرد و یا توسط شرکت/ فرد از سیستم‌هاي مختلف بانك استخراج می گردد را به صورت محرمانه نگهداري نموده و برای هیچ شخص حقیقی و حقوقی مگر پس از کسب موافقت کتبی بانک، افشای ننماید.

۲. شرکت/ فرد متعهد گردید، اقدامات لازم را به منظور جلوگیري از دسترسي افراد غیرمجاز به اطلاعات طبقه‌بندی شده بانك به عمل آورد.

۳. شرکت/ فرد متعهد گردید تا از هرگونه کپی، تکثیر اطلاعات طبقه بندی شده جز در راستای اجرای فعالیت های محوله اجتناب نماید و تعداد این کپی‌ها و تکثیرها نباید بیشتر از میزان نیاز جهت همکاری باشد.

۴. شرکت/ فرد متعهد گردید در صورت درخواست بانک، گزارشات اقدامات انجام شده در خصوص جلوگیری از عدم افشای اطلاعات طبقه بندی شده را به بانک ارائه نماید.

۵. شرکت/ فرد متعهد گردید همهٔ اصل مدارك، کپي‌ها، اطلاعات طبقه بندی شده یا دریافتي از طرف بانك به صورت مستندات مکتوب و یا برروي هر گونه ادوات ذخیره‌سازي (ازقبیل Floppy Disk، CD،DVD،Flash memory ، نوار ویدئو و کاست) را در صورت درخواست بانك بازگردانده و یا امحای ایمن آن ها را گواهي نماید.

۶. شرکت/ فرد مي‌بایست به محض ظن و یا کشف هرگونه استفاده و یا افشای غیرمجاز اطلاعات یا هر شکل دیگر نقض بندهاي این تعهدنامه از جانب خود، بانك را مطلع نموده و به هر روش ممکن با بانك در جهت بازیابي مالکیت اطلاعات همکاري نموده و مانع استفاده غیرمجاز آن در آینده گردد.

۷. بانک مجاز است با تشخیص خود، در ۱صورت ایراد خسارت ناشي از عدم پایبندي شرکت/ فرد به مفاد این تعهدنامه، به نحو مقتضي نسبت به ادعاي خسارت در محاکم قضائي و جبران خسارت اقدام نماید.

بانک حق دارد هرگونه خسارت مالي وارده به خود، ناشي از عدم اجراي این تعهدنامه را از هرگونه موجودي حساب و یا سایر اموال شرکت/ فرد نزد خود رأساً و بدون هیچ‌گونه تشریفات قانوني یا قضائي نموده و بابت جبران خسارات وارده به خود منظور نماید. صرف تشخیص و اعلام بانک نسبت به ورود خسارت و میزان آن مورد پذیرش شرکت/ فرد بوده و شرکت/ فرد حق هرگونه اعتراضي را دراین خصوص از خود سلب و اسقاط نمود.

۸. منظور از اطلاعات طبقه بندی شده در این تعهدنامه، همه اطلاعات برچسب گذاری شده غیر از برچسب طبقه عمومی می باشد.

شایان ذکر است اطلاعاتی که از سمت بانک به صورت شفاهی به عنوان اطلاعات دارای طبقه بندی اعلام و ارائه گردیده است نیز، مشمول تعهدات فوق می باشد.

۹. رعایت مفاد این تعهدنامه صرفاً محدود به زمان خاصی نبوده و از تاریخ امضای آن لازم الاجرا است و پس از تغییر یا خاتمه روابط کاري طرفین نیز همچنان به قوت خود باقي خواهد بود.

۱۰. شرکت/ فرد به موجب این تعهدنامه اقرار نمود که صلاحیت لازم جهت پذیرش و انجام موضوع این تعهد را دارد.

امضا و مهر شرکت / امضا فرد

تاریخ تنظیم تعهدنامه

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- با مفهوم تعهدنامه عدم افشای اطلاعات آشنا شدید.	
۲- با کاربردهای تعهدنامه عدم افشای اطلاعات آشنا شدید.	

خودآزمایی جلسه پانزدهم :

۱. کدامیک از جملات زیر در خصوص تعهدنامه عدم افشای اطلاعات (NDA) صحیح نمی‌باشد.
الف) لازم است پیش از اعطای دسترسی و یا انتقال اطلاعات طبقه‌بندی شده سازمان به اشخاص حقیقی و حقوقی در قالب هر نوع تعامل و ارتباط فیمابین، نسبت به تکمیل، امضا و نگهداری تعهدنامه عدم افشای اطلاعات ((NDA اقدام شود.
ب) تعهدنامه عدم افشای اطلاعات حتماً می‌بایست در قالب یک سند و قرارداد مجزا منعقد شود.
ج) تعهدنامه عدم افشای اطلاعات اطمینان دو طرفه ایجاد می‌کند تا طرفین به راحتی اطلاعات، دانش و اسرار تجاری خود را که در قرارداد همکاری فیمابین، بر روی آن توافق کرده‌اند به اشتراک بگذارند.
د) منظور از اطلاعات محرمانه در تعهدنامه عدم افشاء اطلاعات، اطلاعاتی است که افشای آن ها امنیت سیستم را به خطر می‌اندازد و یا ممکن است ضرر مالی به طرفین وارد نماید و یا اسرار و مزیت های رقابتی هر یک از طرفین را افشا نماید.

۲. تعهدات کلی در تفاهم نامه عدم افشای اطلاعات (NDA) شامل کدامیک از موارد زیر است؟
الف) عدم افشا و انتشار اسناد و اطلاعات محرمانه طرفین
ب) عدم آسیب رساندن به صحت اطلاعات دریافت شده
ج) حفظ همهٔ حقوق معنوی طرفین در خصوص اطلاعات و اسناد کسب شده
د) همه موارد

۳. چه زمانی لازم است تعهدنامه عدم افشای اطلاعات، تهیه و امضا شود؟
الف) پیش از اعطای دسترسی و یا انتقال اطلاعات طبقه‌بندی شده سازمان به اشخاص حقیقی و حقوقی
ب) در زمان عقد قرارداد میان سازمان و سایر شرکت‌ها
ج) در زمان عقد قرارداد میان سازمان و پرسنل
د) همه موارد

۴. کدامیک از موارد زیر در دامنه شمول تعهدنامه عدم افشای اطلاعات قرار نمی‌گیرند؟
الف) اطلاعات محرمانه ب) اطلاعات طبقه‌بندی شده ج) اطلاعات عمومی د) اسناد فنی پروژه

پاسخ‌نامه تشریحی

خودآزمایی جلسه پانزدهم

۱. پاسخ صحیح، گزینه «ب»

NDA می‌تواند در قالب یک ماده در داخل قرارداد اصلی و یا در قالب یک سند توافق‌نامه مجزا به امضای طرفین قرارداد برسد.

۲. پاسخ صحیح، گزینه «د»

- حفظ و حراست از اطلاعات محرمانه و طبقه بندی شده و مستندات فنی و غیرفنی طرفین در برابر تهدیدات احتمالی همچون افشا و انتشار و آسیب رساندن به صحت اطلاعات دریافت شده
- حفظ همهٔ حقوق معنوی طرفین در خصوص اطلاعات و اسناد کسب شده

۳. پاسخ صحیح، گزینه «د»

تعهدنامه عدم افشای اطلاعات (NDA) عمدتاً میان سازمان و پرسنل، پیمانکاران و سایر افراد حقیقی یا حقوقی (اشخاص ثالث) که به نوعی به اطلاعات محرمانه و حساس سازمان دسترسی دارند، منعقد می‌گردد.

۴. پاسخ صحیح، گزینه «ج»

اطلاعات عمومی

خلاصه فصل هفتم

جلسه شانزدهم

بر طبق تعاریف قانونی، سوءاستفاده از رایانه‌ها شامل هررفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار و انتقال داده را جرم رایانه‌ای می‌نامند. به‌عبارت دیگر، هر عمل مثبت یا منفی غیرقانونی که رایانه در آن ابزار یا موضوع جرم باشد، جرم رایانه‌ای خوانده می‌شود. جرایم رایانه‌ای را می‌توان به سه دسته تقسیم نمود:

۱. جرایمی که در آن ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شود، مانند: سرقت و تخریب

۲. جرایمی که در آن ها رایانه به عنوان ابزار ارتکاب جرم بکار گرفته می‌شود که معمولاً از طریق شبکه‌های رایانه‌ای و اینترنت رخ می‌دهند، مانند: کلاهبرداری، جعل و سرقت رایانه‌ای

۳. جرایمی که در فضای مجازی به وقوع می پیوندد اما آثار آن ها در دنیای واقعی ظاهر می‌شود، مانند: نفوذ غیرمجاز، شنود غیرمجاز، انتشار ویروس و کرم‌های رایانه‌ای

به منظور رسیدگی و بررسی جرایم رایانه‌ای و رسیدگی به شکایات افراد در خصوص این جرایم، قانون جرایم رایانه‌ای کشور، مشتمل بر ۵۶ ماده و ۲۵ تبصره در جلسه علنی در سال ۱۳۸۸ در مجلس شورای اسلامی تصویب و به تأیید شورای نگهبان رسید و دادسرای رسیدگی به جرایم رایانه‌ای مسئول رسیدگی به این جرایم می‌باشد.

با توجه به اهمیت حوزه بانکی از منظر نوع و اهمیت اطلاعات مورد استفاده و مخاطرات احتمالی پیش‌رو، بانک ملت نیز تخلفات الکترونیک حوزه فناوری اطلاعات را، در قالب شانزده تخلف با درجه اهمیت‌های متفاوت براساس طبقه‌بندی تخلفات آیین‌نامه انضباطی بانک دسته‌بندی و از سال ۱۳۹۳ در محتوای تخلفات آیین‌نامه انضباطی بانک درج نموده است و در صورت محرز شدن ارتکاب هر یک از این تخلفات توسط کارکنان، مطابق با طبقه تخلفاتی مربوطه و تنبیهات تعریف شده متناظر در آئین‌نامه انضباطی بانک، با فرد خاطی برخورد خواهد شد.

جلسه پانزدهم

تعهدنامه عدم افشای اطلاعات (NDA) توافق‌نامه ای است که بین حداقل دو طرف حاصل می‌شود و براساس آن یکی از طرفین و یا هر دو توافق می‌کنند که یک رشته اطلاعات محرمانه شامل دانش و اطلاعات که به منظور خاصی به طرف مقابل عرضه می‌گردد، بازنشر نداشته باشد و صرفاً در همان منظور خاص مورد استفاده قرار گیرد. اطلاعات محرمانه می‌تواند شامل اطلاعات دارایی‌ها، برنامه‌ها، فرایند انجام کارها، اهداف یک سازمان و یا اطلاعات در مورد نقاط ضعف آن سازمان باشد.

تعهدنامه عدم افشای اطلاعات (NDA) عمدتاً میان سازمان و پرسنل، پیمانکاران و سایر افراد حقیقی یا حقوقی (اشخاص ثالث) که به نوعی به اطلاعات محرمانه و حساس سازمان دسترسی دارند، منعقد می‌گردد. تعهدنامه عدم افشای اطلاعات می‌تواند در قالب یک ماده در داخل قرارداد اصلی و یا در قالب یک سند توافق‌نامه مجزا باشد و به امضای طرفین قرارداد و یا همکاری برسد.

در تعهدنامه عدم افشای اطلاعات، طرفین قرارداد متعهد به پایبندی به مفاد زیر می‌باشند:

- حفظ و حراست از اطلاعات محرمانه و مستندات فنی و غیرفنی طرفین در برابر تهدیدات احتمالی همچون افشا و انتشار اسناد و اطلاعات محرمانه و آسیب رساندن به صحت اطلاعات دریافت شده
- حفظ همهٔ حقوق معنوی طرفین در خصوص اطلاعات و اسناد کسب شده

در بانک ملت نیز، در صورت نیاز به ارائه دسترسی و یا انتقال اطلاعات طبقه‌بندی شده بانک به اشخاص حقیقی و حقوقی درقالب هر نوع تعامل و ارتباط فیمابین، لازم است پیش از اعطای دسترسی، نسبت به تکمیل، امضا و نگهداری "تعهدنامه عدم افشای اطلاعات (اشخاص حقیقی و حقوقی)" اقدام شود.

فصل اول: آشنایی با مفاهیم امنیت اطلاعات
فصل دوم: امنیت فیزیکی و محیطی
فصل سوم: تهدیدات امنیتی در شبکه های رایانه‌ای
فصل چهارم: امنیت در مقابله با تهدیدات فضای سایبری
فصل پنجم: امنیت تجهیزات قابل حمل
فصل ششم: توصیه های امنیتی در خدمات بانکی
فصل هفتم: جرایم رایانه‌ای و تعهدنامه عدم افشای اطلاعات

فصل هشتم

پیاده‌سازی امنیت در سازمان ها

جلسه شانزدهم:
سیستم مدیریت امنیت اطلاعات (ISMS)

جلسه هفدهم:
تشکیلات سازمانی امنیت و نقش نیروی انسانی در تأمین امنیت سازمان

جلسه هجدهم:
لزوم وجود سیاست های امنیتی و ضرورت انطباق با آن ها

جلسه شانزدهم

سیستم مدیریت امنیت اطلاعات (ISMS)

۱۸۷	اهداف یادگیری
۱۸۸	پیش آزمون
۱۹۰	راهکار مناسب تأمین امنیت اطلاعات
۱۹۲	سیستم مدیریت امنیت اطلاعات (ISMS)
۱۹۲	پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در بانک ملت
۱۹۷	خط مشی سیستم مدیریت امنیت اطلاعات (ISMS)
۱۹۸	میزان دستیابی به اهداف یادگیری
	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. با سیستم مدیریت امنیت اطلاعات آشنا شود.
۲. کاربرد و مفهوم خط‌مشی امنیت اطلاعات بانک ملت را درک نماید.

پیش‌آزمون جلسه شانزدهم :

۱. کدامیک از سیستم‌های مدیریتی زیر، به سازمان این امکان را می‌دهد تا بتوانند امنیت سیستم‌های خود را با به حداقل رساندن ریسک‌های تجاری کنترل نمایند؟

الف) سیستم مدیریت تداوم کسب و کار

ب) سیستم مدیریت امنیت اطلاعات

ج) سیستم مدیریت کیفیت

د) هیچ کدام

۲. کدامیک از موارد زیر درباره سیستم مدیریت امنیت اطلاعات صحیح نمی‌باشد؟

الف) باعث حفظ محرمانگی، یکپارچگی و در دسترس بودن اطلاعات می‌شود.

ب) باعث اطمینان از تداوم کسب و کار سازمان می‌شود.

ج) پیاده‌سازی آن منجر به افزایش هزینه‌های سازمان می‌شود.

د) امکان رقابت بهتر را با رقبا ایجاد می‌کند.

پاسخ‌نامه

پیش‌آزمون جلسه شانزدهم

:

	الف	ب	ج	د
۱				
۲				

راهکار مناسب تأمین امنیت اطلاعات

:

همانطور که برای سفر به یک کشور خارجی، برقرار بودن امنیت آن کشور یکی از مهم ترین معیارها برای انتخاب آنجا به عنوان مقصد می‌باشد و همین موضوع باعث ترغیب توریست‌ها برای سفر و سرمایه‌گذاری در آن کشور می‌شود، در مورد سازمان‌ها به ویژه بانک ها و مؤسسات مالی نیز موضوع به همین منوال است.
به عبارت دیگر مردم ترجیح می دهند در جایی سرمایه های مالی خود را نگهداری کنند که احتمال خطر کمتری داشته باشد. اگرچه در ظاهر ممکن است میزان پایداری و موفقیت کسب و کاری یک سازمان و یا بانک معیار انتخاب قرار بگیرد، امّا حفظ ملاحظات امنیتی در زیرساخت ها و خدمات در حال ارائه آن نیز تأثیر مستقیم در میزان شهرت و موفقیت سازمان دارد. علاوه برآن، در عصر کنونی و با توجه به سرعت تبادل وانتقال اطلاعات ، شرایط به گونه ای است که هرگونه ضعف یا نقص در امنیت اطلاعات یک خدمت، با سرعت غیر قابل کنترلی در جامعه نشر پیدا می کند و اکثریت جامعه هدف، از موضوع به نحوی مطلع می گردند.
پس، هرگونه کمبود یا بی توجهی در مقوله حفظ و ارتقای امنیت اطلاعات می تواند جایگاه رقابتی یک سازمان را تحت تأثیر قرار دهد.
بنابراین، برای بقای و حفظ جایگاه رقابتی یک سازمان در عرصه اجتماع و بر اساس آنچه در فصول قبل در مورد تهدیدات و راهکارهای آن مطرح شد، سازمان‌ها ناگزیر به دنبال یافتن راهکارهای مناسب جهت تأمین امنیت اطلاعات و ارتباطات خواهند بود.
لازم است بدانید ، برای پیاده‌سازی و برقراری امنیت، فقط توجه به مسائل فنی و تکنیکی کافی نیست، بلکه ایجاد سیاست‌های کنترلی و استاندارد کردن آن و همچنین ایجاد روال‌های صحیح و ارتقای فرهنگ سازمانی، سطح امنیت اطلاعات را بالا خواهد برد. اگر سازمان یا بانکی بتواند مدل و راهکار امنیتی مناسبی را به درستی پیاده‌سازی و مدیریت کند، در فضای کسب و کار و مواجهه با مشتریان خود با ریسک کمتری رو به رو خواهد شد. بنابراین، می‌توان گفت انتخاب مدل و راهکار مدیریتی حفظ امنیت اطلاعات و فراهم آوردن شرایط اجرای آن راهکار، مهم ترین گام در ایجاد یک سیستم حفاظت از امنیت اطلاعات و پیوستگی ارائه خدمات در یک سازمان می‌باشد.
روش های فنی متفاوتی ازجنبه های مختلف برای حفظ و ارتقای امنیت وجود دارد که از جمله این راهکارها می توان به رمزنگاری اطلاعات، استفاده از نرم افزار ضدویروس، استفاده از دیوارآتش، بکارگیری سیاست‌های کنترل دسترسی، استفاده از رمزعبور مناسب، تهیه نسخ پشتیبان و ...، اشاره کرد که در فصول قبل نیز با مفاهیم و کاربرد آن ها آشنا شده ایم. اگرچه هر یک از این روش ها به تنهایی جنبه ای از حوزه فناوری اطلاعات را تحت پوشش قرار می دهند امّا نکته اصلی این است که مجموعه ای از راهکارهای امنیتی در فرایند امنیت اطلاعات لازم است و برای هماهنگی بیشتر بین اجزای مختلف ایجاد روال های مشخص و به عبارت بهتر روش های مدیریت امنیت اطلاعات نیاز می باشد. بنابراین، بهتر است مدلی را برای تأمین امنیت اطلاعات انتخاب نمود که مجموعه‌ای از راهکارهای امنیتی ونیز همه جوانب امنیت اطلاعات را پوشش دهد.

سیستم مدیریت امنیت اطلاعات (ISMS)

:

سیستم به معنی مجموعه‌ای از اجزا است که برای رسیدن به هدف خاصی در کنار هم جمع شده‌اند. "سیستم مدیریت امنیت اطلاعات" نیز مجموعه‌ای از اجزائی است که برای رسیدن به هدف خاصی که در اینجا تأمین و مدیریت امنیت اطلاعات سازمان می‌باشد، در کنار هم جمع شده‌اند.
با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵ تحت عنوان ISO ۲۷۰۰۱ (که به اختصار آن را ISMS می نامند)، نگرش سیستماتیک و فرایندی به مقوله امنیت اطلاعات شکل گرفت. براساس این نگرش، تأمین امنیت اطلاعات در یک مجموعه سازماني، باید به صورت مداوم و مستمر در یک چرخه امن‌سازي براساس چرخه PDCA (چرخه دمینگ)، شامل مراحل طراحي و برنامه‌ریزی (Plan)، اجرا و پیاده‌سازي(Do) ، بررسی و ارزیابي(Check) و اقدام و اصلاح(Act) انجام گردد. براي این منظور لازم است هر سازمان براساس یک متدلوژي مشخص، ضمن تهیه

طرح‌هـا و برنامه‌هـاي امنيتـي مـورد نيـاز خـود، تشـكيلات لازم جهـت ايجـاد و تـداوم امنيـت اطلاعـات را نيـز ايجـاد نمـوده و نقش‌هـا و مسـئوليت‌هاى امنيتـى هـر يـک از كاركنـان در ايـن تشـكيلات سـازمانى را مشـخص نمايـد.

شكل ۱: چرخه PDCA يا چرخه دمينگ

مـدل مديريتـى پيشـنهاد شـده در سيسـتم مديريـت امنيـت اطلاعـات (ISMS)، از جملـه موفق‌تريـن مدل‌هـاى فراينـد محـور بـراى تأمـين امنيـت اطلاعـات مى‌باشـد. ايـن مـدل بـا تعريـف امنيـت و سياسـت‌گذارى‌هاى مربـوط بـه آن، بحـث در مـورد سـاختار سـازمانى و نهـاد امنيتـى و نقش‌هـا و مسـئوليت‌هاى امنيتـى كاركنـان، تعييـن چشـم انـداز و مأموريت‌هـاى امنيتـى سـازمان و مـوارد ديگـر از قبيـل شناسـايى و ارزيابـى ريسـک‌هاى امنيتـى، ايجـاد امنيـت و فرهنـگ سـازى در نيـروى انسـانى، امنيـت فيزيكـى و محيطـى، امنيـت عمليـات و ارتباطـات، كنـترل دسترسـى، امنيـت شـبكه هـا و انطبـاق بـا قوانيـن و مقـررات امنيتـى و ...، مـدل مديريتـى كارايـى را پيشـنهاد مى‌كنـد.
بنابرايـن، سيسـتم مديريـت امنيـت اطلاعـات، بـا انتخـاب كنترل‌هـاى امنيتـى كافـى و مناسـب، بـه مديـران ايـن امـكان را مى‌دهـد تـا بتواننـد امنيـت سيسـتم‌هاى خـود را بـا بـه حداقـل رسـاندن ريسـک‌هاى امنيتـى كنـترل نماينـد كـه به‌صـورت كلـى باعـث اطمينـان از تـداوم كسـب و كار سـازمان از طريـق جلوگيـرى و بـه حداقـل رسـاندن ريسـک‌ها و اثـرات حـوادث امنيتـى مى‌شـود.

شكل ۲: حوزه‌هاى كنترلى سيستم مديريت امنيت اطلاعات

ساير مزاياى حاصل از استقرار سيستم مديريت امنيت اطلاعات كه از اهداف پياده سازى آن در يک سازمان مى باشد، شامل موارد زير است :

- برقرارى امنيت اطلاعات و ارتباطات
- حفظ محرمانگى، يكپارچگى و در دسترس بودن اطلاعات (مثلث CIA)
- شناسايى، ارزيابى و حفاظت از دارايى‌هاى مهم همچون: اطلاعات، پرسنل، شهرت و اعتبار سازمان
- حفظ اطلاعات از بُروز تهديدات، آسيب پذيرى‌ها و ريسک‌ها در حد امكان
- ايجاد اطمينان بيشتر براى مديران، كاركنان، مشتريان و ساير ذينفعان سازمان در مورد امنيت اطلاعات
- كاهش هزينه از دست دادن اطلاعات
- آمادگى براى رو به رو شدن با حوادثى كه امنيت اطلاعات را به مخاطره مى اندازند
- كاهش هزينه‌هاى ترميم خسارات ناشى از حوادث امنيتى
- حصول اطمينان از تداوم كسب وكار سازمان
- امكان رقابت بهتر با رقبا

پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در بانک ملت

:

با توجه به اهمیت پیاده‌سازی فرایندهای امنیت اطلاعات در سازمان‌ها براساس آنچه پیش از این مطرح شد، بانک ملت از سال ۱۳۸۸ طراحی و استقرار سیستم مدیریت امنیت اطلاعات (ISMS) را در محدوده خدمات بانکداری اینترنتی آغاز نمود و درسال ۱۳۹۰ (به عنوان نخستین بانک ایرانی) موفق به دریافت گواهینامه بین‌المللی براساس استاندارد ISO ۲۷۰۰۱ گردید.

پس از دریافت موفقیت‌آمیز این گواهینامه و حسب الزامات مراجع بالادستی، مبنای اعتباردهی سیستم مدیریت امنیت اطلاعات از نظام بین المللی به نظام ملی مدیریت امنیت اطلاعات (نما) تغییر یافت و به این ترتیب دوره جدید توسعه و گسترش سیستم در قالب چرخه ای آغاز شد. با هدف ارتقای سطح امنیت خدمات بانکداری اینترنتی بانک و همچنین به منظور بهبود مستمر و جاری بودن چرخه PDCA، استقرار سیستم جدید از تیر ماه سال ۱۳۹۴ در محدوده خدمات بانکداری اینترنتی، آغاز و در تیرماه سال ۱۳۹۵ با موفقیت به پایان رسید و در بهمن ماه همان سال، بانک ملت موفق به دریافت گواهینامه ملی این سیستم (مورد تایید مرکز راهبردی دفتر ریاست جمهوری و سازمان فناوری اطلاعات ایران) گردید.

شکل ۳: گواهینامه سیستم مدیریت امنیت اطلاعات بانک ملت

خط‌مشی سیستم مدیریت امنیت اطلاعات (ISMS)

:

به منظور شفاف‌سازی اهداف کلان امنیتی مورد نظر در فرایند استقرار سیستم مدیریت امنیت اطلاعات در یک سازمان، سندی با عنوان "خط‌مشی سیستم مدیریت امنیت اطلاعات" تهیه می‌گردد. سند خط‌مشی سیستم مدیریت امنیت اطلاعات، یکی از اصلی‌ترین سیاست‌های امنیتی سازمان است. این سند بسیار کلان بوده و بیانگر تعهدات مدیریت و نقش‌ها و مسئولیت‌های کارکنان در جهت رسیدن به اهداف امنیتی سازمان می‌باشد. این سند که دربرگیرنده محدوده استقرار سیستم مدیریت امنیت اطلاعات، اهداف مورد نظر از استقرار سیستم و تشریح کننده وظایف و نقش مدیریت و کارکنان در قبال امنیت اطلاعات می‌باشد، با امضای مدیریت ارشد سازمان، رسمیت یافته و همهٔ کارکنان، پیمانکاران و ذینفعان سازمان، ملزم به تبعیت و پیروی از این خط‌مشی خواهند بود.

به عنوان نمونه و با توجه به استقرار سیستم مدیریت امنیت اطلاعات در محدوده خدمات بانکی غیرحضوری در بانک ملت، سند خط مشی توصیف شده با عنوان "بیانیه خط مشی سیستم مدیریت امنیت اطلاعات" تهیه و در

معـرض اطـلاع کارکنـان محـدوده اسـتقرار سیسـتم قـرار گرفتـه اسـت. بدیهـی اسـت در راسـتای بهبـود ایـن اسـناد و اهـداف تعریـف شـده در آن، لازم اسـت در ابتـدای اجـرای هـر چرخـهPDCA مـورد بررسـی قـرار بگیرنـد و در صـورت لـزوم بازنگـری شـوند. بیانیـه خـط مشـی سیسـتم مدیریـت امنیـت اطلاعـات بانـک ملـت در هشـت بنـد بـه شرح ذیـل تدویـن شـده اسـت:

۱. توسعه زیرساخت های فنی و سازمانی به منظور حفظ و بهبود مستمر تداوم کسب وکار

۲. راه انـدازی زیرسـاخت هـای مرکـز عملیـات امنیـت بانـک و اسـتقرار مدیریـت رخدادهـای امنیتـی بـا هـدف اتخـاذ راهکارهـای مناسـب جهـت پیشـگیری و مقابلـه بـا رخدادهـای امنیتـی

۳. آگاهی رسانی و گسترش فرهنگ امن اندیشی برای تمامی کارکنان و مشتریان بانک ملت

۴. تقویت زیرساخت های موثر امنیتی با تأکید بر حفظ محرمانگی اطلاعات و اسرار همهٔ ذینفعان و مشتریان بانک

۵. اتخاذ رویکرد مکانیزه و بهبود فرایند مدیریت تغییرات با محوریت ارزیابی ریسک های مترتبه

۶. ارتقـای سـطح امنیـت محصـولات و خدمـات ارائـه شـده توسـط شرکـت هـای پیمانـکار از طریـق اعـمال الزامـات امنیتـی در پیـمان هـای حقوقـی

۷. بهبود امنیت فیزیکی و محیطی مراکز داده بانک

۸. استقرار مدیریت ریسک در فرایند مدیریت پروژه های فناوری اطلاعات

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید،
در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- با سیستم مدیریت امنیت اطلاعات آشنا شدید.	
۲- کاربرد و مفهوم خط مشی امنیت اطلاعات بانک ملت را درک کردید.	

خودآزمایی جلسه شانزدهم :

۱. سیستم مدیریت امنیت اطلاعات کدامیک از موارد زیر را پوشش می‌دهد؟

الف) امنیت منابع انسانی

ب) امنیت عملیات و ارتباطات

ج) امنیت فیزیکی و محیطی

د) همه موارد

۲. کدامیک از افراد زیر می‌بایست از خط‌مشی امنیت اطلاعات تبعیت کند؟

الف) مدیران ب) همهٔ کارکنان، پیمانکاران و ذینفعان سازمان ج)مدیرعامل د) کمیته امنیت

۳. محتوای خط‌مشی امنیت اطلاعات شامل کدامیک از موارد زیر می‌باشد؟

الف) نقش‌ها و مسئولیت های کارکنان در قبال امنیت اطلاعات

ب) اهداف سازمان از استقرار سیستم مدیریت امنیت اطلاعات

ج) تعهد مدیریت در جهت رسیدن به اهداف امنیتی سازمان

د) همه موارد

۴. جاهای خالی را با عبارات مناسب پُر کنید؟

سیستم مدیریت امنیت اطلاعات، با انتخاب ..... مناسب و با به حداقل رساندن ..... باعث اطمینان از ..... کسب و کار سازمان می‌شود.

الف) ریسک‌های امنیتی، کنترل‌های امنیتی، تداوم

ب) کنترل‌های امنیتی، ریسک‌های امنیتی، تداوم

ج) راهکارهای امنیتی، تداوم سازمان، امنیت

د) راهکارهای امنیتی، امنیت سازمان، تداوم

پاسخ‌نامه تشریحی

خودآزمایی جلسه شانزدهم

۱. پاسخ صحیح، گزینه «د»

سیستم مدیریت امنیت اطلاعات با تعریف امنیت و سیاست‌گذاری‌های مربوط به آن، بحث در مورد ساختار سازمانی و نهاد امنیتی و نقش‌ها و مسئولیت‌های امنیتی کارکنان، تعیین چشم‌انداز و مأموریت‌های امنیتی سازمان و موارد دیگر از قبیل شناسایی و ارزیابی ریسک‌های امنیتی، ایجاد امنیت در نیروی انسانی، امنیت فیزیکی و محیطی، امنیت عملیات و ارتباطات، کنترل دسترسی، امنیت شبکه¬ها و انطباق با قوانین و مقررات امنیتی و ...، مدل مدیریتی کارایی را پیشنهاد می‌کند.

۲. پاسخ صحیح، گزینه «ب»

همهٔ کارکنان، پیمانکاران و ذینفعان سازمان، ملزم به تبعیت و پیروی از خط‌مشی امنیت اطلاعات سازمان خواهند بود.

۳. پاسخ صحیح، گزینه «د»

سند خط‌مشی امنیت اطلاعات، دربرگیرنده اهداف سازمان از استقرار سیستم مدیریت امنیت اطلاعات بوده و بیانگر تعهدات مدیریت در جهت رسیدن به اهداف امنیتی سازمان و نقش‌ها و مسئولیت‌های کارکنان در قبال امنیت اطلاعات می‌باشد.

۴. پاسخ صحیح، گزینه «ب»

سیستم مدیریت امنیت اطلاعات، با انتخاب کنترل‌های امنیتی مناسب و با به حداقل رساندن ریسک‌های امنیتی، باعث اطمینان از تداوم کسب و کار سازمان می‌شود.

جلسه هفدهم

تشکیلات سازمانی امنیت و نقش نیروی انسانی در تأمین امنیت سازمان

۱۸۷	اهداف یادگیری
۱۸۸	پیش آزمون
۱۹۰	تشکیلات سازمانی امنیت اطلاعات
۱۹۲	شرح وظایف کلی ساختار امنیت اطلاعات بانک ملت
۱۹۲	نقش نیروی انسانی در تأمین امنیت اطلاعات
۱۹۷	میزان دستیابی به اهداف یادگیری
۱۹۸	خودآزمایی

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. تشکیلات سازمانی امنیت را بشناسد.
۲. اهمیت نقش نیروی انسانی در تأمین امنیت سازمان را درک کند.
۳. با نقش‌ها و مسئولیت‌های کلیدی کارکنان در قبال امنیت اطلاعات آشنا شود.

پیش‌آزمون جلسه هفدهم :

۱. حفظ امنیت اطلاعات، مسئولیتی مشترک بین ..... سازمان می‌باشد.

الف) مدیران

ب) همه پرسنل

ج) اعضای هیئت مدیره

د) سهامداران

۲. به نظر شما، کدامیک از موارد زیر می‌تواند بیش ترین احتمال آسیب به سیستم‌های اطلاعاتی را به خود اختصاص دهد؟

الف) خطاهای سهوی کارکنان

ب) خرابی تجهیزات

ج) کارکنان ناراضی

د) مورد الف و ج

پاسخ‌نامه

پیش‌آزمون جلسه هفدهم

:

	الف	ب	ج	د
۱				
۲				

تشکیلات سازمانی امنیت اطلاعات

:

استقرار و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) فرایندی است که مستلزم صرف بودجه و ایجاد ساختار و تشکیلات سازمانی مناسب می‌باشد. حفظ امنیت اطلاعات، مسئولیتی مشترک بین همه پرسنل سازمان است. لذا، لازم است کمیته یا واحدی خاص برای راهبری فعالیت‌های امنیتی و با تأکید بر ارائه تعاریف واضح و شفاف نقش‌ها و مسئولیت‌های ایشان، ایجاد شود. وظیفه این کمیته ترویج آموزه‌های امنیتی در سازمان از طریق ایجاد التزام و تعهد در کارکنان و تدارک منابع کافی برای آن می‌باشد.
از سوی دیگر ، بر اساس آنچه در فصول قبل فرا گرفته شد ، زمینه های آسیب پذیری در حوزه امنیت اطلاعات و به سبب آن راهکارهای مقابله ای متنوع و فراوانی وجود دارد که شناسایی ، اجرا و نظارت بر آن ها در سازمان های بزرگ، نیازمند ساختار و تشکیلات سازمانی مشخصی می باشد. بنابراین، همه سازمان‌های استفاده کننده از اطلاعات به ویژه بانک‌ها و موسسات مالی که جزو سازمان‌های بزرگ و دارای دارایی‌های اطلاعاتی مهم محسوب می‌شوند، باید جایگاه و تشکیلات سازمانی امنیت اطلاعات را تعریف نموده و نقش‌ها، مسئولیت‌ها و حوزه فعالیت آن را تعیین نمایند.
به این منظور و بر اساس نیازهای تعریف شده، در بانک ملت نیز به فراخور وسعت کسب وکار و بلوغ ایجاد شده ، تشکیلات سازمانی امنیت اطلاعات از سالیان پیش ایجاد شده است و بر اساس نیاز و تجارب کسب شده در طی این دوران ، در ساختار آن تغییرات لازم اعمال گردیده و نقش ها و مسئولیت های بخش های مختلف آن تشریح و تبیین شده اند.
ساختار امنیت اطلاعات و وظایف آن در سه سطح "راهبری و سیاست گذاری کلان" ، "مدیریت اجرایی" و "فنی و کارشناسی" توصیف می شود که در رأس این ساختار، وظایف راهبری و سیاست گذاری کلان با هدایت مدیران ارشد اجرا می شود و به ترتیب، وظایف مدیریت اجرایی و فنی و کارشناسی از طریق مدیران میانی و گروه های کارشناسی پیش بینی شده، انجام می گردد. در جهت پوشش نیازها، کمیته ای تحت عنوان "کمیته امنیت اطلاعات بانک" نیز قرار دارد که این کمیته از مدیران ارشد حوزه فناوری اطلاعات و سایر حوزه‌های موثر در سیاست گذاری، اجرا و نظارت تشکیل شده است و وظایف دبیری این کمیته بر عهده بخش امنیت اطلاعات است. این کمیته نقش ها و وظایف "سیاست گذاری و راهبری کلان در حوزه امنیت اطلاعات" ، "کمیته راهبردی سیستم مدیریت امنیت اطلاعات" و "کمیته عالی مدیریت رخداد" را در بانک برعهده دارد.

شرح وظایف کلی ساختار امنیت اطلاعات بانک ملت

:

بخش امنیت اطلاعات بانک ملت به عنوان متولی سیاست گذاری و نظارت در حفظ امنیت اطلاعات در بانک، مسئولیت تهیه، تدوین و ابلاغ سیاست‌ها و دستورالعمل‌های امنیتی، برنامه‌ریزی، هماهنگی، پیاده‌سازی راهکارهای امنیتی ، برنامه های آموزشی و آگاهی رسانی جهت ارتقای سطح دانش و فرهنگ امنیت اطلاعات کارکنان بانک و همچنین ارائه راهکارهای فرایند محور جهت شناسایی و مدیریت رخدادها و حوادث امنیتی ، ممیزی و نظارت بر امنیت سامانه‌ها و زیرساخت ها را بر عهده دارد.

نقش نیروی انسانی در تأمین امنیت اطلاعات

:

اگر سازمانی بهترین سیستم‌های سخت‌افزاری و تجهیزات امنیتی را بکار گیرد، امّا کاربران و یا عوامل انسانی، پارامترهای امنیتی را رعایت نکنند، آن سازمان در حوزه تأمین امنیت، کاری را از پیش نخواهد برد. این وضعیت مشابه این است که شما بهترین اتومبیل با درجه بالای امنیت را تهیه نمائید، امّا آن را در اختیار افرادی قرار دهید که نسبت به اصول اولیه رانندگی آگاه نباشند!
پس، سازمان چه کاری می‌بایست انجام دهد تا از فناوری‌های روز دنیا، استفاده مفیدی کند و در عین حال از تهدیدات مستقیم و یا غیرمستقیم متوجه آن ها نیز مصون باشد؟ قطعاً نقش نیروی انسانی که کاربران و استفاده‌کنندگان

مستقیم این نوع فناوری‌ها می‌باشند، بسیار محسوس و مهم خواهد بود و با وجود همه فناوری‌های امنیتی، کارکنان حلقه تکمیل کننده امنیت هستند و همه آن ها در قبال حفظ و ارتقای امنیت، مسئول می‌باشند.
بنابراین، هر یک از افرادی که به گونه‌ای به سیستم‌های اطلاعاتی سازمان دسترسی دارند، حرکت و یا اقدامات اشتباه آن ها (عمدی و سهوی) می‌تواند پیامدهای منفی در ارتباط با امنیت اطلاعات به‌دنبال داشته باشد، پس، لازم است مسئولیت هر یک از کارکنان و منابع انسانی مرتبط با سازمان، برای حفاظت از تجهیزات و دارایی‌های اطلاعاتی، توسط مراجعی در سازمان که نقش تبیین وظایف سازمانی را دارند مشخص گردد. به طور معمول وظایف کارکنان براساس پست و جایگاه سازمانی تعریف می شود که به این ترتیب ضروری است هر یک از پرسنل در جایگاه شغلی خود از وظایف محوله به خوبی آگاه گردد. همینطور ساختار امنیت اطلاعات با استفاده از ابزارها و امکانات تحت اختیار نظیر اطلاعیه ها، بروشور ، پوستر ، وب سایت های اینترانتی سعی در ارتقای دانش کارکنان در حوزه امنیت اطلاعات و آگاهی رسانی در زمینه وظایف مرتبط در این حوزه را بر عهده دارد. برای موفقیت فردی و سازمانی، این مهم است که هر یک از کارکنان به وضوح با نقش خود ارتباط برقرار کرده و آن را درک کند.
برخی از نقش‌های مورد انتظار از نیروی انسانی در حفظ و ارتقای امنیت اطلاعات به شرح ذیل خواهد بود:

- حفاظت و استفاده صحیح از دارایی‌ها و تجهیزات در اختیار
- حفظ امنیت دارایی‌های اطلاعاتی و عدم افشای اسرار و اطلاعات محرمانه سازمان
- گزارش‌دهی حوادث و نقض‌های امنیتی
- پاسخگویی در قبال پیامدهای ناشی از خطاهای امنیتی
- بکارگیری و اجرای سیاست‌ها و روال‌های امنیتی و رعایت قوانین و مقررات امنیتی حاکم بر سازمان
- حضور و مشارکت در دوره‌ها و سمینارهای آموزشی امنیت اطلاعات برگزار شده از طرف سازمان
- همکاری با کمیته امنیت و اعضای تشکیلات سازمانی امنیت سازمان

با وجود تمام ملاحظات امنیتی، ممکن است حوادث و نقض‌های امنیتی رخ دهد، لذا، در بانک ملت در کنار سایر وظایف بخش امنیت اطلاعات ، یک واحد کارشناسی با عنوان "واحد کارشناسی مدیریت رخداد" ایجاد شده تا در صورت بروز چنین حوادثی نسبت به انجام هماهنگی های لازم در جهت واکنش و رفع آن ها اقدام نماید. این واحد وظیفه دارد ، در صورت دریافت گزارش (گزارشاتی) از وقوع رخداد ، ضمن طبقه بندی آن بر اساس درجه اهمیت تعریف شده، اقدامات لازم را در راستای ارجاع به بخش های مرتبط (اعم از واحدهای داخلی یا شرکت های تابعه بانک)، هماهنگی بین بخش های مختلف ، برگزاری جلسات هماهنگی و
تصمیم گیری و پیگیری و پایش پاسخ مناسب و به موقع به رخداد انجام دهد . همچنین مسئولیت ارائه گزارش از علل وقوع رخداد، اقدامات انجام شده و میزان پیشرفت اقدامات واکنشی به مدیران و مراجع بالادستی نیز از وظایف واحد کارشناسی مدیریت رخداد است. برطبق آنچه پیش از این گفته شد، نقش مدیریتی در اتخاذ تصمیم های مهم و راهبردی در شرایط وقوع رخداد برعهده کمیته امنیت اطلاعات بانک است.
موارد ذیل، مثال‌هایی از حوادث امنیت اطلاعات می‌باشند:

- o تلاش براي دستيابي به يك دسترسي غيرمجاز به يک سامانه يا پايگاه اطلاعاتي
- o قطعي‌ها و خرابی‌هاي سرويس‌های حساس
- o اختلالات نرم افزاري يا سخت افزاري در تجهيزات که موجب اختلال در بخشی از فرايندهای کسب و کار گردند
- o نفوذ و يا امکان دسترسی‌های غيرمجاز به يک رايانه ، سامانه و يا يک خدمت
- o خطاهاي عمدی يا سهوی پرسنل که موجب نقض پارامترهای امنيتی شوند
- o خرابي‌های مشکوک در نرم افزارها يا سخت افزارها
- o تحريف و افشاي غيرمجاز اطلاعات

پس، با توجه به موارد ذکر شده، پیشرفت‌های فنی و تکنولوژی‌های امنیتی، همیشه تضمین کننده تأمین امنیت سازمان نیست، بلکه عوامل انسانی نقش بسیار مهمی برای امنیت اطلاعات سازمان بازی می‌کنند.
حفظ و ارتقای امنیت اطلاعات در سازمان با همکاری مناسب همه همکاران امکان‌پذیر خواهد بود.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱- با تشکیلات سازمانی امنیت آشنا شدید.	
۲- اهمیت نقش نیروی انسانی در تأمین امنیت سازمان را درک کردید.	
۳- با نقش‌ها و مسئولیت‌های کلیدی کارکنان در قبال امنیت اطلاعات آشنا شدید.	

خودآزمایی جلسه هفدهم :

۱. کدامیک از موارد زیر از وظایف نیروی انسانی در قبال امنیت اطلاعات می‌باشد؟

الف) بکارگیری و اجرای سیاست‌ها و روال‌های امنیتی و رعایت قوانین و مقررات امنیتی حاکم بر سازمان

ب) شرکت در دوره‌ها و سمینارهای آموزشی امنیت که از طرف سازمان تدارک دیده می‌شود

ج) همکاری با کمیته امنیت و اعضای تشکیلات سازمانی امنیت

د) همه موارد

۲. با وجود همه فناوری‌های امنیتی، ..... حلقه تکمیل کننده امنیت هستند و همه آن ها در قبال امنیت مسئول می‌باشند.

الف) کارکنان

ب) اشخاص ثالث

ج) اعضای هیئت مدیره

د) هیچ کدام

۳. کدامیک از موارد زیر از حوادث امنیت اطلاعات نمی‌باشد؟

الف) نفوذ یا دسترسی‌های غیرمجاز

ب) عدم رعایت خط‌مشي‌ها و دستورالعمل‌هاي فني و امنیتی

ج) استفاده از اطلاعات محرمانه

د) تحریف و افشاي غیرمجاز اطلاعات

۴. کدامیک از موارد زیر از وظایف تیم امنیت اطلاعات در بانک ملت می‌باشد؟

الف) تهیه، تدوین و ابلاغ سیاست‌ها و دستورالعمل‌های امنیتی

ب) پیاده‌سازی اقدامات و سامانه‌های امنیتی برای محافظت از اطلاعات

ج) ارائه راهکارهایی جهت شناسایی و مدیریت رخدادها و حوادث امنیتی

د) همه موارد

پاسخ‌نامه تشریحی

خودآزمایی جلسه هفدهم

۱. پاسخ صحیح، گزینه «د»

برخی از نقش‌های مورد انتظار از نیروی انسانی در تأمین امنیت اطلاعات به شرح ذیل خواهد بود:

- مسئولیت حفظ امنیت هریک از تجهیزات و دارایی‌های اطلاعاتی برعهده شخص استفاده کننده و کاربر آن می‌باشد. بنابراین، لازم است هر شخص به صورت روزانه، وضعیت امنیتی دارایی‌ها و سیستم‌های اطلاعاتی در اختیار خود را کنترل کرده و به سرعت نسبت به امکان بُروز خطاهای امنیتی واکنش نشان دهد.
- دارنده دارایی اطلاعاتی هیچ‌گاه مجاز به شانه خالی کردن در قبال پیامدهای ناشی از خطاهای امنیتی نمی باشد.
- بکارگیری و اجرای سیاست‌ها و روال‌های امنیتی و رعایت قوانین و مقررات امنیتی حاکم بر سازمان از وظایف اصلی کارکنان می‌باشد.
- کارکنان می‌بایست در دوره‌ها و سمینارهای آموزشی امنیت که از طرف سازمان تدارک دیده می‌شود، حضور پیدا کنند.
- همچنین باید با کمیته امنیت و اعضای تشکیلات سازمانی امنیت همکاری لازم را داشته باشند.

۲. پاسخ صحیح، گزینه «الف»

با وجود همه فناوری‌های امنیتی، کارکنان حلقه تکمیل کننده امنیت هستند و همه آنها در قبال امنیت مسئول هستند.

۳. پاسخ صحیح، گزینه «ج»

استفاده از اطلاعات محرمانه در صورت دارا بودن مجوزدسترسی ، رخداد محسوب نمی گردد.

۴. پاسخ صحیح، گزینه «د»

بخش امنیت بانک ملت به عنوان متولی سیاست گذاری ونظارت برامنیت اطلاعات در بانک، مسئولیت تهیه، تدوین و ابلاغ سیاست‌ها و دستورالعمل‌های امنیتی، برنامه ریزی، هماهنگی و پیاده‌سازی اقدامات و سامانه‌های امنیتی برای محافظت از اطلاعات، ارائه روش هایی جهت ارتقای سطح دانش و فرهنگ امنیت کارکنان بانک و همچنین ارائه راهکارهای فرایند محور جهت شناسایی و مدیریت رخدادها و حوادث امنیتی و همچنین ممیزی و نظارت بر امنیت سامانه‌ها و زیرساخت ها را بر عهده دارد.

جلسه هجدهم

لزوم وجود سیاست‌های امنیتی و ضرورت انطباق با آن‌ها

۱۸۷	اهداف یادگیری
۱۸۸	پیش آزمون
۱۹۰	سیاست‌های امنیتی و لزوم وجود آن‌ها
۱۹۲	ضرورت انطباق با سیاست‌های امنیتی
۱۹۲	میزان دستیابی به اهداف یادگیری
۱۹۷	خودآزمایی
۱۹۸	خلاصه فصل هشتم

اهداف یادگیری :

فراگیر پس از مطالعه این جلسه باید:

۱. نقش وجود سیاست‌ها در تأمین امنیت را درک کند.
۲. ضرورت انطباق با سیاست‌های امنیتی را بیان کند.

پیش‌آزمون جلسه هجدهم :

۱. کدامیک از مستندات زیر در اولویت هرم مستندات یک سازمان قرار دارد؟

الف) روش‌های اجرایی و دستورالعمل‌ها

ب) خط مشی‌ها و سیاست‌ها

ج) راهنماها

د) استانداردها

۲. انطباق با کدامیک از سیاست‌های امنیتی زیر برای یک سازمان الزامی است؟

الف) سیاست کنترل دسترسی

ب) سیاست مدیریت کلمه عبور

ج) سیاست مدیریت حوادث امنیتی

د) همه موارد

پاسخ‌نامه

پیش‌آزمون جلسه هجدهم

:

	الف	ب	ج	د
۱				
۲				

سیاست‌های امنیتی و لزوم وجود آن‌ها

:

همانطور که در زندگی شخصی، هر خانواده‌ای اصول و چارچوب مشخصی برای انجام امور مختلف زندگی از جمله تربیت فرزندان، خوردن غذا، پوشیدن لباس و سایر امور وجود دارد، هر سازمان نیز باید برای اداره امور مختلف از جمله تأمین امنیت، قوانین و چارچوب‌هایی را رعایت کند که اصطلاحاً به آن سیاست گفته می‌شود.

سیاست در ارتباط با مقوله امنیت، معاني زيادي دارد. سیاست امنیتی به معناي دستورات، قوانين و تصميمات سازمان براي ايجاد يك برنامه امنيتي، پايه‌ريزي اهداف و تخصيص مسووليت‌هاست. يك سیاست امنیتی ترکیبی از خواسته‌ها و فرهنگ سازمان و متأثر از اندازه و اهداف آن سازمان است. همهٔ سازمان‌ها به ویژه سازمان‌های بزرگ که شبکه‌های گسترده‌ای دارند، مانند بانک‌ها و موسسات مالی، باید سیاست‌های امنیتی خود را تدوین کنند و آن را به اجرا بگذارند.

پس از تعيين اهداف يك سازمان از استقرار امنيت اطلاعات، خط‌مشی‌ها و سياست‌هاي امنيتی جهت رسيدن به آن اهداف، تعيين می‌شود، سپس استانداردها و راهنماها و رويه‌ها و روش‌های اجرايی و دستورالعمل‌های امنيتي مربوطه براي پياده‌سازي آن سياست‌ها تدوين شده و توسعه می‌يابد و برای اجرا در اختيار كاربران قرار می‌گيرد. براي رسيدن به امنيت مورد نظر در سازمان، اين سياست‌ها بايد به‌طور كامل پياده‌سازي و اجرا شوند. بنابراين، لازم است سياست‌های امنيتی با دقت و توجه فراوان تدوين شوند؛ چرا كه هرگونه اشتباه در اين مرحله ممكن است برای امنيت سازمان مشكل ساز شود.

سیاست های یک سازمان در واقع مرجع سایر اسناد سازمان نظیر راهنماها و دستورالعمل هاست. به عبارت دیگر، سیاست ها در رأس هرم مستندات مرجع سازمانی قرار می گیرند. در متن سیاستنامه ها مجموعه ای از باید و نبایدهایی که می بایست مورد رعایت کارکنان قرار بگیرد، بیان شده است. بر اساس موضوع و حیطه تحت پوشش، برای یک سیاستنامه ، ممکن است مستندی با ده ها صفحه محتوا و یا اطلاعیه ای کوتاه برای مخاطبین خاص یا کل کارکنان یک سازمان تهیه و ابلاغ شود.

شکل ۴: هرم مستندات سازمانی

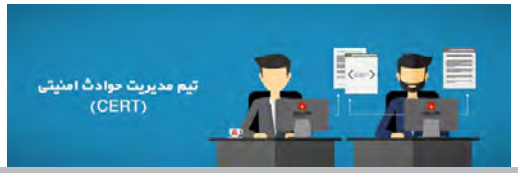
به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود، به این معنا که فرایند تکمیل، اصلاح و توسعه آن هیچ‌گاه متوقف نشده و متناسب با تغییر فناوری و نیازهای سازمان به‌روز می‌شود.

خط‌مشی‌ها و سیاست‌های امنیتی مختلفی در سازمان‌ها وجود دارد، از آن جمله مي‌توان به موارد زیر اشاره کرد:

• خط‌مشی امنیت اطلاعات: همانطور که در بخش قبلی اشاره شد، سند خط‌مشی امنیت اطلاعات، یکی از اصلی‌ترین سیاست‌های امنیتی سازمان است. این سند بسیار کلان بوده و بیانگر تعهدات مدیریت و نقش‌ها و مسئولیت‌های کارکنان در جهت رسیدن به اهداف امنیتی سازمان می‌باشد.

• خط‌مشی کنترل دسترسي: اين سياست مشخص مي‌كند چه افرادي اجازه دسترسي به منابع و دارايی‌های اطلاعاتی مختلف را دارند. سطح و ميزان دسترسي آن‌ها نيز در اين سياست مشخص مي‌شود. به این معنا که این افراد چه کاربری و به چه اطلاعاتی، چه نوع دسترسی، دارند.

• خط‌مشی مدیریت حوادث امنیتی: این سیاست، انواع حوادث و رخدادهای امنیتی را مشخص می‌کند. در این سیاست، اینکه رخداد ها و حوادث چگونه و به چه کساني گزارش داده شوند و همچنین چگونگی نحوه واکنش و پاسخ به رخدادهای امنیتی و نقش افراد و واحدها ، گنجانده می‌شود.



• خط‌مشی مدیریت کلمه عبور: نحوه شناسایی افراد و کاربران مختلفی که متقاضی ورود به شبکه و استفاده از منابع و دارایی‌های اطلاعاتی هستند را مشخص می‌کند. در این سیاست، نحوه انتخاب کلمات عبور، مدت اعتبار آن، تعداد و نوع کاراکترهای انتخابی و ...، تعیین می‌شود.

بهتر است بدانیم که سیاست های امنیتی براساس موضوع تحت پوشش و مخاطبان آن، دارای طبقه بندی محرمانگی اطلاعات هستند. یعنی برخی از سیاست نامه ها در طبقه اطلاعات محرمانه قرار دارند وفقط افراد دارای مجوز امکان دسترسی به آن ها را خواهند داشت و برخی از این اطلاعات در طبقه اطلاعات درون سازمانی به اطلاع همهٔ کارکنان می رسد. سیاست های دارای طبقه بندی محرمانه، معمولاً مرتبط با موضوعاتی نظیر ایجاد و نحوه نگهداری و سرویس دهی خدمات زیرساختی، سامانه ها و سرویس ها و یا نحوه اجرای برخی فرایندهای خاص مثل مدیریت رخدادهای امنیتی هستند. به طور معمول مستندات دارای طبقه بندی درون سازمانی از جمله سیاست نامه ها، پس از ابلاغ، به نحوی در دسترسی همیشگی کارکنان سازمان قرار می گیرند. برای مطلع و به روز بودن از این سیاست ها بهتر است، گاهاً به این مراجع که عموماً در قالب وب سایت های اینترانتی سازمان هستند، مراجعه شود.

ضرورت انطباق با سیاست‌های امنیتی

:

سیاست‌های امنیتی عمدتاً توسط بخش امنیت اطلاعات سازمان تدوین شده و سپس بر اساس نوع طبقه بندی محرمانگی اطلاعات آن به صورت اطلاعیه‌ها یا خط‌مشی‌های سازمانی به همهٔ کارکنان یا مخاطبان خاص ابلاغ می‌شوند. همانطور که در بخش قبل گفته شد، تمامی کارکنان سازمان نیز، به عنوان یکی از نقش‌ها و مسئولیت‌های خود، ملزم به اجرا و رعایت سیاست‌ها و روال‌های امنیتی سازمان می‌باشند. مسئولیت تهیه، تدوین و ابلاغ سیاست‌ها و دستورالعمل‌های امنیتی در بانک ملت، بر عهده بخش امنیت بانک است.

در واقع، سیاست‌های امنیتی سه نقش عمده را ایفا می‌کنند:

• مشخص می‌کنند از چه چیزی و چرا حفاظت می‌شود.

• مسوولیت‌های افراد در تأمین این حفاظت را مشخص می‌کنند.

• عواقب عدم پیروی از سیاست‌های امنیتی سازمان و نحوی برخورد با متخلفین را مشخص می‌کنند.

از آنجایی که مقوله امنیت در قالب یک چرخه مستمر همواره در جریان است، کارکنان سازمان نیز همواره باید به اجرا و رعایت سیاست ها و دستورالعمل های ابلاغ شده توجه نمایند. علاوه بر آن برای اطمینان از کفایت و اثربخشی اجرای سیاست ها و دستورالعمل های ابلاغ شده از یک سو و اطمینان از اجرای صحیح سیاست ها ودستورالعمل ها توسط کارکنان از سوی دیگر، لازم است سازمان، به‌طور منظم و مستمر، میزان انطباق با سیاست‌های امنیتی را بررسی و در صورت نیاز مورد بازنگری قرار دهد.

نحوه بررسی میزان انطباق با سیاست های بیان شده از طریق روش های پایش مکانیزه، ارزیابی های امنیتی سامانه ها و سرویس ها و همچنین در قالب برنامه های ممیزی حضوری توسط بخش امنیت انجام می شود. با این توضیحات و بر اساس آنچه پیش از این در مورد سیستم مدیریت امنیت اطلاعات (ISMS) مطرح شد، بهتر است بدانیم، در فرایند استقرار سیستم مدیریت امنیت اطلاعات (ISMS) سیاست های مرتبط بر اساس حوزه های تعریف شده در الزامات استاندارد، بیان می شوند که توسط کارکنان محدوده استقرار، اجرا شده و به منظور کنترل میزان انطباق الزامات تعریف شده و اثر بخشی آن ها به صورت دوره ای، توسط ممیزهای مورد تأیید مراجع صدور گواهی مورد ممیزی قرار می گیرند.

قابل توجه است که وجود سیاست‌های امنیتی بدون آنکه کارکنان نسبت به آن‌ها آگاهی کافی داشته باشند، نتایج مثبت و مشهودی را به دنبال نخواهد داشت. بنابراین، به منظور انطباق با سیاست‌های امنیتی باید فرایند مناسبی جهت آموزش، آگاهی و اطلاع‌رسانی به کارکنان وجود داشته باشد. بخشی از این فرایند، آموزش هایی در قالب برگزاری دوره های آموزشی، تهیه و انتشار کتاب و جزوات آموزشی، برگزاری آزمون و مسابقات انگیزشی، انتشار پوستر و اینفوگراف و ...، است تا از این طریق اطمینان حاصل شود کارکنان ضرورت کارهایی را که باید در راستای انطباق و اجرای سیاست‌ها و رویه‌های امنیتی انجام دهند دریافته اند و آن‌ها را رعایت می‌کنند. پس، همانطور که کیفیت تدوین سیاست ها، برنامه های آموزشی و اطلاع رسانی و روش های نظارتی در حفظ و

ارتقـای سـطح امنیـت کارکنـان موثـر اسـت، بـه همیـن میـزان توجـه کارکنـان بـه آمـوزش هـا و اطـلاع رسـانی هـای انجـام شـده و اجـرای صحیـح و کامـل الزامـات ابـلاغ شـده در حفـظ و ارتقـای سـطح امنیـت سـازمان قابـل توجـه بـوده وبسـیار پـر اهمیـت اسـت.

میزان دستیابی به اهداف یادگیری :

چنانچه در یادگیری اهداف زیر موفق بوده اید، گزینه تسلط را علامت ✓ بزنید، در غیر اینصورت متن را دوباره بخوانید.

اهداف یادگیری	تسلط
۱-نقش سیاست‌ها در تأمین امنیت را درک می‌کنید.	
۲- ضرورت انطباق با سیاست‌های امنیتی را بیان می کنید.	

خودآزمایی جلسه هجدهم :

۱. .....، بـه معنـاي دسـتورات، قوانـين و تصميـمات سـازمان بـراي ايجـاد يـك برنامـه امنيتـي، پايه‌ريـزي اهـداف و تخصيـص مسووليت‌هاسـت.

الف) روش‌های اجرایی ب) استانداردها ج) سیاست امنیتی د) دستورالعمل‌ها

۲.وظیفه تبعیت از سیاست‌های امنیتی برعهده کدامیک از موارد زیر می‌باشد؟

الف) همهٔ کارکنان ب) کمیته امنیت ج) کارکنان فناوری اطلاعات د) کارکنان حراست

۳. کدامیک از موارد زیر در مورد یک سیاست امنیتی صحیح نمی‌باشد؟

الف) یک سیاست امنیتی مشخص می‌کند از چه چیزی حفاظت می‌شود و چرا حفاظت می‌شود.

ب) یک سیاست امنیتی برای هر سازمان یکبار تدوین می شود و نیاز به بازنگری و پایش مستمر ندارد.

ج) یک سیاست امنیتی مسوولیت‌های افراد در تأمین امنیت اطلاعات را مشخص می‌کند.

د) یک سیاست امنیتی عواقب عدم پیروی از قوانین امنیتی سازمان را مشخص می‌کند.

۴. کدامیـک از سیاسـت‌های امنیتـی زیـر مشـخص می‌کنـد چـه کاربـری، بـه چـه اطلاعاتـی چـه نـوع دسترسـی، دارد؟

الف) سیاست مدیریت کلمه عبور

ب) سیاست مدیریت حوادث امنیتی

ج) سیاست کنترل دسترسی

د) هیچ کدام

پاسخ‌نامه تشریحی

خودآزمایی جلسه هجدهم

:

۱. پاسخ صحیح، گزینه «ج»

سیاست امنیتی، به معنای دستورات، قوانین و تصمیمات سازمان برای ایجاد یک برنامه امنیتی، پایه‌ریزی اهداف و تخصیص مسوولیت‌هاست.

۲. پاسخ صحیح، گزینه « الف »

وظیفه تبعیت از سیاست‌های امنیتی بر عهده همهٔ کارکنان سازمان می‌باشد.

۳. پاسخ صحیح، گزینه «ب»

به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود، به این معنا که فرایند تکمیل، اصلاح و توسعه آن هیچ‌گاه متوقف نشده و متناسب با تغییر فناوری و نیازهای سازمان به‌روز می‌شود.

۴. پاسخ صحیح، گزینه «ج»

سیاست کنترل دسترسی مشخص می‌کند چه کاربری، به چه اطلاعاتی چه نوع دسترسی، دارد.

خلاصه فصل هشتم

جلسه شانزدهم

انتخاب مدل و راهکار مدیریتی حفظ امنیت اطلاعات و فراهم آوردن شرایط اجرای آن راهکار، مهم ترین گام در ایجاد یک سیستم حفاظت از امنیت اطلاعات و پیوستگی ارائه خدمات در یک سازمان است.

مدل‌ها و راهکارهای مدیریتی مختلفی در زمینه حفظ امنیت اطلاعات وجود دارد. مدل مدیریتی پیشنهاد شده در سیستم مدیریت امنیت اطلاعات (ISMS)، بهترین راهکار برای تأمین امنیت اطلاعات می‌باشد. این مدل با تعریف امنیت و سیاست گذاری‌های مربوط به آن، بحث در مورد ساختار سازمانی و نهاد امنیتی و موارد دیگر از قبیل روش‌های ارزیابی ریسک، ایجاد امنیت و فرهنگ سازی در نیروی انسانی، امنیت فیزیکی، کنترل دسترسی، امنیت شبکه¬ها و انطباق با قوانین و مقررات و ممیزی امنیت، مدل مدیریتی کارایی را پیشنهاد می-کند.

سیستم مدیریت امنیت اطلاعات مبتنی بر استاندارد ISO ۲۷۰۰۱ بوده و با انتخاب کنترل‌های امنیتی کافی و مناسب، به مدیران این امکان را می‌دهد تا بتوانند امنیت سیستم‌های خود را با به حداقل رساندن ریسک‌های امنیتی، کنترل نمایند.

در این راستا، بانک ملت به عنوان نخستین بانک ایرانی موفق به پیاده‌سازی ISMS در محدوده خدمات بانکداری اینترنتی و دریافت گواهینامه این سیستم براساس استاندارد ISO ۲۷۰۰۱ شده است.

جلسه هفدهم

استقرار و پیاده‌سازی سیستم مدیریت امنیت اطلاعات فرایندی است که مستلزم صرف بودجه و ایجاد ساختار و تشکیلات سازمانی مناسب می‌باشد.

حفظ امنیت اطلاعات، مسئولیتی مشترک میان همه پرسنل سازمان می‌باشد. لذا، لازم است کمیته یا واحدی خاص برای راهبری فعالیت‌های امنیتی و با تأکید بر ارائه تعاریف واضح و شفاف نقش‌ها و مسئولیت‌های ایشان، ایجاد شود. بنابراین، همه سازمان‌های استفاده کننده از دارایی‌های اطلاعاتی باید جایگاه و تشکیلات سازمانی امنیت اطلاعات را تعریف نموده و نقش‌ها، مسئولیت‌ها و حوزه فعالیت آن را تعیین نمایند. بانک ملت نیز دارای تشکیلات سازمانی امنیت اطلاعات با شرح وظایف و مسئولیت‌های مشخص می‌باشد.

همچنین، نقش نیروی انسانی به عنوان کاربران و استفاده کنندگان مستقیم دارایی‌های اطلاعاتی، بسیار محسوس و مهم خواهد بود. برخی از نقش‌های مورد انتظار از نیروی انسانی در تأمین امنیت اطلاعات به شرح ذیل خواهد بود:

- حفاظت و استفاده صحیح از دارایی‌ها و تجهیزات در اختیار
- حفظ امنیت دارایی‌های اطلاعاتی و عدم افشاء اسرار و اطلاعات محرمانه سازمان
- گزارش‌دهی حوادث و نقض‌های امنیتی
- پاسخگویی در قبال پیامدهای ناشی از خطاهای امنیتی
- بکارگیری و اجرای سیاست‌ها و روال‌های امنیتی و رعایت قوانین و مقررات امنیتی حاکم بر سازمان
- حضور و مشارکت در دوره‌ها و سمینارهای آموزشی امنیت اطلاعات برگزار شده از طرف سازمان
- همکاری با کمیته امنیت و اعضای تشکیلات سازمانی امنیت سازمان

جلسه هجدهم

:

سیاست امنیتی به معنای دستورات، قوانین و تصمیمات سازمان برای ایجاد یک برنامه امنیتی، پایه‌ریزی اهداف و تخصیص مسوولیت‌ها می‌باشد. کلیه سازمان‌ها به‌خصوص سازمان‌های بزرگ که شبکه‌های گسترده‌ای دارند، مانند بانک‌ها و موسسات مالی، باید سیاست‌های امنیتی خود را تدوین کنند و آن را به اجرا بگذارند.

خط‌مشی‌ها و سیاست‌های امنیتی مختلفی مانند سیاست کنترل دسترسی، سیاست گزارش حوادث و تخلفات امنیتی، سیاست مدیریت کلمه عبور و... در سازمان‌ها وجود دارد.

سیاست‌های امنیتی عمدتاً توسط بخش امنیت اطلاعات سازمان تدوین شده و سپس به صورت اطلاعیه‌ها یا خط‌مشی‌های سازمانی به کارکنان ابلاغ می‌شود.

سیاست‌های امنیتی سه نقش عمده را ایفا می‌کنند:

- مشخص کنند از چه چیزی و چرا حفاظت می‌شوند.
- مسوولیت‌های افراد را در تامین این حفاظت مشخص می‌کنند.
- عواقب عدم پیروی از سیاست‌های امنیتی سازمان و نحوه برخورد با متخلفین را مشخص می‌کند.

لازم است سازمان، به‌طور منظم و مستمر، میزان انطباق با سیاست‌های امنیتی را بازنگری کند تا از کفایت و اثربخشی اجرا و بکارگیری سیاست‌های امنیتی توسط پرسنل خود، اطمینان حاصل نماید.

به منظور انطباق با سیاست‌های امنیتی باید فرایند مناسبی جهت آگاهی و اطلاع‌رسانی به پرسنل وجود داشته باشد و پرسنل سازمان در رابطه با آن سیاست‌ها آموزش ببینند.

فهرست منابع :

اکبصورت‌های مالی، انتشارات سازمان حسابرسی.