# ICDL IT security

این سند حاوی برنامه درسی ICDL IT Security می‌باشد. این برنامه درسی به واسطه نتایج یادگیری که به وجود می‌آورد بیانگر دانش و مهارت‌هایی است که داوطلب باید در ICDL IT security داشته باشد. این برنامه درسی مبنایی برای آزمون تئوری و عملی این ماژول می باشد.

## اهداف ماژول

در ماژول ICDL IT security داوطلب باید مفاهیم اصلی کاربرد امن ICT در زندگی روزمره را بشناسد و از تکنیک ها و برنامه های مرتبط برای داشتن یک اتصال امن شبکه استفاده کند، اینترنت را به صورت صحیح و مطمئن به کاربرد و داده‌ها و اطلاعات را به شیوهای مناسب مدیریت نماید. داوطلبان قادر خواهند بود از ICT به صورت ایمن استفاده نموده و مشکلات امنیتی مربوط به استفاده از ICT را برطرف نمایند.

**داوطلبان قادر خواهند بود:**

- مفاهیم کلیدی مربوط به اهمیت اطلاعات و داده‌های ایمن، امنیت فیزیکی، محدوده شخصی و سرقت هویت را بشناسند.
- از یک کامپیوتر، ابزار یا شبکه در مقابل نرم افزارهای مخرب و دسترسی غیر مجاز محافظت کنند.
- انواع شبکه‌ها اتصال‌ها و مسائل خاص شبکه از جمله firewall را بشناسند.
- در تار جهان گستر( world wide web) جستجو کنند و در اینترنت با امنیت ارتبا برقرار نمایند.
- با مسائل امنیتی مربوط به ارتباطات از جمله ایمیل و پیام فوری (IM) آشنا باشند.
- داده‌ها و اطلاعات را به صورت مناسب و مطمئن ذخیره کرده و از آنها پشتیبان بگیرند و داده‌ها و ابزارها را به صورت ایمن حذف نمایند.

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| 12.1 مفاهیم امنیت داده | 12.1.1 خطرات | 12.1.1.1 | تفاوت میان داده و اطلاعات را بدانند. |

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| | | 12.1.1.2 | مفهوم اصطلاح جرم الکترونیکی (cybercrime) را بدانید. |
| | | 12.1.1.3 | تفاوت میان هک کردن، شکستن قفل ( cracking) و هک کردن اخلاقی (جهت ارزیابی میزان امنیت سیستم توسط مدیر سیستم)را بدانید. |
| | | 12.1.1.4 | تهدیدات غیر قابل پیشگیری داده مثل آتش سوزی، سیل، جنگ و زلزله را تشخیص دهید. |
| | | 12.1.1.5 | تهدیدات داده از سوی، کارمندان، ارائه دهندگان خدمات و افراد خارج از مجموعه را تشخیص دهید. |
| | 12.1.2 ارزش اطلاعات | 12.1.2.1 | دلایل حفاظت از اطلاعات شخصی مثل جلوگیری از سرقت هویت، کلاهبرداری را بدانید. |
| | | 12.1.2.2 | دلایل حفاظت از اطلاعات حساس تجاری مثل جلوگیری از سرقت یا سوء استفاده از جزئیات مشتریان، اطلاعات مالی را بدانید. |
| | | 12.1.2.3 | اقدامات جلوگیری از دسترسی غیر مجاز به داه نظیر کد گذاری و رمز عبور را تشخیص دهید. |
| | | 12.1.2.4 | ویژگی‌های اساسی امنیت اطلاعات مانند محرمانه بودن، یکپارچگی و در دسترس بودن را بشناسید. |
| | | 12.1.2.5 | شرایط اصلی حفاظت، ابقا و کنترل داده / حریم شخصی در کشور خود را بدانید. |
| | | 12.1.2.6 | اهمیت ایجاد و پیروی از دستورالعمل‌ها و سیاست‌های استفاده از ICT را بدانید. |

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| | 12.1.3 اطلاعات شخصی | 12.1.3.1 | با اصطلاح مهندسی اجتماعی و تأثیرات آن مانند جمع‌آوری اطلاعات، کلاهبرداری، دسترسی به سیستم کامپیوتر آشنا باشید. |
| | | 12.1.3.2 | متدهای مهندسی اجتماعی مانند تماس‌های تلفنی، phishing, shoulder surfing را بدانید. |
| | | 12.1.3.3 | با مفهوم سرقت هویت وتأثیرات آن از جمله تأثیرات فردی، مالی، تجاری و قانونی آشنایی داشته باشید. |
| | | 12.1.3.4 | متدهای سرقت هویت مانند information diving, skimming و pretexting را بشناسید. |
| | 12.1.4 امنیت فایل | 12.1.4.1 | تأثیر فعال‌سازی/ غیر فعال سازی تنظیمات امنیتی ماکرو را بدانید. |
| | | 12.1.4.2 | برای فایل‌هایی مانند اسناد، فایل‌های فشرده، صفحات گسترده رمز عبور بگذارید. |
| | | 12.1.4.3 | مزایا و محدودیت‌های رمز گذاری (encryption) را بدانید. |
| Malware 12.2 | 12.2.1 تعریف و عملکرد | 12.2.1.1 | واژه نرم افزار مخرب (malware) را بشناسید. |
| | | 12.2.1.2 | روش‌های مختلفی که نرم افزار مخرب می‌تواند مخفی شود مانند تروجان‌ها، rootkits وback doors را بشناسید. |
| | 12.2.2 انواع | 12.2.2.1 | انواع نرم افزارهای مخرب سرایت کننده و نحوه کار آنها را تشخیص دهید: کرم‌ها، ویروس‌ها |
| | | 12.2.2.2 | انواع سرقت داده، نرم افزارهای مخرب سودآور/ اخاذی و |

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| | | | نحوه کار آنها را بشناسید مانند: adware، spyware، botnet، keystroke logging (واقعه نگاری) و dialler |
| | 12.2.3 محافظت | 12.2.3.1 | نحوه کار و محدودیت های نرم افزار آنتی‌ویروس را بدانید. |
| | | 12.2.3.2 | درایوها، پوشه‌ها و فایل‌های خاصی را با استفاده از نرم افزار آنتی ویروس اسکن کنید. با استفاده از نرم افزار برنامه زمانی اسکن‌ها را تعیین نمایید. |
| | | 12.2.3.3 | مفهوم قرنطینه (quarantine) و تأثیرات قرنطینه کردن فایل‌های آلوده/ مشکوک را بدانید. |
| | | 12.2.3.4 | اهمیت دانلود نصب نسخه‌های به روز شده نرم افزار و فایل‌های تعریف آنتی ویروس را بدانید. |
| 12.3 امنیت شبکه | 12.3.1 شبکه‌ها | 12.3.1.1 | با اصطلاح شبکه و انواع متداول شبکه مانند شبکه محلی (LAN)، شبکه گسترده (WAN)، شبکه مجازی خصوصی (VPN)، آشنا باشید. |
| | | 12.3.1.2 | نقش مدیر شبکه در مدیریت تأیید اعتبار (Authentication)، دادن مجوز و ایجاد account در داخل یک شبکه را بدانید. |
| | | 12.3.1.3 | عملکرد و محدودیت‌های یک firewall را بشناسید. |
| | 12.3.2 اتصالات شبکه | 12.3.2.1 | گزینه‌های اتصال به یک شبکه مانند کابل، بی‌سیم (wireless) را بشناسید. |
| | | 12.3.2.2 | بدانید که چگونه اتصال به یک شبکه بر امنیت تأثیر می‌گذارد. نرم افزار مخرب، دسترسی غیر مجاز به داده، |

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| | | | حفظ حریم شخصی |
| | 12.3.3.1 امنیت wireless | 12.3.3.1 | اهمیت درخواست رمز عبور برای حفاظت از دسترسی به شبکه wireless را بدانید. |
| | | 12.3.3.2 | انواع مختلف امنیت wireless را بشناسید از جمله : Wire Equivalent privacy (WEP) ، کنترل دسترسی به رسانه (MAC) |
| | | 12.3.3.3 | آگاه باشید که استفاده از شبکه wireless حفاظت نشده ممکن است باعث دسترسی افراد فرصت طلب به داده‌های شما گردد. |
| | | 12.3.3.4 | به یک شبکه wireless محافظت شده /محافظت نشده متصل شوید. |
| | 12.3.4.1 کنترل دسترسی | 12.3.4.1 | هدف از یک account شبکه و نیز نحوه دسترسی به آن از طریق نام کاربری و رمز عبور را بدانید. |
| | | 12.3.4.2 | سیاست‌های مناسب رمز عبور را بدانید از جمله : عدم به اشتراک گذاشتن رمز عبور با دیگران، تعویض منظم رمز عبور، رمز عبوری با تعداد حروف و اعداد مناسب، ترکیبی از اعداد مناسب، ترکیبی از اعداد و حروف خاص |
| | | 12.3.4.3 | تکنیک های متداول امنیت از طریق شناسایی اعضای بدن (biometric) در کنترل دسترسی را تشخیص دهید از جمله : اثر انگشت، اسکن چشم |
| 12.4 استفاده از وب امن و مطمئن | 12.4.1 مرورکردن وب | 12.4.1.1 | این نکته را بدانید که انجام فعالیت‌های آنلاین خاص (خرید،تبادلات مالی) فقط باید در صفحات وب امن انجام گیرد. |

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| | | 12.4.1.2 | وب سایت‌های امن را تشخیص دهید نظیر : https، علامت قفل |
| | | 12.4.1.3 | با pharming آشنا باشید. |
| | | 12.4.1.4 | با مفهوم مجوز دیجیتال آشنا باشید و یک مجوز دیجیتال را معتبر سازید. |
| | | 12.4.1.5 | مفهوم رمز عبور یکبارمصرف (one-time password) را بدانید |
| | | 12.4.1.6 | تنظیمات مناسبی برای فعال سازی، غیر فعال سازی تکمیل خودکار (Autocomplete) و ذخیره سازی خودکار (AutoSaved) در حین پر کردن فرم اعمال کنید. |
| | | 12.4.1.7 | با مفهوم cookie آشنا باشید. |
| | | 12.4.1.8 | تنظیمات مناسبی برای اجازه ورود، مسدود کردن cookie انتخاب نمایید. |
| | | 12.4.1.9 | داده‌های شخصی خاصی را از یک مرورگر پاک کنید مانند: History مرورگر، cookie داده‌هایی که در بخش تکمیل خودکار هستند. |
| | | 12.4.1.10 | هدف، عملکرد و انواع نرم افزارهای کنترل محتوا را بدانید: نرم افزار فیلتر کردن اینترنت، نرم افزار کنترل والدین |
| | 12.4.2 شبکه‌سازی اجتماعی | 12.4.2.1 | اهمیت آشکار ساختن اطلاعات محرمانه در سایت‌های شبکه‌های اجتماعی را بدانید. |

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| | | 12.4.2.2 | از نیاز به استفاده از تنظیمات مناسب برای حفظ حریم شخصی account در شبکه اجتماعی آگاه باشید. |
| | | 12.4.2.3 | خطرات احتمالی در هنگام استفاده از سایت‌های شبکه‌های اجتماعی را بدانید مانند: آزار اینترنتی، اطلاعات گمراه کننده / خطرناک، هویت‌های جعلی، پیام‌ها ولینک‌های کلاهبرداری |
| 12.5 ارتباطات | 12.5.1 پست الکترونیک | 12.5.1.1 | هدف از کدگذاری، باز کردن رمز یک ایمیل را بدانید. |
| | | 12.5.1.2 | مفهوم امضای دیجیتالی را بدانید. |
| | | 12.5.1.3 | یک امضای دیجیتالی ایجاد و اضافه نمایید. |
| | | 12.5.1.4 | از احتمال دریافت ایمیل‌های شیادانه و ناخواسته آگاهی داشته باشید. |
| | | 12.5.1.5 | مفهوم اصطلاح phishing را بدانید. ویژگیهای متداول phishing را تشخیص دهید : استفاده از اسم شرکت‌های قانونی، افراد، لینک‌های اشتباه وب |
| | | 12.5.1.6 | از خطر آلوده شدن کامپیوتر به نرم افزارهای مخرب به واسطه باز کردن فایل‌های ضمیمه ایمیل که حاوی ماکرو یا یک فایل اجرایی هستند آگاه باشید. |
| | 12.5.2 پیام‌های فوری | 12.5.2.1 | اصطلاح پیام فوری را بشناسید و از آن استفاده کنید. |
| | | 12.5.2.2 | با اصطلاح پیام فوری (IM) و کاربردهای آن آشنا باشید. آسیب‌های امنیتی IM را بشناسید از جمله: نرم افزارهای مخرب، دسترسی میان‌بر (backdoor access)، دسترسی به فایل‌ها |

| بخش | مجموعه مهارت | مرجع | موضوع کار |
|---|---|---|---|
| | | 12.5.2.3 | متدهای اطمینان از محرمانه بودن اطلاعات شخصی در حین استفاده IM را بشناسید: کد گذاری، عدم فاش کردن اطلاعات مهم، محدود ساختن به اشتراک گذاری فایل‌ها |
| 12.6 مدیریت امن اطلاعات | 12.6.1 ایمن‌سازی و پشتیبانی داده | 12.6.1.1 | روش‌های اطمینان از امنیت فیزیکی ابزارها را تشخیص دهید مانند: ثبت وقایع محل و جزئیات تجهیزات، استفاده از قفل‌های کابل، کنترل دسترسی |
| | | 12.6.1.2 | اهمیت داشتن یک پروسه پشتیبان‌گیری در صورت از بین رفتن داده‌ها، اسناد مالی، bookmark/ history وب را بدانید. |
| | | 12.6.1.3 | شناسایی ویژگیهای یک پروسه پشتیبان‌گیری مانند: منظم بودن (regularity)، تعداد دفعات (frequency)، برنامه زمانی(schedule)، محل ذخیره سازی(storage location) |
| | | 12.6.1.4 | از داده‌ها پشتیبان بگیرید. |
| | | 12.6.1.5 | بازیابی و اعتباردهی به داده‌های پشتیبان گرفته شده |
| | 12.6.2 تخریب امنیت داده | 12.6.2.1 | علت پاک کردن دائمی اطلاعات از درایوها و ابزارها را بدانید. |
| | | 12.6.2.2 | تفاوت میان پاک کردن و از بین بردن دائمی داده‌ها را بدانید. |
| | | 12.6.2.3 | متدهای متداول از بین بردن دائمی داده‌ها را بشناسید مانند: shredding، از بین بردن drive /media، degaussing، استفاده از برنامه‌های کاربردی از بین بردن داده‌ها. |