EUROPEAN COMPUTER DRIVING LICENCE / INTERNATIONAL COMPUTER DRIVING LICENCE - IT Security SYLABUS 1.0 (M12)

Upozornění:

Oficiální znění ECDL/ICDL Sylabu IT Security 1.0 je publikováno na webových stránkách ECDL Foundation - www.ecdl.org a jeho lokalizovaná verze na webových stránkách pracovní skupiny ECDL-CZ - www.ecdl.cz.

Přes veškerou péči, kterou ECDL Foundation (vlastník práv konceptu ECDL) a společnost CertiCon a.s. (národní sublicenciát) věnovaly přípravě a lokalizaci tohoto Sylabu, ECDL Foundation ani CertiCon a.s. neručí za kompletnost informací v něm obsažených a také nezodpovídají za jakékoli chyby, vynechaný text, nepřesnosti, ztrátu nebo poškození informací , instrukcí či pokynů v tomto Sylabu obsažených. Tento Sylabus nesmí být reprodukován jako celek ani po částech bez předchozího souhlasu vlastníků práv. ECDL Foundation může na základě vlastní úvahy a kdykoli bez ohlášení provádět jakékoli změny.

Modul 12 Bezpečnost při využívání informačních a komunikačních technologií

Modul č. 12 ECDL IT Security Sylabu 1.0, *Bezpečnost při využívání informačních a komunikačních technologií (IT Security),* definuje základní rozsah teoretických znalostí a praktických dovedností nutných pro úspěšné složení testu ECDL z tohoto modulu.

Cíle modulu

Modul 12

Bezpečnost při využívání informačních a komunikačních technologií - vyžaduje, aby uchazeč porozuměl základním principům bezpečného využívání informačních a komunikačních technologií v každodenním životě, uměl používat odpovídající techniky a aplikace pro zajištění bezpečného připojení k počítačové síti, spolehlivě a bezpečně používat Internet a odpovídajícím způsobem spravovat data. Úspěšný absolvent bude dobře připraven na bezpečnou práci s informačními a komunikačními technologiemi, bude schopen spolehlivě dodržovat bezpečnostní pravidla a rozpoznat běžné bezpečnostní problémy, které se mohou při využívání těchto technologií vyskytnout.

Uchazeč by měl být schopen…

- Pochopit základní pojmy týkající se důležitosti zabezpečení informací a dat, fyzické bezpečnosti, ochrany osobních údajů a krádeží identity.
- Zabezpečit počítač, datová média nebo počítačovou síť před účinky škodlivých programů a před neoprávněným přístupem.
- Znát druhy počítačových sítí, druhy připojení k těmto sítím a základní problematiku sítí, zejména firewallů.
- Bezpečně se pohybovat a komunikovat na síti Internet.
- Chápat bezpečnostní rizika týkající se zejména komunikace prostřednictvím elektronické pošty a komunikace na síti v reálném čase.
- Správně a bezpečně zálohovat data, obnovovat data ze zálohy, bezpečně odstraňovat data a mazat datová média.

KATEGORIE		OBLAST ZNALOSTÍ		ODKAZ	ROZSAH ZNALOSTI
12.1	**Koncepce bezpečnosti**	*12.1.1*	*Ohrožení dat*	12.1.1.1	Rozlišovat mezi pojmy data a informace.
				12.1.1.2	Rozumět pojmu počítačová kriminalita.
				12.1.1.3	Rozumět rozdílu mezi pojmy hacking, cracking a etický hacking.
				12.1.1.4	Chápat nebezpečí ohrožení dat z vyšší moci, jako je požár, záplavy, válka, zemětřesení.
				12.1.1.5	Rozpoznat nebezpečí ohrožení dat ze strany zaměstnanců, poskytovatelů služeb připojení na Internet a externích osob.
		12.1.2	*Hodnota informace*	12.1.2.1	Rozumět důvodům pro ochranu osobních údajů, jako jsou krádeže identity nebo finanční podvody.
				12.1.2.2	Rozumět důvodům pro ochranu obchodně citlivých informací jako jsou odcizení nebo zneužití klientských údajů nebo odcizení finančních informací.
				12.1.2.3	Znát opatření k zabránění neoprávněného přístupu k datům, jako jsou šifrování nebo používání hesel.
				12.1.2.4	Rozumět základním charakteristikám informační bezpečnosti, jako je důvěrnost, integrita, dostupnost.
				12.1.2.5	Znát hlavní principy a zásady pro ochranu, uchovávání a řízení přístupu k datům a osobním informacím platné v České republice.
				12.1.2.6	Chápat význam vytváření a dodržování obecných zásad bezpečnostní politiky pro použití informačních a komunikačních technologií.
		12.1.3	*Osobní bezpečnost*	12.1.3.1	Rozumět pojmu sociální inženýrství a jeho důsledkům, jako jsou například zneužití osobních informací, finanční podvody, získání neoprávněného přístupu.
				12.1.3.2	Rozumět metodám sociálního inženýrství, jako jsou napodobování telefonního hlasového automatu (IVR), podvrhování falešných zpráv (phishing) nebo odezírání z obrazovky (shoulder surfing).
				12.1.3.3	Rozumět pojmu krádež identity a jeho dopadům v oblasti osobní, finanční, obchodní a právní.

KATEGORIE		OBLAST ZNALOSTÍ		ODKAZ	ROZSAH ZNALOSTI
				12.1.3.4	Rozumět metodám krádeže identity, jako jsou information diving (obnovování smazaných dat, vyhledávání informací ve vyhozených datových médiích, ...), skimming (používání technických zařízení ke krádeži dat nebo přihlašovacích údajů, ...), pretexting (zneužívání vymyšlených scénářů k podvodu).
		12.1.4	*Bezpečnost souborů*	12.1.4.1	Rozumět důsledkům povolení / zakázání maker.
				12.1.4.2	Nastavení hesla pro soubory typu dokumenty, komprimované archivy a tabulky.
				12.1.4.3	Rozumět výhodám a nevýhodám šifrování souborů.
12.2	**Škodlivý software**	*12.2.1*	*Definice a funkce*	12.2.1.1	Rozumět pojmu malware (škodlivý software).
				12.2.1.2	Znát různé techniky, jakými se škodlivý software skrývá nebo pracuje, jako jsou trojské koně, softwarové maskování (rootkit), zadní vrátka (back door).
		12.2.2	*Typy*	12.2.2.1	Znát různé druhy "nakažlivého" škodlivého software, jako jsou počítačové viry nebo červi a rozumět tomu, jak fungují.
				12.2.2.2	Rozumět tomu, jak funguje škodlivý software typu adware (škodlivý reklamní software), spyware (software odesílající data bez vědomí uživatele), botnety (automaticky fungující škodlivý software) a odchytávání stisknutých kláves.
		12.2.3	*Ochrana*	12.2.3.1	Rozumět funkci antivirového programu a znát jeho omezení.
				12.2.3.2	Umět pomocí antivirového programu zkontrolovat diskovou jednotku, složku nebo soubory. Umět plánovat provedení antivirového testu.
				12.2.3.3	Rozumět pojmu karanténa a znát důsledky umístění infikovaných nebo podezřelých souborů do karantény.
				12.2.3.4	Chápat důležitost aktualizace antivirového programu a jeho virové databáze.
12.3	**Bezpečnost počítačových sítí**	*12.3.1*	*Počítačové sítě*	12.3.1.1	Rozumět termínu počítačová síť a rozlišovat běžné typy počítačových sítí, jako jsou místní síť (LAN), rozlehlé sítě (WAN), virtuální privátní sítě (VPN).
				12.3.1.2	Pochopit roli správce sítě při ověřování identity uživatelů sítě, údržbě a správě uživatelských účtů v rámci sítě.
				12.3.1.3	Rozumět pojmu firewall,jeho funkci a omezením.
		12.3.2	*Připojování k síti*	12.3.2.1	Rozlišovat možnosti připojení k síti, jako je připojení kabelem nebo bezdrátové připojení.
				12.3.2.2	Vědět, jaká bezpečnostní rizika může mít připojení k počítačové síti, jako je škodlivý software, neoprávněný přístup k datům a osobním údajům.
		12.3.3	*Zabezpečení bezdrátové sítě*	12.3.3.1	Chápat význam vyžadování hesla pro přístup k zabezpečené bezdrátové síti.
				12.3.3.2	Rozlišovat různé typy zabezpečení bezdrátové sítě, jako je Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).
				12.3.3.3	Uvědomovat si, že použití nezabezpečené bezdrátové sítě zvyšuje nebezpečí neoprávněného přístupu k vašim datům.
				12.3.3.4	Připojit počítač k zabezpečené / nezabezpečené bezdrátové síti.
		12.3.4	*Řízení přístupu k síti*	12.3.4.1	Porozumět účelu síťového účtu a chápat význam uživatelského jména a hesla pro přístup k počítačové síti.
				12.3.4.2	Znát zásady pro volbu hesel a pro práce s hesly, jako např. nesdílení hesla, pravidelná změna hesla, přiměřená délka hesla, vhodná struktura hesla (kombinace písmen, číslic a speciálních znaků).
				12.3.4.3	Znát techniky přístupu k síti na bázi kontroly biometrických údajů, jako je otisk prstu nebo sken oka.

KATEGORIE		OBLAST ZNALOSTÍ		ODKAZ	ROZSAH ZNALOSTI
12.4	**Bezpečné používání Internetu**	*12.4.1*	*Prohlížení webových stránek*	12.4.1.1	Uvědomovat si, že určité činnosti při práci s Internetem (online nákupy, finančních transakce) by měly být prováděny na zabezpečených webových stránkách.
				12.4.1.2	Vědět, jak rozpoznat zabezpečenou webovou stránku (protokol https nebo symbol zámku).
				12.4.1.3	Uvědomovat si, co znamená pojem pharming (technické povrhování webových stránek).
				12.4.1.4	Rozumět pojmu digitální certifikát. Vědět, jak ověřit digitální certifikát.
				12.4.1.5	Rozumět pojmu jednorázové heslo.
				12.4.1.6	Umět zvolit vhodné nastavení povolení / zakázání automatického dokončování a automatického ukládání při vyplňování formulářů.
				12.4.1.7	Rozumět pojmu cookie.
				12.4.1.8	Umět zvolit vhodné nastavení pro povolení nebo blokování cookies.
				12.4.1.9	Umět smazat soukromá data z prohlížeče, jako jsou historie prohlížení, cache (dočasné soubory), hesla, cookies, data automatického dokončování.
				12.4.1.10	Rozumět účelu, funkci a znát typy softwarové kontroly obsahu webových stránek, jako je filtrování obsahu a rodičovská kontrola.
		12.4.2	*Sociální sítě*	12.4.2.1	Chápat důležitost nesdělování důvěrných osobních informací na stránkách sociálních sítí.
				12.4.2.2	Uvědomovat si důležitost vhodného nastavení osobního účtu na sociální síti.
				12.4.2.3	Znát potenciální nebezpečí spojená s používáním sociálních sítí, jako jsou internetová šikana, přestírání cizí identity (grooming), zavádějící nebo nebezpečné informace, falešná totožnost, podvodné odkazy nebo zprávy.
12.5	**Komunikace**	*12.5.1*	*Elektronická pošta*	12.5.1.1	Rozumět důvodům pro šifrování zpráv elektronické pošty.
				12.5.1.2	Rozumět pojmu digitální podpis.
				12.5.1.3	Vytvořit digitální certifikát a podepsat jím zprávu elektronické pošty nebo dokument v příloze (docx, pdf).
				12.5.1.4	Uvědomovat si možnost přijetí podvodné nebo nevyžádané zprávy elektronické pošty.
				12.5.1.5	Rozumět pojmu phishing. Znát charakteristické znaky phishingu, jako je používání oficiálních názvů firem, používání jmen kompetentních osob, používání falešných webových odkazů.
				12.5.1.6	Uvědomovat si nebezpečí nákazy počítače škodlivým softwarem otevřením přílohy elektronické pošty, která obsahuje makro nebo spustitelný soubor.
		12.5.2	*Komunikace na síti v reálném čase*	12.5.2.1	Rozumět pojmu instant messaging (IM - komunikace na síti v reálném čase) a jeho použití.
				12.5.2.2	Chápat bezpečnostní rizika komunikace v reálném čase, jako je škodlivý software, přístup "zadními vrátky", neoprávněný přístup k datům.
				12.5.2.3	Znát zásady zabezpečení důvěrných informací při komunikaci na síti v reálném čase, jako jsou šifrování, nezveřejňování důležitých informací, zákaz sdílení souborů.
12.6	**Bezpečná správa dat**	*12.6.1*	*Bezpečnost a zálohování dat*	12.6.1.1	Znát způsoby, jak zajistit fyzickou bezpečnost zařízení s daty, jako umístění zařízení na vhodném místě, použití kabelových zámků, omezení a zabezpečení přístupu.
				12.6.1.2	Chápat, že je důležité mít záložní postup pro případ ztráty dat, finančních záznamů, webových záložek nebo historie procházení.

KATEGORIE	OBLAST ZNALOSTÍ	ODKAZ	ROZSAH ZNALOSTI
		12.6.1.3	Znát zásady správného zálohování, jako je pravidelnost a frekvence zálohování, plán zálohování, umístění datového úložiště.
		12.6.1.4	Umět zálohovat data.
		12.6.1.5	Umět obnovit a ověřit data ze zálohy.
	12.6.2 Bezpečná likvidace	12.6.2.1	Chápat důvody pro trvalé odstranění dat z disků a datových médií.
		12.6.2.2	Rozlišovat mezi mazáním a trvalým odstraněním dat.
		12.6.2.3	Znát metody pro trvalé odstranění dat jako jsou fyzická likvidace zařízení a médií, demagnetizace (degaussing), použití programových nástrojů na likvidaci dat.