Bezpečné používání informačních technologií (Cyber Security)
ECDL / ICDL Sylabus 2.1

Modul 12 Bezpečné používání informačních technologií

Sylabus 2.1, *Bezpečné používání informačních technologií,* definuje základní rozsah teoretických znalostí a praktických dovedností nutný pro úspěšné složení ECDL zkoušky z tohoto modulu.

Cíle modulu

Modul 12 Úspěšný absolvent zkoušky z tohoto modulu by měl být schopen:

- Pochopit, že je důležité udržet data a informace zabezpečené, znát hlavní způsoby ochrany osobních údajů a dat a ovládat principy zálohování a přístupu k datům.
- Uvědomovat si, že využívání webových úložišť a řady dalších služeb internetu je spojeno s rizikem zneužití osobních údajů a dat.
- Používat přístupová hesla a šifrovat soubory s daty nebo dokumenty.
- Chápat, že počítače, mobilní zařízení i servery v počítačových sítích mohou být napadeny škodlivými programy a znát základní typy škodlivých programů.
- Vědět, co je počítačová síť, znát základní způsoby zabezpečení bezdrátových sítí a umět používat osobní firewall a hotspot.
- Chránit počítač nebo mobilní zařízení před neoprávněným přístupem a být schopen bezpečně spravovat hesla.
- Umět nastavit a bezpečně používat webový prohlížeč a ověřovat bezpečnost webových stránek.
- Pochopit bezpečnostní problémy online komunikace, které mohou nastat při používání e-mailu, sociálních médií a mobilních zařízení.
- Zálohovat a obnovit data na libovolné zařízení nebo webové úložiště a bezpečně data smazat.

KATEGORIE	OBLAST ZNALOSTÍ	ODKAZ	ROZSAH ZNALOSTI
12.1 Koncepce bezpečnosti	*12.1.1 Ohrožení dat*	12.1.1.1	Chápat významový rozdíl mezi pojmy „data“ a „informace“.
		12.1.1.2	Rozumět pojmu „počítačová kriminalita“ a vědět, co znamená „hacking“.
		12.1.1.3	Rozpoznat nebezpečí úmyslného nebo náhodného ohrožení dat ze strany zaměstnanců, externích spolupracovníků, poskytovatelů připojení k internetu nebo spolupracujících organizací.
		12.1.1.4	Uvědomovat si, že mimořádné okolnosti, jako jsou požáry, povodně, ozbrojené konflikty nebo zemětřesení, mohou ohrozit data.
		12.1.1.5	Vědět, že používání webových (cloudových) úložišť může být spojeno s rizikem ztráty soukromí nebo zneužití přístupu provozovatele služeb k uloženým datům.
	12.1.2 Hodnota informací a dat	12.1.2.1	Chápat základní charakteristiky informační bezpečnosti, jako je důvěrnost, integrita a dostupnost.
		12.1.2.2	Chápat důvody pro ochranu osobních údajů, jako je možná krádež totožnosti, podvod nebo zneužití soukromí.
		12.1.2.3	Chápat důvody pro ochranu informací a dat uložených v počítačích nebo v dalších zařízeních na pracovišti, jako je krádež, zneužití, náhodná ztráta dat nebo sabotáž.
		12.1.2.4	Znát hlavní principy a zásady pro ochranu, uchovávání a řízení přístupu k datům a osobním údajům, jako jsou přehlednost, strukturované uspořádání nebo přístupová oprávnění.
		12.1.2.5	Rozumět pojmům „subjekt údajů“, „správce údajů“ a „zpracovatel údajů“ a vědět, jakými principy přístupu a uchovávání se ochrana dat a osobních údajů řídí.
		12.1.2.6	Chápat důležitost dodržování obecných zásad a pravidel bezpečnostní politiky pro používání informačních a komunikačních technologií.
	12.1.3 Osobní bezpečnost	12.1.3.1	Rozumět pojmu „sociální inženýrství“ a jeho důsledkům, jako jsou získání neoprávněného přístupu k počítači a k dalším zařízením, neoprávněné shromažďování informací nebo podvody.

KATEGORIE	OBLAST ZNALOSTÍ	ODKAZ	ROZSAH ZNALOSTI
		12.1.3.2	Rozumět metodám sociálního inženýrství, jako jsou napodobování telefonního hlasového automatu, podvrhování falešných zpráv nebo odkazů na falešné webové stránky (phishing) nebo odezírání z obrazovky (shoulder surfing).
		12.1.3.3	Rozumět pojmu „krádež totožnosti“ a jeho možným dopadům v oblasti osobní, finanční, obchodní nebo právní.
		12.1.3.4	Znát metody krádeže totožnosti, jako je obnovování smazaných dat, získávání informací z vyhozených datových nosičů (information diving), používání technických zařízení ke zjištění přihlašovacích údajů (skimming) nebo zneužívání vymyšlených scénářů k podvodu (pretexting).
	12.1.4 Bezpečnost souborů	12.1.4.1	Uvědomovat si důsledky povolení/zakázání spouštění maker.
		12.1.4.2	Rozumět výhodám a omezením šifrování souborů. Uvědomovat si nebezpečí vyzrazení šifrovacího klíče, hesla nebo digitálního certifikátu nebo jeho ztráty.
		12.1.4.3	Umět zašifrovat soubor, složku (adresář) nebo diskovou jednotku.
		12.1.4.4	Umět zabezpečit heslem dokument textového editoru, tabulku nebo komprimovaný archiv.
12.2 Škodlivé programy	*12.2.1 Druhy a techniky fungování*	12.2.1.1	Vědět, co znamená pojem „malware“. Znát různé techniky, jakými se škodlivé programy skrývají nebo jak se chovají, jako je technika trojského koně (Trojan), programového maskování (rootkit) nebo zadních vrátek (back door).
		12.2.1.2	Znát různé druhy nakažlivých škodlivých programů, jako jsou počítačové viry nebo červi a chápat, jak fungují.
		12.2.1.3	Rozumět tomu, jak fungují škodlivé reklamní programy (adware), programy odesílající data bez vědomí uživatele (spyware), internetové roboty (botnets), programy pro odchytávání stisků kláves (keystroke logging) nebo programy, které zašifrují data a požadují výkupné za jejich dešifrování (ransomware).
	12.2.2 Ochrana	12.2.2.1	Chápat, jak pracuje antivirový program a znát jeho omezení.
		12.2.2.2	Vědět, že antivirové programy by měly být instalovány na všech počítačích i mobilních zařízeních.
		12.2.2.3	Chápat důležitost pravidelné bezpečnostní aktualizace programů, jako jsou antivirové programy, webové prohlížeče, zásuvné moduly nebo operační systém.
		12.2.2.4	Umět pomocí antivirového programu zkontrolovat různé diskové jednotky, složky nebo soubory. Umět naplánovat provedení antivirové kontroly.
		12.2.2.5	Uvědomovat si riziko spojené s používáním zastaralých a nepodporovaných programů, jako je vyšší náchylnost k nakažení škodlivými programy nebo nižší kompatibilita s aktuálními operačními systémy.
	12.2.3 Nakládání s nakaženými nebo podezřelými soubory	12.2.3.1	Rozumět pojmu „karanténa“ a chápat smysl umístění nakažených nebo podezřelých souborů do karantény.
		12.2.3.2	Umět umístit nakažené nebo podezřelé soubory do karantény, zobrazit obsah nebo smazat obsah karantény.
		12.2.3.3	Vědět, že napadení počítače škodlivým programem může být odhaleno a vyřešeno pomocí antivirového programu, specializovaných stránek dostupných na internetu nebo stránek pro podporu operačního systému.
12.3 Bezpečnost počítačových sítí	*12.3.1 Počítačové sítě a připojení*	12.3.1.1	Rozumět termínu „počítačová síť“ a rozlišovat běžné typy počítačových sítí, jako jsou místní síť (LAN), bezdrátová místní síť (WLAN), rozlehlá sít (WAN) nebo virtuální privátní síť (VPN).
		12.3.1.2	Uvědomovat si bezpečnostní rizika spojená s připojením do počítačové sítě, jako jsou nebezpečí nakažení škodlivými programy, možný neoprávněný přístup uživatelů sítě k datům nebo ohrožení soukromí.
		12.3.1.3	Chápat hlavní úkoly správce sítě, jako jsou správa a autorizace uživatelských účtů, instalace nástrojů pro zabezpečení sítě a jejich aktualizace, monitorování síťového provozu a zasahování při zjištění škodlivých programů v síti.

KATEGORIE	OBLAST ZNALOSTÍ	ODKAZ	ROZSAH ZNALOSTI
		12.3.1.4	Rozumět funkci firewallu na osobním počítači (personal firewall) a znát jeho omezení.
		12.3.1.5	Umět zapnout a vypnout firewall na osobním počítači. Umět povolit nebo blokovat komunikaci konkrétních programů nebo služeb skrz firewall na osobním počítači.
	12.3.2 Zabezpečení bezdrátové sítě	12.3.2.1	Rozlišovat různé technologie zabezpečení bezdrátových sítí a jejich omezení, jako jsou technologie WPA (Wi-Fi Protected Access) nebo WPA2 (Wi-Fi Protected Access 2), filtrování MAC adres (MAC filtering) nebo skrývání identifikace bezdrátové sítě - SSID (Service Set Identifier).
		12.3.2.2	Vědět, že práce v nezabezpečené bezdrátové síti může vést ze strany neoprávněných osob k odposlouchávání komunikace, ukradení sítě (network hijacking) nebo vstupování do komunikace a její ovlivňování.
		12.3.2.3	Rozumět pojmu „osobní hotspot“.
		12.3.2.4	Umět zapnout nebo vypnout osobní hotspot a umět se k němu bezpečně připojit nebo se od něj odpojit.
12.4 Řízení přístupu k síti	*12.4.1 Techniky přístupu*	12.4.1.1	Znát techniky pro zamezení neoprávněného přístupu k datům, jako jsou používání uživatelského jména, hesla, PIN kódu, biometrických údajů, šifrování nebo opakované ověřování totožnosti uživatele.
		12.4.1.2	Rozumět pojmu „jednorázové heslo“ a znát typické případy jeho využití.
		12.4.1.3	Rozumět pojmu „uživatelský účet“ v počítačové síti (network account).
		12.4.1.4	Chápat, že uživatelský účet v počítačové síti by měl být zabezpečen uživatelským jménem a heslem. Chápat význam odhlášení se ze sítě.
		12.4.1.5	Znát biometrické techniky využívané při řízení přístupu k datům, jako jsou snímání otisku prstu, skenování oka, rozpoznávání obličejových rysů nebo rozpoznávání geometrie ruky uživatele.
	12.4.2 Správa hesel	12.4.2.1	Znát zásady pro tvorbu a používání hesel, jako jsou přiměřená délka hesla, vhodná struktura hesla (kombinace písmen, číslic a speciálních znaků), opakovaná obměna hesla nebo používání různě bezpečných hesel pro různé služby.
		12.4.2.2	Rozumět smyslu a omezením programů pro evidenci a správu hesel.
12.5 Bezpečné využívání webových stránek	*12.5.1 Nastavení webového prohlížeče*	12.5.1.1	Umět povolit nebo zakázat automatické dokončování a automatické ukládání dat při vyplňování formulářů.
		12.5.1.2	Umět odstranit uživatelsky citlivé informace z webového prohlížeče, jako je historie prohlížení, historie stahování, dočasné soubory (cache), použitá hesla, tzv. cookies nebo data automatického dokončování.
	12.5.2 Bezpečné prohlížení webových stránek	12.5.2.1	Uvědomovat si, že některé činnosti, například nakupování na internetu nebo využívání internetového bankovnictví, by měly být prováděny pouze na zabezpečených webových stránkách pomocí zabezpečeného připojení k síti.
		12.5.2.2	Umět rozpoznat, co zvyšuje důvěryhodnost webových stránek nebo potvrzuje jejich pravost, jako je kvalita obsahu stránek, lokální měna, očekávaná URL adresa, uvedení informací o provozovateli, uvedení kontaktních informací, zabezpečení webové stránky digitálním certifikátem.
		12.5.2.3	Rozumět pojmu „pharming“.
		12.5.2.4	Chápat smysl a znát základní typy programů pro kontrolu obsahu webových stránek, jako jsou programy pro filtrování obsahu nebo programy pro rodičovskou kontrolu.
12.6 Komunikace	*12.6.1 Elektronická pošta*	12.6.1.1	Rozumět důvodům pro šifrování zpráv elektronické pošty.
		12.6.1.2	Rozumět pojmu „digitální podpis zprávy elektronické pošty“.
		12.6.1.3	Umět rozpoznat podvodnou nebo nevyžádanou zprávu elektronické pošty.

KATEGORIE	OBLAST ZNALOSTÍ	ODKAZ	ROZSAH ZNALOSTI
		12.6.1.4	Umět rozpoznat charakteristické příznaky podvrhování falešných zpráv nebo odkazů (phishing), jako jsou používání oficiálních názvů organizací, jejich log nebo značek, používání jmen kompetentních osob, používání falešných hypertextových odkazů.
		12.6.1.5	Vědět, že zjištěné pokusy o podvržení falešné zprávy nebo odkazu na falešnou webovou stránku (phishing) je možné a vhodné nahlásit zneužitému subjektu nebo příslušným úřadům.
		12.6.1.6	Uvědomovat si možné nebezpečí nakažení počítače nebo mobilního zařízení škodlivým programem při otevření přílohy zprávy elektronické pošty, která obsahuje makro nebo spustitelný soubor.
	12.6.2 Sociální média a sociální sítě	12.6.2.1	Chápat důležitost nezveřejňování osobních údajů nebo důvěrných informací v sociálních sítích.
		12.6.2.2	Uvědomovat si potřebu využívat možnosti v nastavení uživatelského účtu na sociálních médiích, jako je možnost zveřejnění a omezení rozsahu osobních údajů nebo zveřejňování údajů o aktuální poloze.
		12.6.2.3	Znát možnosti v nastavení uživatelského účtu na sociálních médiích, jako je možnost zveřejnění a omezení rozsahu osobních údajů nebo zveřejňování údajů o aktuální poloze.
		12.6.2.4	Uvědomovat si nebezpečí hrozící v sociálních sítích, jako jsou kyberšikana, vábení (grooming), zveřejňování citlivých osobních informací, používání falešné totožnosti, podvrhování falešných URL odkazů nebo nepravdivých informací.
		12.6.2.5	Vědět, že nevhodný obsah nebo chování v sociální síti je možné nahlásit provozovateli sociálního média, správci sociální sítě nebo příslušným úřadům.
	12.6.3 Telefonování přes internet a textová komunikace v reálném čase	12.6.3.1	Uvědomovat si bezpečnostní rizika telefonování přes internet a využívání komunikace v reálném čase, jako je riziko nakažení škodlivými programy, přístup neoprávněné osoby zadními vrátky, neoprávněný přístup k souborům nebo odposlouchávání.
		12.6.3.2	Znát techniky zvyšující bezpečnost telefonování přes internet a textové komunikace v reálném čase, jako jsou šifrování hovoru, nepoužívání důležitých informací nebo osobních údajů a omezení sdílení souborů.
	12.6.4 Mobilní zařízení a aplikace	12.6.4.1	Uvědomovat si, že používání aplikací pro mobilní zařízení z neoficiálních zdrojů je spojeno s riziky, jako je možné nakažení škodlivými programy, nestabilita aplikací nebo nízká ochrana osobních údajů a dat.
		12.6.4.2	Vědět, že některé mobilní aplikace mohou vyžadovat přístup k datům uživatele nebo technickým prostředkům mobilního zařízení.
		12.6.4.3	Uvědomovat si, že mobilní aplikace mohou získávat z mobilního zařízení informace, jako jsou kontakty, události, polohové informace, fotografie nebo dokumenty.
		12.6.4.4	Znát nouzové postupy pro případ ztráty mobilního zařízení, jako jsou vzdálené vypnutí, vzdálené vymazání uživatelských dat nebo lokalizace zařízení.
12.7 Bezpečná správa dat	*12.7.1 Zálohování dat*	12.7.1.1	Znát způsoby fyzického zabezpečení počítačů a mobilních zařízení proti odcizení nebo zneužití, jako je neponechávání zařízení bez dozoru, vzdálené monitorování zařízení kamerovým systémem, používání kabelových zámků nebo zamezení přístupu neoprávněných osob.
		12.7.1.2	Uvědomovat si důležitost zálohování dat pro případ ztráty dat z počítačů nebo mobilních zařízení.
		12.7.1.3	Znát základní charakteristiky procesu zálohování jako je pravidelnost, četnost nebo plán zálohování, umístění datového úložiště nebo komprese dat.
		12.7.1.4	Umět zálohovat data na různá datová úložiště, jako je místní disk, externí disk, USB flash disk, optické médium, NAS nebo webové (cloudové) úložiště.
		12.7.1.5	Umět obnovit data ze zálohy na různých úložištích, jako je místní disk, externí disk, USB flash disk, optické médium, NAS nebo webové (cloudové) úložiště.

KATEGORIE	OBLAST ZNALOSTÍ	ODKAZ	ROZSAH ZNALOSTI
	12.7.2 Bezpečné mazání a likvidace dat	12.7.2.1	Chápat rozdíl mezi smazáním souboru a trvalým odstraněním dat z paměťového úložiště.
		12.7.2.2	Chápat důvody pro trvalé odstranění dat z datových úložišť.
		12.7.2.3	Uvědomovat si, že vymazání dat nemusí být trvalé při využívání webových (cloudových) služeb, jako jsou sociální média, webové stránky, internetová fóra nebo webová (cloudová) úložiště.
		12.7.2.4	Znát postupy a techniky pro trvalé odstranění dat jako je fyzická likvidace datových úložišť nebo použití programů pro trvalé odstranění dat.
12.8 Bezpečné využívání nástrojů a technologií umělé inteligence (AI)	*12.8.1 Deepfake technologie*	12.8.1.1	Chápat, co jsou deepfake technologie využívající umělou inteligenci a uvědomovat si, že mohou být použity k vytváření falešných obrázků a videí.
		12.8.1.2	Umět rozpoznat příznaky deepfake obrázků a videí, jako mohou být nepřesné proporce a geometrické tvary předmětů, umělá textura povrchů, nesrovnalosti v obličejových rysech osob, pohybech rtů nebo blikání očí.
		12.8.1.3	Znát základní metody a nástroje pro ověřování pravosti obrázků a videí, jako jsou online nástroje pro detekci deepfake. Umět kontrolovat zdroje a metadata obrázků a videí pro ověření jejich pravosti.
	12.8.2 Podvody se syntézou řeči při komunikaci na dálku	12.8.2.1	Vědět, že technologie umělé inteligence mohou být snadno použity k vytváření realistických syntetických hlasů, které mohou být použity k podvodům při komunikaci.
		12.8.2.2	Umět rozpoznat známky syntetických hlasů, jako jsou nesrovnalosti v intonaci, rytmu nebo přirozenosti řeči.
		12.8.2.3	Znát základní metody pro ověřování identity volajícího, jako je zpětné volání na známé číslo. Umět ověřovat osobní informace nebo používat bezpečnostní otázky pro potvrzení identity volajícího.