ICDL
The Digital Skills Standard

MODUL ICDL

CYBER SECURITY

Versiune Syllabus 2.0

Programă analitică

Obiective

Aceasta reprezintă programa pentru modulul *ICDL Cyber Security*. Ea descrie, prin rezultatele învăţării, cunoştinţele şi competenţele pe care un candidat ar trebui să le aibă. Programa prezintă, de asemenea, baza pentru testul teoretic şi proba practică a acestui modul.

Disclaimer

Chiar dacă în pregătirea acestei publicații au fost luate toate măsurile de precauție de către Fundația ICDL, aceasta nu poate oferi nicio garanție ca editor cu privire la complexitatea informațiilor conținute în ea. Fundația ICDL nu este responsabilă de eventualele erori, omisiuni, inexactități, pierderi sau distrugeri de informații și instrucțiuni conținute în această publicație. Fundația ICDL poate modifica această programă oricând, fără un aviz prealabil.

Cyber Security

Modulul Cyber Security solicită candidatului să înțeleagă principalele concepte legate de utilizarea în siguranță a tehnologiei informației în viața de zi cu zi și să utilizeze tehnologii și aplicații relevante pentru a menține o conexiune sigură, să utilizeze Internetul în condiții de siguranță și să gestioneze datele și informațiile în mod corespunzător.

Obiectivele modulului

Candidații vor fi capabili să:

- Înțeleagă conceptele cheie legate de importanța securității datelor și informațiilor și identificarea principiilor comune legate de protecția, stocarea și controlul datelor.
- Recunoască amenințările legate de securitatea datelor personale prin furtul de date, precum și potențialele pericole asociate utilizării cloud computing.
- Utilizeze parole și să cripteze date și fișiere.
- Înțeleagă amenințările cauzate de malware, să cunoască modalități de protejare a unui computer, dispozitiv sau rețea împotriva malware, precum și măsurile ce trebuie întreprinse în cazul unui atac de tip malware.
- Recunoască principalele tipuri de securitate asociate rețelelor și să cunoască modul de utilizare al unui firewall și al unui hotspot personal.
- Protejeze un computer sau un dispozitiv împotriva accesului neautorizat și să gestioneze în siguranță politicile de parolare.
- Utilizeze setările corespunzătoare ale unui browser web și să înțeleagă modul de autentificare și de navigare pe Internet în siguranță.
- Înțeleagă problemele de securitate asociate utilizării poștei electronice, rețelelor de socializare, VoIP, mesageriei instantanee și dispozitivelor mobile.
- Realizeze back up şi restaurare a datelor local sau pe locații de stocare online în mod corespunzător şi în condiţii de siguranţă, să șteargă și să distrugă datele și dispozitivele în condiții de siguranță.

CATEGORIE	SET APTITUDINI	REF.	TEMATICĂ
1 Concepte legate de securitate	*1.1 Amenințări legate de date*	1.1.1	Diferențierea termenilor date și informații.
		1.1.2	Înțelegerea termenilor cybercrime, hacking.
		1.1.3	Recunoașterea amenințărilor rău intenționate sau accidentale legate de date cauzate de: salariați, furnizorii de servicii și organizații externe.
		1.1.4	Recunoașterea amenințărilor legate de date, cauzate de forță majoră, precum: incendii, inundații, război, cutremure.
		1.1.5	Recunoașterea amenințărilor legate de date, cauzate de utilizarea cloud computing, precum: pierderea controlului datelor, încălcarea confidențialității.
	1.2 Valoarea informației	1.2.1	Înțelegerea caracteristicilor de bază legate de securitatea informațiilor: confidențialitate, integritate, disponibilitate.

CATEGORY	SKILL SET	REF.	TASK ITEM
		1.2.2	Înțelegerea motivelor de protejare a datelor personale, precum: evitarea furtului de identitate, fraudă, protejarea intimității.
		1.2.3	Înțelegerea motivelor de protejare a informațiilor comerciale, precum: prevenirea furtului, folosire frauduloasă, pierderea accidentală a datelor, sabotaj.
		1.2.4	Identificarea principiilor comune de protecție, stocare și control a datelor/ confidențialității: transparență, utilizarea datelor în scopuri legitime, proporționalitate.
		1.2.5	Înțelegerea termenilor de subiecți și operatori de date cu caracter personal și a modului de aplicare a principiilor de protecție și control a datelor pentru aceștia.
		1.2.6	Înțelegerea importanței aderării la liniile directoare și politicile de utilizare TIC.
	1.3 Securitate personală	1.3.1	Înțelegerea termenului de inginerie socială și a implicațiilor sale, precum: accesul neautorizat la computer și alte dispozitive, culegerea informațiilor neautorizate, fraudă.
		1.3.2	Identificarea metodelor ingineriei sociale, precum: apeluri telefonice, phishing, shoulder surfing.
		1.3.3	Înțelegerea termenului de furt de identitate și a implicațiilor sale: personale, financiare, comerciale, legale.
		1.3.4	Identificarea metodelor de furt de identitate, precum: information diving, skimming, pretexting.
	1.4 Securitatea fișierelor	1.4.1	Înțelegerea efectului activării/dezactivării setărilor de securitate legate de macrocomenzi.
		1.4.2	Înțelegerea avantajelor și limitărilor criptării datelor. Conștientizarea importanței nedezvăluirii sau pierderii parolei, cheii sau a certificatului de criptare.
		1.4.3	Criptarea unui fișier, director, disc (drive).
		1.4.4	Stabilirea unei parole pentru fișiere de tip documente, arhive, registre de calcul tabelar.

CATEGORY	SKILL SET	REF.	TASK ITEM
2 Malware	*2.1 Tipuri și metode*	2.1.1	Înțelegerea termenului de malware. Recunoașterea diferitelor moduri sub care malware se poate ascunde: trojan, rootkits și back doors.
		2.1.2	Recunoașterea tipurilor de malware și cunoașterea modului în care acționează: viruși, viermi.
		2.1.3	Recunoașterea tipurilor de malware legate de furtul datelor, generarea de profit/extorsiune de fonduri și înțelegerea modului lor de funcționare: adware, ransomware, spyware, botnets, keystroke logging, diallers.
	2.2 Protecție	2.2.1	Înțelegerea modului de funcționare a unei aplicații antivirus și a limitărilor sale.
		2.2.2	Înțelegerea importanței instalării unei aplicații antivirus pe computere și dispozitive.
		2.2.3	Înțelegerea importanței actualizării periodice a aplicațiilor software: anti-virus, browser web, plug-in-uri, aplicații, sistem de operare.
		2.2.4	Scanarea partițiilor, directoarelor, fișierelor cu o aplicație antivirus. Programarea scanărilor cu ajutorul unei aplicații antivirus.
		2.2.5	Înțelegerea riscurilor asociate utilizării unui software depășit, pentru care nu se mai oferă suport tehnic: riscuri crescute de virusare a computerului, incompatibilitate.
	2.3 Curățare și Eliminare	2.3.1	Înțelegerea termenului de carantină și efectului de introducere în carantină a fișierelor infectate/suspecte.
		2.3.2	Introducerea în carantină, ștergerea fișierelor infectate/suspecte.
		2.3.3	Înțelegerea faptului că un atac malware poate fi diagnosticat și rezolvat utilizând resurse online: site-uri ale sistemelor de operare, antivirus, furnizori de browsere web, site-urile web ale autorităților relevante.
3 Securitate rețele	*3.1 Rețele și conexiuni rețele*	3.1.1	Înțelegerea termenului de rețea și recunoașterea principalelor tipuri de rețele: local area network (LAN), wireless local area network (WLAN), wide area network (WAN), virtual private network (VPN).

CATEGORY	SKILL SET	REF.	TASK ITEM
		3.1.2	Înțelegerea riscurilor de securitate asociate conectării la o rețea, precum: malware, accesul neautorizat la date, nerespectarea confidențialității datelor.
		3.1.3	Înțelegerea rolului unui administrator de rețea în gestionarea autentificării și autorizării utilizatorilor, monitorizării și instalării patch-urilor and update-urilor de securitate relevante, monitorizării traficului de rețea și gestionarea malware în cadrul unei rețele.
		3.1.4	Înțelegerea funcției și limitărilor unui firewall.
		3.1.5	Pornirea, oprirea unui firewall. Permiterea, blocarea unei aplicații, serviciu/ caracteristici prin intermediul unui firewall personal.
	3.2 Securitate rețele wireless	3.2.1	Recunoașterea diferitelor tipuri de securitate wireless și a limitărilor acestora, precum: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) / Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC), Service Set Identifier (SSID).
		3.2.2	Conșientizarea faptului că utilizarea unei rețele wireless neprotejate poate permite atacuri de tipul: eavesdroppers, network hijacking, man in the middle.
		3.2.3	Înțelegerea termenului de hotspot personal.
		3.2.4	Activarea, dezactivarea unui hotspot personal securizat și conectarea, deconectarea în siguranță a dispozitivelor.
4 Controlul accesului la date	*4.1 Metode*	4.1.1	Identificarea măsurilor de prevenire a accesului neautorizat la date, precum: folosirea unui nume de utilizator, a unei parole, a unui cod PIN, criptarea, autentificarea multiplă.
		4.1.2	Înțelegerea termenului de “one-time password” și a utilizării ei.
		4.1.3	Înțelegerea scopului unui cont de utilizator în rețea.
		4.1.4	Înțelegerea faptului că un cont de utilizator în rețea ar trebui accesat prin intermediul unui nume de utilizator și a unei parole și ar trebui blocat sau delogat atunci când computerul nu este folosit.

CATEGORY	SKILL SET	REF.	TASK ITEM
		4.1.5	Identificarea tehnicilor de bază de securitate biometrică, utilizate în controlul accesului, precum: amprente, scanare oculară, recunoașterea feței, geometria mâinii.
	4.2 Politici de parolare	4.2.1	Recunoașterea regulilor de bună practică legate de politicile de parolare, precum: stabilirea unei lungimi adecvate a parolei prin combinarea literelor, cifrelor și caracterelor speciale, nedivulgarea parolelor, schimbarea lor regulată, utilizarea de parole diferite pentru servicii diferite.
		4.2.2	Înțelegerea funcțiilor și limitărilor unei aplicații de gestionare a parolelor.
5 Utilizarea în siguranță a Internetului	*5.1 Setările browser-ului web*	5.1.1	Stabilirea setărilor adecvate pentru activarea, dezactivarea opțiunilor de completare și salvare automată a datelor introduse în cadrul formularelor online.
		5.1.2	Ștergerea datelor private dintr-un browser web: istoricul de navigare, istoricul descărcărilor de fișiere, fișierele temporare de Internet, parolele, fișierele cookie, datele completate automat în cadrul formularelor online.
	5.2 Navigarea pe Internet în siguranță	5.2.1	Conștientizarea faptului că activitățile online (cumpărături, tranzacții financiare) trebuie efectuate numai pe site-uri protejate, utilizând o conexiune securizată.
		5.2.2	Identificarea modalităților de confirmare a autenticității unui site web: calitatea conținutului, actualitate, URL valid, informații legate de proprietar, informații de contact, certificat digital, validarea proprietarului domeniului.
		5.2.3	Înțelegerea termenului de pharming.
		5.2.4	Înțelegerea funcției și tipurilor de aplicații software pentru controlul conținutului: aplicații de filtrare a paginilor web, aplicații de control parental.
6 Comunicații	*6.1 E-Mail*	6.1.1	Înțelegerea scopului criptării și decriptării unui e-mail.
		6.1.2	Înțelegerea termenului de semnătură digitală.
		6.1.3	Identificarea mesajelor nesolicitate, potențial frauduloase.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.1.4	Identificarea caracteristicilor specifice phishing-ului, precum: utilizarea numelor unor persoane sau companii legitime, linkuri, logo-uri și brand-uri false, încurajarea dezvăluirii informațiilor confidentiale.
		6.1.5	Conștientizarea posibilității de raportare a atacurilor de tip phishing la organizațiile abilitate sau autoritățile relevante.
		6.1.6	Conștientizarea pericolului de infectare a computerului cu viruși la deschiderea unui fișier atașat unui email, ce conține o macrocomandă sau un fișier executabil.
	6.2 Rețele sociale	6.2.1	Înțelegerea importanței nedezvăluirii informațiilor confidențiale în cadrul rețelelor de socializare.
		6.2.2	Conștientizarea necesității aplicării și revizuirii regulate a setărilor de securitate corespunzătoare conturilor existente pe rețelele sociale: confidențialitate cont, locație.
		6.2.3	Aplicarea setărilor de securitate corespunzătoare conturilor existente pe rețelele sociale: confidențialitate cont, locație.
		6.2.4	Înțelegerea pericolelor potențiale asociate utilizării site-urilor de rețele sociale, precum: cyber bullying, grooming, dezvăluirea malițioasă a informațiilor confidențiale, identități false, linkuri, conținut și mesaje frauduloase sau malițioase.
		6.2.5	Conștientizarea posibilității de raportare a comportamentelor inadecvate din cadrul rețelelor de socializare la furnizorul serviciului sau autoritățile relevante.
	6.3 VoIP și mesagerie instantanee	6.3.1	Înțelegerea vulnerabilității securității mesageriei instantanee și a VoIP, precum: malware, acces la fișiere, backdoor access, eavesdropping.
		6.3.2	Recunoașterea metodelor de asigurare a confidențialității în utilizarea IM și VoIP: criptarea, nedezvăluirea informațiilor importante, restricționarea partajării fișierelor.
	6.4 Tehnologii mobile	6.4.1	Înțelegerea implicațiilor posibile ale utilizării aplicațiilor descărcate din magazine de aplicații neautorizate: malware, utilizarea inutilă a resurselor, accesarea datelor personale, calitate slabă, costuri ascunse.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.4.2	Înțelegerea termenului de permisiuni ale aplicației.
		6.4.3	Conștientizarea faptului că aplicațiile mobile pot extrage informații private de pe dispozitive mobile, precum: detalii de contact, istoricul locațiilor vizitate, imagini.
		6.4.4	Conștientizarea măsurilor de urgență și precauție ce se impun la pierderea unui dispozitiv: dezactivare de la distanță, ștergerea datelor de la distanță, localizare dispozitiv.
7 Managementul datelor în condiții de siguranță	*7.1 Realizarea de back up a datelor în condiții de siguranță*	7.1.1	Recunoașterea modurilor de asigurare a securității fizice a computerelor și dispozitivelor, precum: nelăsarea dispozitivului nesupravegheat, înregistrarea locației și detaliilor echipamentelor, utilizarea de încuietori pentru cabluri, controlul accesului.
		7.1.2	Recunoașterea importanței existenței unei proceduri de back-up în cazul pierderii datelor de pe computere sau dispozitive.
		7.1.3	Identificarea caracteristicilor unei proceduri de backup, precum: regulat/frecvent, programat, locație stocare, arhivare date.
		7.1.4	Realizare back up date într-o locație precum: disc local, disc/media extern, servicii de stocare online.
		7.1.5	Recuperare date de pe disc local, disc/media extern, cloud.
	7.2 Distrugerea în siguranță a datelor si dispozitivelor	7.2.1	Diferența dintre ștergerea și distrugerea definitivă a datelor.
		7.2.2	Înțelegerea motivului ștergerii definitive a datelor de pe discuri (drives) și dispozitive.
		7.2.3	Conștientizarea faptului că ștergerea datelor poate să nu fie permanentă în cazul rețelelor sociale, blogurilor, forumurilor de discuții pe Internet, serviciilor de stocare online.
		7.2.4	Identificarea metodelor de bază de distrugere permanentă a datelor, precum: mărunțirea, distrugerea dispozitivelor, demagnetizarea, utilizarea programelor utilitare de distrugere a datelor.