ECDL Foundation

IT Security

Syllabus Versiune 1.0

Obiective

Aceasta reprezintă programa pentru modulul ECDL *IT 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 ECDL, aceasta nu poate oferi nicio garanție ca editor cu privire la complexitatea informațiilor conținute în ea. Fundația ECDL nu este responsabilă de eventualele erori, omisiuni, inexactități, pierderi sau distrugeri de informații și instrucțiuni conținute în această publicație. Fundația ECDL poate modifica această programă oricând, fără un aviz prealabil.

Versiunea oficială a Programei Analitice ECDL pentru **Modulul IT Security** este publicată în secțiunea **Download** a website-ului **www.ecdl.ro**

ECDL Foundation

IT Security

Modulul IT 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

Candidatul va trebui să știe să:

- Înțeleagă conceptele cheie legate de importanța securității datelor și informațiilor, a securității fizice și a furtului de date.
- Protejeze un computer, dispozitiv sau rețea împotriva virușilor și accesului neautorizat.
- Înțeleagă principalele tipuri de rețele, conexiuni și probleme asociate rețelelor, inclusiv firewall-uri.
- Navigheze și să comunice pe Internet în siguranță.
- Înțeleagă problemele de securitate asociate comunicațiilor, inclusiv email și mesagerie instantanee.
- Realizeze back up şi restaurare a datelor în mod corespunzător şi în condiţii de siguranţă și să păstreze 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 termenului cybercrime.
		1.1.3	Înțelegerea diferenței dintre hacking, cracking și ethical hacking.
		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: salariați, furnizorii de servicii și persoane fizice externe.
	1.2 Valoarea informației	1.2.1	Înțelegerea motivelor de protejare a datelor personale, precum: evitarea furtului de identitate, fraudă.

CATEGORIE	SET APTITUDINI	REF.	TEMATICĂ
		1.2.2	Înțelegerea motivelor de protejare a informațiilor comerciale, precum: prevenirea furtului sau abuzului datelor clienților și a informațiilor financiare
		1.2.3	Identificarea măsurilor de prevenire a accesului neautorizat la date, precum: criptare, parolare.
		1.2.4	Înțelegerea caracteristicilor de bază legate de securitatea informațiilor: confidențialitate, integritate, disponibilitate.
		1.2.5	Identificarea principalelor cerințe legate de protecția datelor/identității în țara dvs
		1.2.6	Înțelegerea importanței creării și 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: culegerea informațiilor, fraudă, accesul la calculator.
		1.3.2	Identificarea metodelor ingineriei sociale, precum: telefoane, phishing, shoulder surfing.
		1.3.3	Înțelegerea termenului de furt de identitate și a implicațiilor sale: personale, financiare, de afaceri, 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 macro.
		1.4.2	Stabilirea unei parole pentru fișiere de tip documente, arhive, registre de calcul tabelar.
		1.4.3	Înțelegerea avantajelor și limitărilor criptării datelor

CATEGORIE	SET APTITUDINI	REF.	TEMATICĂ
2 Malware	*2.1 Definire și funcții*	2.1.1	Înțelegerea termenului de malware.
		2.1.2	Recunoașterea diferitelor moduri sub care malware se poate ascunde: trojan, rootkits și back doors.
	2.2 Tipuri	2.2.1	Recunoașterea tipurilor de malware și cunoașterea modului în care acționează: viruși, viermi.
		2.2.2	Recunoașterea virușilor legați de furtul datelor, generarea de profit/extorsiune de fonduri și înțelegerea modului lor de funcționare: adware, spyware, botnets, keystroke logging, diallers.
	2.3 Protecție	2.3.1	Înțelegerea modului de funcționare a unei aplicații antivirus și a limitărilor sale.
		2.3.2	Scanarea partițiilor, directoarelor, fișierelor cu o aplicație antivirus. Programarea scanărilor cu ajutorul unei aplicații antivirus.
		2.3.3	Înțelegerea termenului de carantină și efectului de introducere în carantină a fișierelor infectate/suspecte.
		2.3.4	Înțelegerea importanței actualizării periodice a aplicației antivirus
3 Securitate rețele	*3.1 Rețele*	3.1.1	Înțelegerea termenului de rețea și recunoașterea principalelor tipuri de rețele: local area network (LAN), wide area network (WAN), virtual private network (VPN).
		3.1.2	Înțelegerea rolului unui administrator de rețea în gestionarea autentificării și autorizării în cadrul unei rețele.
		3.1.3	Înțelegerea funcției și limitărilor unui firewall.

CATEGORIE	SET APTITUDINI	REF.	TEMATICĂ
	3.2 Conexiune rețele	3.2.1	Recunoașterea modurilor de conectare la o rețea: cablu, wireless.
		3.2.2	Înțelegerea faptului că, conectarea la o rețea implică anumite riscuri de securitate, precum:: viruși, accesul neautorizat la date, nerespectarea confidențialității.
	3.3 Securitate rețele wireless	3.3.1	Recunoașterea importanței solicitării unei parole pentru protejarea accesului la o rețea wireless.
		3.3.2	Recunoașterea diferitelor tipuri de securitate wireless, precum: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).
		3.3.3	Conșientizarea faptului că utilizarea unei rețele wireless neprotejate poate permite accesul persoanelor neautorizate la date.
		3.3.4	Conectarea la o rețea wireless protejată/neprotejată.
	3.4 Controlul accesului la date	3.4.1	Înțelegerea scopului unui cont de utilizator în cadrul unei rețele și accesarea lui cu ajutorul unui nume de utilizator și a unei parole.
		3.4.2	Recunoașterea regulilor legate de politicile de parolare: nedivulgarea parolelor, schimbarea lor regulată, stabilirea unei lungimi adecvate a parolei prin combinarea literelor, cifrelor și caracterelor speciale.
		3.4.3	Identificarea tehnicilor de bază de securitate biometrică, utilizate în controlul accesului, precum: amprente, scanare oculară.

CATEGORIE	SET APTITUDINI	REF.	TEMATICĂ
4 Utilizarea în siguranță a Internetului	*4.1 Navigarea pe Internet*	4.1.1	Conștientizarea faptului că activitățile online (cumpărături, tranzacții financiare) trebuie efectuate numai pe site-uri protejate.
		4.1.2	Identificarea unui site protejat: https, simbolul unui lacăt.
		4.1.3	Conștientizarea termenului de pharming.
		4.1.4	Înțelegerea termenului de certificat digital. Validarea unui certificat digital.
		4.1.5	Înțelegerea termenului de “one-time password”.
		4.1.6	Stabilirea setărilor corespunzătoare pentru activarea, dezactivarea opțiunilor de completare și salvare automată în cadrul unui formular.
		4.1.7	Înțelegerea termenului cookie.
		4.1.8	Stabilirea setărilor corespunzătoare pentru permiterea sau blocarea elementelor cookie.
		4.1.9	Ștergerea datelor private dintr-un browser web, precum: istoric pagini vizitate, fișiere cache, parole, cookie, date autocompletate.
		4.1.10	Înțelegerea scopului, funcției și tipurilor de aplicații software pentru controlul conținutului: aplicații de filtrare a paginilor web, aplicații de control parental.
	4.2 Rețele sociale	4.2.1	Înțelegerea importanței nedezvăluirii informațiilor confidențiale în cadrul site-urilor de rețele sociale.
		4.2.2	Conștientizarea necesității aplicării setărilor de securitate corespunzătoare conturilor existente pe rețelele sociale.

CATEGORIE	SET APTITUDINI	REF.	TEMATICĂ
		4.2.3	Înțelegerea pericolelor potențiale asociate utilizării site-urilor de rețele sociale: cyber bullying, grooming, informații înșelătoare/periculoase, identități false, linkuri și mesaje frauduloase.
5 Comunicații	*5.1 E-Mail*	5.1.1	Înțelegerea scopului criptării și decriptării unui email.
		5.1.2	Înțelegerea termenului de semnătură digitală..
		5.1.3	Crearea și adăugarea unei semnături digitale.
		5.1.4	Conștientizarea posibilității de a primi mesaje frauduloase și nesolicitate.
		5.1.5	Înțelegerea termenului phishing. Identificarea caracteristicilor specifice phishing-ului: utilizarea numelor unor persoane sau companii legitime, linkuri web false.
		5.1.6	Conștientizarea pericolului de infectare a computerului cu viruși la deschiderea unui fișier atașat unui email, ce conține un macro sau un fișier executabil.
	5.2 Mesagerie instantanee	5.2.1	Înțelegerea termenului de mesagerie instantanee (IM) și a principalelor utilizări.
		5.2.2	Înțelegerea vulnerabilității securității mesageriei instantanee: viruși, acces la fișiere, backdoor access.
		5.2.3	Recunoașterea metodelor de asigurare a confidențialității în utilizarea IM: criptare, nedezvăluirea informațiilor importante, restricționarea partajării fișierelor.

CATEGORIE	SET APTITUDINI	REF.	TEMATICĂ
6 Managementul datelor în condiții de siguranță	*6.1 Realizarea de back up a datelor în condiții de siguranță*	6.1.1	Recunoașterea modurilor de asigurare a securității fizice a dispozitivelor, precum: înregistrarea locației și detaliilor echipamentelor, utilizarea de încuietori pentru cabluri, controlul accesului.
		6.1.2	Recunoașterea importanței existenței un proceduri de back-up în cazul pierderii datelor, înregistrărilor financiare, semnelor de carte web sau istoricului paginilor web vizitate..
		6.1.3	Identificarea proprietăților unei proceduri de backup, precum: regulat/frecvent, programat, locație stocare.
		6.1.4	Realizare back up date.
		6.1.5	Recuperare și validare a datelor.
	6.2 Distrugerea în siguranță a datelor și dispozitivelor	6.2.1	Înțelegerea motivului ștergerii definitive a datelor de pe partiții și dispozitive.
		6.2.2	Diferența dintre ștergerea și distrugerea definitivă a datelor.
		6.2.3	Identificarea metodelor de bază de distrugere permanentă a datelor: mărunțirea, distrugerea dispozitivelor, demagnetizarea.