ECDL / ICDL IT Security
Syllabus Version 1.0

Qëllimi

Ky dokument detajon planin mësimor për ECDL / ICDL Bazat e Kompjuterit. Syllabusi përshkruan, nëpërmjet rezultateve të mësimit , njohuritë dhe aftësitë që një kandidat duhet të posedojë për ECDL / ICDL Bazat e Kompjuterit. Syllabusi gjithashtu ofron bazën e provimit teorik dhe praktik për këtë modul.

Përjashtimi i përgjegjësisë

Edhe pse Fondacioni ECDL ka punuar me shumë kujdes në përgatitjen e këtij botimi, nuk jep asnjë lloj garancioni si botues, në lidhje me tërësinë e informatave të cilat i përmban ky botim, si dhe ECDL Foundation nuk është përgjegjës dhe nuk e mban përgjegjësinë për ndonjë gabim, lëshim, pasaktësi, humbje ose dëmtim të çfarëdollojshëm që mund të jetë si pasojë e informacioneve, udhëzimeve apo këshillave që përmban ky publikim. Ndryshimet mund të bëhen nga ECDL Foundation në diskrecionin e vet dhe në çdo kohë pa paralajmërim.

ECDL / ICDL IT Security

Ky modul përcakton konceptet themelore në lidhje me aftësinë për të kuptuar nocionet kryesore që kanë të bëjnë me aplikimin e sigurt të TIK-ut në jetën e përditshme, përdorimin e teknikave dhe aplikacioneve të përshtatshme për të mbajtur një lidhje të sigurt të rrjetit, përdorimin e internetit në mënyrë të sigurt, dhe për të menaxhuar të dhënat dhe informacionet në mënyrën e duhur.

Qëllimi i modulit

Kandidatët e suksesshëm do të jenë në gjendje të:

- Kuptojnë konceptet kyçe që lidhen me rëndësinë e informacionit të sigurt dhe të dhënave, të sigurisë fizike , intimitetit dhe vjedhjet e identitetit .
- Mbroj një kompjuter, pajisje ose rrjet nga malwer-et dhe qasjet e paautorizuara.
- Kuptoj llojet e rrjeteve, llojet e kyçjes dhe çështjet specifike të rrjetit duke përfshirë firewalls .
- Shfletoj World Wide Web dhe të komunikoj sigurt në internet.
- Kuptoj çështjet e sigurisë që lidhen me komunikimin, duke përfshirë e-mail dhe SMS .
- Bëj ruajtjen dhe rivendosjen e të dhënave në mënyrë të drejtë dhe të sigurt, si dhe fshirjen /shkatërrimin e sigurt të të dhënave dhe të pajisjeve.

Kategoria		*Lëmi i njohurive*		*Ref.*	*Objektivat*
1	**Konceptet e sigurisë**	1.1	Kërcënimi i të dhënave	1.1.1	Dallimi në mes të dhënave dhe informacionit.
				1.1.2	Kuptojnë termin krimi kibernetik.
				1.1.3	Kuptojnë dallimin në mes të piraterisë, cracking dhe ethical hacking
				1.1.4	Njohin kërcënimet e të dhënave nga forcat madhore si: zjarri, tërmeti, vërshimet, lufta
				1.1.5	Njohin kërcënimet e të dhënave nga: të punësuarit, ofruesit e shërbimeve dhe individët e jashtëm.
		1.2	Vlera e Informacionit	1.2.1	Kuptojnë arsyet për mbrojtjen e informacionit personal si : mbrojtja nga vjedhjet e identitetit, mashtrimi
				1.2.2	Kuptojnë arsyet për mbrojtjen e informacionit të ndjeshëm komercial si: parandalimin e vjedhjes ose keqpërdorimit të të dhënave të klientit informacionit financiar

Kategoria	*Lëmi i njohurive*		*Ref.*	*Objektivat*
			1.2.3	Identifikimi i masave për parandalimin e qasjes së paautorizuar në të dhënat si: shifrimi , passwords.
			1.2.4	Kuptojnë karakteristikat themelore të sigurisë së informacionit të tilla si: konfidencialiteti , integriteti, disponibiliteti. Identifikimi i të dhënave kryesore/ mbrojtjen e privatësisë, ruajtjen dhe mbajtjen nën kontroll të kërkesave në vendin tuaj.
			1.2.6	Kuptojnë rëndësinë e krijimit dhe respektimit të udhëzimeve dhe politikave për përdorimin e TIKut.
		1.3 Siguria Personale	1.3.1	Kuptojnë termin social engineering dhe implikimet saj si: mbledhjen e informacionit , mashtrimi , qasja në sistemin kompjuterik
			1.3.2	Identifikoni metodat e social engineering si: thirrje telefonike , phishing , shoulder surfing.
			1.3.3	Kuptojnë termin vjedhje e identitetit dhe implikimet e saj : personale , financiare, biznesore, ligjore.
			1.3.4	Identifikoni metodat e vjedhjes së identitetit si: marrja e informacionit, skimming , pretexting.
		1.4 Siguria e dokumentit	1.4.1	Kuptojnë efektin e aktivizimit / deaktivizimit të parametrave makro të sigurisë.
			1.4.2	Vendosni një fjalëkalim për fajllat si: dokumente, fajllat e ngjeshur, fletët punuese.
			1.4.3	Kuptojnë avantazhet dhe kufizimet e shifrimit.
2	Malware	2.1 Përkufizimi dhe Funksioni	2.1.1	Kuptojnë termin malware.
			2.1.2	Njohin mënyra të ndryshme që malware mund të fshihet si : trojanet, rootkits.
		2.2 Llojet	2.2.1	Njohin llojet e malwar-ve infektues dhe të kuptojnë se si ata punojnë si : viruset , worms.
			2.2.2	Njohin llojet e vjedhjes së të dhënave, fitimi gjeneruese / grabitje malware dhe të kuptojnë se si ata punojnë si: adware, spyware, botnets,

Kategoria		*Lëmi i njohurive*		*Ref.*	*Objektivat*
					prerjet keystroke dhe dialers.
		2.3	Mbrojtja	2.3.1	Kuptojnë se si punon softueri anti -virus dhe kufizimet e tij.
				2.3.2	Skanimi i fajllave specifik, dosjeve duke përdorur softuer anti - virus. Organizimi i skanimeve duke përdorur softuer anti – virus
				2.3.3	Kuptojnë termin karantinë afatgjatë dhe efektin e fajllit të infektuar, të dyshimtë.
				2.3.4	Kuptojnë rëndësinë e përditësimeve të softuerëve –virus.
3	Siguria e Rrjeteve	3.1	Rrjetet	3.1.1	Kuptojnë termin rrjet dhe njohin llojet e zakonshme të rrjetit si: Local Area Network (LAN) Wide Area Network (WAN), rrjet virtual privat (VPN).
				3.1.2	Kuptojnë rolin e administratorit te rrjetit ne menaxhimin, autorizimin, vërtetimin dhe mbajtjen e llogarisë brenda një rrjeti.
				3.1.3	Kuptojnë funksionin dhe kufizimet e një firewall.
		3.2	Kyçjet ne rrjete	3.2.1	Njohim mundësitë për lidhjen në një rrjet si : kabllor, tel.
				3.2.2	Kuptojnë se lidhja në një rrjet ka implikime për sigurinë si : malware , qasjes të paautorizuar të të dhënave, ruajta e privatësisë
		3.3	Siguria e Wireless-it	3.3.1	Njohin rëndësinë qe ka fjalëkalimi për të mbrojtur qasjen ne rrjet.
				3.3.2	Njohin llojet e ndryshme të sigurisë se rrjetit si: Wired Equivalent Privacy (WEP) , Wi -Fi Protected Access (WPA) , Media Access Control MAC)
				3.3.3	Të jenë të vetëdijshëm se duke përdorur një rrjet të pambrojtur mund të lejojnë seavesdroppers wireless për të hyrë në të dhënat tuaja.
				3.3.4	Lidheni në një rrjet të mbrojtur / të pambrojtur.
		3.4	Kontrolli ne qasje	3.4.1	Kuptojnë qëllimin e një llogarie në rrjet dhe si duhet ti qasen nëpërmjet një përdoruesi dhe fjalëkalimi.

Kategoria	*Lëmi i njohurive*		*Ref.*	*Objektivat*
			3.4.2	Njohim rregullat për një fjalëkalim si: përdorimi i përbashkët i fjalëkalimeve, ndryshimin e tyre rregullisht, gjatësinë adekuate të fjalëkalimeve, shkronjat adekuate, përzgjedhja e numrave dhe karaktereve speciale.
			3.4.3	Identifikimi i teknikave të përbashkëta biometrike të sigurisë gjatë kontrollit të qasjes si: gjurmët e gishtave, skanimi i syve.
4	4.1	Kërkimi ne ueb	4.1.1	Vetëdijesimi se veprimtaria e sigurt online (blerjet,transaksionet financiare) duhet të bëhen vetëm në faqet e sigurta të internetit.
			4.1.2	Identifikimi një faqe interneti të sigurt si: https , simbol lock.
			4.1.3	Te jeni te vetëdijshëm për pharming**.**
			4.1.4	Kuptojnë termin certifikatë digjitale. Vlefshmëria e certifikatës digjitale.
			4.1.5	Kuptojnë termin fjalëkalim one-time.
			4.1.6	Zgjidh parametrat e duhura për të mundësuar , pamundësuar veprimin autocomplete, autosave për kompletimin e një forme.
			4.1.7	Kuptojnë termin cookie.
			4.1.8	Zgjidh parametrat e duhura për të lejuar, bllokuar cookie.
			4.1.9	Fshij të dhënat private nga një shfletues si : Historia e shfletimit, fajllat e pranuar nga interneti, fjalëkalime,cookies.
			4.1.10	Kuptojnë qëllimin, funksionin dhe llojet e përmbajtjes softuer i kontrolluar si: softueri i filtrimit të internetit, softueri i kontrollit prindëror.
	4.2	Rrjetet Sociale	4.2.1	Kuptojnë rëndësinë e mos zbulimit te informacionit konfidencial në faqet e rrjeteve sociale.
			4.2.2	Vetëdijesimi për nevojën e aplikimit të parametrave të duhur të privatësisë në rrjetet sociale.

Kategoria		*Lëmi i njohurive*		*Ref.*	*Objektivat*
				4.2.3	Kuptoni rreziqet e mundshme gjatë hapjes së faqeve të rrjeteve sociale si cyber bullying, lidhjeve mashtruese,informacionet e rrezikshme, identitetet e rrejshme, lidhjet dhe mesazhet mashtruese.
5	Komunikimet	5.1	E-mail	5.1.1	Kuptojnë qëllimin e shifrimit, deshifrimit për një e-mail.
				5.1.2	Kuptojnë termin nënshkrimi digjital.
				5.1.3	Të krijoni dhe të shtoni një nënshkrim digjital.
				5.1.4	Te jenë të vetëdijshëm për mundësinë e pranimit te email-ave mashtrues.
				5.1.5	Kuptojnë termin phishing. Identifikimi i karakteristikave të përbashkëta të phishing si : duke përdorur emrat e kompanive të ligjshme, njerëzve, linqet false te ueb-i.
				5.1.6	Të jenë të vetëdijshëm për rrezikun e infektimit të kompjuterit me malware gjatë hapjes së një fajlli të bashkangjitur në email, që përmban një makro
		5.2	Mesazh i menjëhershëm (IM)	5.2.1	Kuptojnë termin Instant Messaging (IM) dhe përdorimin e tij
				5.2.2	Kuptojnë dobësitë e sigurisë të IM-se si: malware qasja back door, qasja në fajlla.
				5.2.3	Njohja e metodave që sigurojnë konfidencialitetin gjatë përdorimit të IM si: shifrimi, ruajtja e informatave të rëndësishme , kufizimin e qasjes në fajlla.
6	Menaxhimi i sigurt i të dhënave	6.1	Sigurimi dhe backup-i i të dhënave	6.1.1	Njohja e metodave për sigurinë fizike të pajisjeve si: Log equipment Location, përdorimi i cable locks, qasja e kontrolluar.
				6.1.2	Njohin rëndësinë e procedurës së backup-it në rast të humbjes së të dhënave, raporteve financiare , shfletimit të historisë.
				6.1.3	Identifikimi i veçorive të një procedure të back-up si: rregullsia / frekuenca, orari, vendi i ruajtjes.

Kategoria	*Lëmi i njohurive*		*Ref.*	*Objektivat*
			6.1.4	Backup-i i të dhënave.
			6.1.5	Kthimi dhe vlefshmëria e të dhënave nga backupi
	6.2	Shkatërrimi i Sigurt	6.2.1	Të kuptojnë arsyen e fshirjes se përhershme të të dhënave nga disqet apo pajisjet.
			6.2.2	Dallimin në mes te fshirjes së përhershme nga shkatërrimi i të dhënave.
			6.2.3	Identifikoni metodat e zakonshme të shkatërrimit të të dhënave: grisja, shkatërrimi i drajverave, përdorimi i shërbimeve për shkatërrimin e të dhënave.