ECDL Informacijska varnost

Učni načrt 1.0

Namen

Ta dokument opredeljuje učni načrt za ECDL Informacijska varnost. Učni načrt opisuje znanja in spretnosti, ki jih kot rezultat učenja mora imeti kandidat za izpit ECDL Informacijska varnost. Učni načrt zagotavlja tudi temelj za teoretične in praktične naloge izpita tega modula.

Omejitev odgovornosti

Čeprav sta ECDL Foundation in SDI pripravila to gradivo z vso skrbnostjo, ECDL Foundation in SDI kot izdajatelja ne dajeta nobenega zagotovila, da so vsebovane informacije celovite. Prav tako ECDL Foundation in SDI ne prevzemata odgovornosti za kakršnekoli napake, pomanjkljivosti, netočnosti ter izgubo in škodo nastalo zaradi informacij, navodil in nasvetov, ki jih vsebuje to gradivo. ECDL Foundation in SDI si pridržujeta pravico, da kadarkoli spremenita vsebino gradiva, na kakršenkoli način, ne glede na razlog in brez predhodnega opozorila.

ECDL Informacijska varnost

Ta modul določa osnovne koncepte in veščine v povezavi s sposobnostjo razumevanja osnovnih pojmov, ki pomenijo podlago za varno uporabo informacijsko komunikacijske tehnologije v vsakodnevnem življenju, ter uporabo ustreznih tehnik in programov za ohranjanje varne omrežne povezave, varne in zaščitene uporabe interneta ter za primerno upravljanje podatkov in informacij.

Cilji modula

Uspešni kandidati bodo:

- poznali ključne pojme v povezavi s pomembnostjo zaščite informacij in podatkov, fizično zaščito, zasebnostjo in krajo identitete.
- zaščitili računalnik, napravo ali omrežje pred zlonamernim programjem in nepooblaščenim dostopom.
- poznali vrste omrežij, načine povezave in omrežno problematiko, vključno s požarnimi zidovi.
- varno brskali po svetovnem spletu in komunicirali preko interneta.
- poznali varnostna vprašanja povezana s komuniciranjem, vključno z elektronsko pošto in takojšnjim sporočanjem.
- ustrezno in varno varnostno kopirali in obnovili podatke ter varno odstranili podatke in naprave.

KATEGORIJA	PODROČJE	OZNAKA	POTREBNA ZNANJA
1 Varnost	*1.1 Podatkovne grožnje*	1.1.1	Razlikovati med podatkom in informacijo.
		1.1.2	Razumeti pojem kibernetski kriminal.
		1.1.3	Razumeti razliko med hekanjem, skrekanjem in etičnim hekanjem.
		1.1.4	Poznati grožnje podatkom zaradi višje sile, kot so ogenj, poplave, vojna in potres.
		1.1.5	Poznati grožnje podatkom s strani: zaposlenih, ponudnikov storitev in tretjih oseb.
	1.2 Vrednost informacij	1.2.1	Poznati razloge za zaščito osebnih informacij, kot sta preprečevanje kraje identitete in prevara.

KATEGORIJA	PODROČJE	OZNAKA	POTREBNA ZNANJA
		1.2.2	Poznati razloge za zaščito poslovno občutljivih informacij, kot so preprečevanje kraje ali nedovoljene uporabe podatkov o strankah in finančnih informacij.
		1.2.3	Prepoznati ukrepe za preprečevanje nepooblaščenega dostopa do podatkov, kot sta šifriranje in gesla.
		1.2.4	Razumeti osnovne lastnosti informacijske varnosti, kot so zaupnost, popolnost in razpoložljivost.
		1.2.5	Prepoznati glavne zahteve glede zaščite podatkov in zasebnosti, hrambe podatkov ter nadzora nad tem v svoji državi.
		1.2.6	Razumeti pomembnost izdelave in upoštevanja smernic in politik za uporabo informacijske tehnologije.
	1.3 Osebna varnost	1.3.1	Razumeti pojem socialni inženiring in njegove posledice, kot so zbiranje informacij, prevare in dostop do računalniških sistemov.
		1.3.2	Prepoznati metode socialnega inženiringa, kot so telefonski klici, zvabljanje in vohunjenje čez ramo.
		1.3.3	Razumeti pojem kraja identitete in njene posledice: osebne, finančne, poslovne, pravne.
		1.3.4	Prepoznati metode kraje identitete, kot so obnavljanje zbrisanih podatkov, posnemanje podatkov in zavajanje.
	1.4 Zaščita datotek	1.4.1	Razumeti posledice omogočanja/onemogočanja varnostnih nastavitev makrov.

KATEGORIJA	PODROČJE	OZNAKA	POTREBNA ZNANJA
		1.4.2	Nastaviti geslo datotekam, kot so dokumenti, stisnjene datoteke in preglednice.
		1.4.3	Razumeti prednosti in omejitve šifriranja.
2 Zlonamerno programje	*2.1 Opredelitev in delovanje*	2.1.1	Razumeti pojem zlonamerno programje.
		2.1.2	Poznati različne načine kako je zlonamerno programje lahko skrito, kot so trojanci, korenski kompleti in stranska vrata.
	2.2 Vrste	2.2.1	Poznati vrste prenosljivega zlonamernega programja in razumeti kako delujejo npr. virusi, črvi.
		2.2.2	Poznati vrste zlonamernega programja za krajo podatkov, za krajo denarja, za izsiljevanje ter razumeti kako deluje npr. oglaševalsko in vohunsko programje, omrežje robotskih računalnikov, beleženje tipkanja, samodejni izbirniki.
	2.3 Zaščita	2.3.1	Razumeti kako deluje protivirusni program in kakšne omejitve ima.
		2.3.2	Pregledati določene pogone, mape, datoteke z uporabo protivirusnega programa. Načrtovati preglede z protivirusnim programom.
		2.3.3	Razumeti pojem karantena in posledice postavitve okuženih ter sumljivih datotek v karanteno.
		2.3.4	Razumeti pomembnost prenašanja in nameščanja programskih posodobitev, zbirke protivirusnih definicij.

KATEGORIJA	PODROČJE	OZNAKA	POTREBNA ZNANJA
3 Omrežna varnost	*3.1 Omrežja*	3.1.1	Razumeti pojem omrežje in poznati običajne tipe omrežja, kot so lokalno omrežje (LAN), prostrano omrežje (WAN) in navidezno zasebno omrežje (VPN).
		3.1.2	Razumeti vlogo omrežnega skrbnika pri upravljanju računov, istovetnosti in avtorizaciji znotraj omrežja.
		3.1.3	Razumeti delovanje in omejitve požarnega zidu.
	3.2 Omrežne povezave	3.2.1	Poznati možnosti za povezavo na omrežje, kot sta kabelska in brezžična.
		3.2.2	Razumeti kako povezovanje na omrežje vpliva na varnost, npr. zlonamerno programje, nepooblaščen dostop do podatkov, vzdrževanje zasebnosti.
	3.3 Brezžična varnost	3.3.1	Poznati pomembnost zahteve za geslo pri zaščiti dostopa do brezžičnega omrežja.
		3.3.2	Poznati različne vrste brezžične zaščite, kot so zasebnost kot v žičnem omrežju (WEP), zaščiteni brezžični dostop (WPA) in krmiljenje dostopa do medija (MAC).
		3.3.3	Zavedati se, da uporaba nezaščitenega brezžičnega omrežja lahko povzroči dostop do naših podatkov preko brezžičnega prisluškovanja.
		3.3.4	Povezati se na zaščiteno ali nezaščiteno brezžično omrežje.
	3.4 Nadzor dostopa	3.4.1	Razumeti namen omrežnega računa ter da se mora do njega dostopati preko uporabniškega imena in gesla.

KATEGORIJA	PODROČJE	OZNAKA	POTREBNA ZNANJA
		3.4.2	Poznati dobro politiko varovanja gesel: ne deli gesel, redno jih menjaj, ustrezna dolžina gesla, ustrezna mešanica črk, številk in posebnih znakov.
		3.4.3	Prepoznati običajne biometrične varnostne tehnike uporabljene pri nadzoru dostopa, kot sta prstni odtis in skeniranje očesa.
4 Varna uporaba spleta	*4.1 Spletno brskanje*	4.1.1	Zavedati se, da določene spletne aktivnosti (nakupovanje, finančne transakcije) lahko opravljamo le na varnih spletnih straneh.
		4.1.2	Prepoznati varno spletno stran: https, simbol ključavnice.
		4.1.3	Zavedati se farminga.
		4.1.4	Razumeti pojem digitalno potrdilo. Preveriti veljavnost digitalnega potrdila.
		4.1.5	Razumeti pojem enkratnega gesla.
		4.1.6	Izbrati ustrezne nastavitve za vključitev, izključitev samodejnega zapolnjevanja, samodejnega shranjevanja pri izpolnjevanju obrazca.
		4.1.7	Razumeti pojem piškotek.
		4.1.8	Izbrati ustrezne nastavitve za omogočanje, blokiranje piškotkov.
		4.1.9	Izbrisati osebne podatke iz brskalnika, kot so zgodovina brskanja, začasne internetne datoteke, gesla, piškotki in podatki obrazcev.
		4.1.10	Razumeti namen, delovanje in vrste programov za nadzor vsebine, kot so programi za filtriranje spletnih strani in programi za starševski nadzor.

KATEGORIJA	PODROČJE	OZNAKA	POTREBNA ZNANJA
	4.2 Socialna omrežja	4.2.1	Razumeti pomembnost varovanja zaupnih informacij na socialnih omrežjih.
		4.2.2	Zavedati se potrebe, da uporabimo ustrezne nastavitve zasebnosti računov socialnih omrežij.
		4.2.3	Poznati možne nevarnosti pri uporabi socialnih omrežij, kot so: kibernetsko nasilje, zavajanje otrok, zavajajoče ali nevarne informacije, lažne identitete, zlonamerne povezave ali sporočila.
5 Komunikacije	*5.1 Elektronska pošta*	5.1.1	Razumeti namen šifriranja, dešifriranja elektronske pošte.
		5.1.2	Razumeti pojem digitalno potrdilo.
		5.1.3	Ustvariti in dodati digitalni podpis.
		5.1.4	Zavedeti se možnosti prejema zlonamerne in neželene elektronske pošte.
		5.1.5	Razumeti pojem zvabljanje. Prepoznati običajne značilnosti zvabljanja, kot so uporaba imen znanih podjetij, oseb in lažnih spletnih povezav.
		5.1.6	Zavedati se nevarnosti okužbe računalnika z zlonamernim programjem zaradi odpiranja priloge elektronske pošte, ki vsebuje makro ali izvršilno datoteko.
	5.2 Takojšnje sporočanje	5.2.1	Razumeti pojem takojšnje sporočanje (IM) in njegovo uporabo.
		5.2.2	Poznati varnostne pomanjkljivosti takojšnjega sporočanja, kot so zlonamerno programje, dostop preko stranskih vrat in dostop do datotek.

KATEGORIJA	PODROČJE	OZNAKA	POTREBNA ZNANJA
		5.2.3	Prepoznati metode za zagotavljanje zaupnosti med uporabo takojšnjega sporočanja, kot so šifriranje, zakrivanje pomembnih informacij in omejevanje deljenja datotek.
6 Varno upravljanje podatkov	*6.1 Zaščita in varnostno kopiranje podatkov*	6.1.1	Prepoznati načine za zagotavljanje fizične varnosti naprav, kot so beleženje lokacije in podrobnosti o napravah, uporaba kabelskih ključavnic in nadzor dostopa.
		6.1.2	Prepoznati pomembnost obstoja postopkov varnostnega kopiranja za primer preprečitve izgube podatkov, finančnih zapisov ter spletnih zaznamkov in zgodovine.
		6.1.3	Prepoznati značilnosti postopka varnostnega kopiranja, kot so rednost, pogostost, načrtovanje in lokacija hranjenja.
		6.1.4	Varnostno kopirati podatke. Back up data.
		6.1.5	Obnoviti in preveriti veljavnost varnostno kopiranih podatkov.
	6.2 Varno uničenje	6.2.1	Razumeti zakaj trajno brišemo podatke s pogonov in naprav.
		6.2.2	Razlikovati med brisanjem in trajnim uničenjem podatkov.
		6.2.3	Prepoznati običajne metode trajnega uničenja podatkov, kot so razrez, uničenje pogonov in nosilcev, razmagnetenje in uporaba orodij za uničenje podatkov.