ECDL Foundation

ECDL / ICDL IT Security
Syllabus Version 1.0

ECDL / ICDL IT Sigurnost
Nastavni plan verzija 1.0

ECDL Foundation

Purpose

This document details the syllabus for *ECDL / ICDL IT Security*. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for *ECDL / ICDL IT Security* should possess. The syllabus also provides the basis for the theory and practice-based test in this module.

Disclaimer

Although every care has been taken by ECDL Foundation in the preparation of this publication, no warranty is given by ECDL Foundation, as publisher, as to the completeness of the information contained within it and neither shall ECDL Foundation be responsible or liable for any errors, omissions, inaccuracies, loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes may be made by ECDL Foundation at its own discretion and at any time without notice.

Cilj

Ovaj dokument detaljno opisuje nastavni plan i program za IT sigurnost. Kroz ishode učenja, nastavni plan opisuje znanja i vještina koje kandidat treba imati. Nastavni plan je osnovica za praktično - primijenjeni test u području ovog modula.

Izjava o odricanju odgovornosti

European Computer Driving Licence Foundation Ltd. (u daljnjem tekstu: ECDL Fondacija) uložila je najveći mogući trud da bi ova publikacija bila što potpunija i točnija, ali to ne podrazumijeva nikakvo jamstvo ili obvezu. ECDL Fondacija kao izdavač nema obvezu ni odgovornost prema bio kojoj osobi ili entitetu u vezi s ikakvom štetom ili gubitkom zbog informacija sadržanih u ovoj publikaciji. ECDL Fondacija može napraviti izmjene po vlastitom nahođenju, u bilo koje vrijeme bez prethodne obavijesti.

Prijevod: HRVATSKI INFORMATIČKI ZBOR (HIZ), © 2012

HRVATSKI INFORMATIČKI ZBOR
10000 ZAGREB, Ilica 191e/II

Tel: +385 1 2222722
Fax: +385 1 2222723
E-mail: hiz@hiz.hr, info@ecdl.hr
URL: www.hiz.hr, www.ecdl.hr

Hrvatski informatički zbor HIZ 1975

ECDL Foundation

ECDL / ICDL IT sigurnost

Ovaj modul definira osnovne pojmove i vještine koje se odnose na sposobnost razumijevanja glavnih pojmova na kojima se temelji sigurno korištenje ICT u svakodnevnom životu i korištenje odgovarajućih tehnika i aplikacija za održavanje sigurnih mrežnih veza, pažljivo i sigurno korištenje Interneta, te prikladno upravljanje podacima i informacijama.

Ciljevi modula

Uspješni kandidati će moći:

- Razumjeti ključne pojmove koji se odnose na sigurnost informacija i podataka, fizičku sigurnost, privatnost i krađu identiteta.
- Zaštititi računalo, uređaj ili mrežu od štetnog softvera i neovlaštenog pristupa.
- Poznavati tipove mreža, načine povezivanja i specifične probleme, uključujući vatrozid.
- Sigurno pregledavati World Wide Web i komunicirati na internetu.
- Poznavati sigurnosne probleme vezane uz komunikaciju, uključujući e-mail i slanje istovremenih poruka.
- Sigurno i pouzdano napraviti rezervne kopije i obnoviti podatke te raspolagati podacima i uređajima

KATEGORIJA	VJEŠTINA	OZN.	ZADATAK
1 Sigurnost - pojmovi	*1.1 Prijetnje podacima*	1.1.1	Razlika između podatka i informacije.
		1.1.2	Razumijevanje pojma kibernetički kriminal.
		1.1.3	Poznavanje razlike između hakiranja, krekiranja i etičkog hakiranja.
		1.1.4	Prepoznavanje prijetnji podacima od strane više sile: kao što su: požar, poplava, rat, potres.
		1.1.5	Prepoznavanje prijetnji podacima od: zaposlenika, davatelja usluga i vanjskih pojedinaca.
	1.2 Vrijednost informacija	1.2.1	Razumijevanje razloga za zaštitu osobnih podataka kao što su: izbjegavanje krađe identiteta, prijevare.
		1.2.2	Razumijevanje razloga za zaštitu komercijalno osjetljivih informacija kao što su: sprječavanje krađe ili zlouporabe detalja o klijentima, financijske informacije.
		1.2.3	Identificiranje mjera za sprečavanje neovlaštenog pristupa podacima kao što su: šifriranje, lozinke.
		1.2.4	Razumijevanje osnovnih karakteristika informacijske sigurnosti kao što su: povjerljivost, integritet, raspoloživost.
		1.2.5	Identificiranje najvažnijih mjera za zaštitu podataka/privatnosti, čuvanje i kontrolu u vašoj zemlji.
		1.2.6	Razumijevanje važnosti stvaranja i pridržavanja smjernica i politika pri korištenju ICT-a.
	1.3 Osobna sigurnost	1.3.1	Razumijevanje pojma socijalnog inženjeringa i posljedica kao što su: prikupljanje informacija, prijevare, pristup računalnom sustavu.
		1.3.2	Identificiranje metoda socijalnog inženjeringa kao što su: telefonski pozivi, pecanje, virenje preko ramena pri surfanju.
		1.3.3	Razumijevanje pojma krađe identiteta i njegovih posljedica: osobnih, financijskih, poslovnih, pravnih.
		1.3.4	Identificiranje metoda za krađu identiteta kao što su: iskopavanje informacija, neovlašteno kopiranje (skimming), izgovaranje (pretexting).
	1.4 Sigurnost datoteka	1.4.1	Razumijevanje učinka omogućiti/onemogućiti sigurnosne postavke makronaredbi.
		1.4.2	Postavljanje lozinke za datoteke kao što su: dokumenti, komprimirane datoteke, proračunske tablice.
		1.4.3	Razumijevanje prednosti i ograničenja šifriranja (enkripcije).

KATEGORIJA	VJEŠTINA	OZN.	ZADATAK
2 Štetan softver	*2.1 Definicije i funkcije*	2.1.1	Razumijevanje pojma malver (malware) – štetan softver.
		2.1.2	Prepoznavanje različitih načina na koje se štetan softver može sakriti kao što su: Trojanci, rootkitovi i zadnja vrata (back doors).
	2.2 Tipovi	2.2.1	Prepoznavanja vrste zaraze štetnim softverom i razumijevanje kako rade kao što su: virusi, crvi.
		2.2.2	Prepoznavanje načina krađe podataka, štetnog softvera za stvaranje / iznudu dobiti i razumijevanje kako rade kao što su: programi s neželjenim oglasima (adware), špijunski softver (spyware), Botneti, zapisivanje tipki (keystroke logging) i programi za neovlašteno uspostavljanje telefonske veze (Diallers).
	2.3 Zaštita	2.3.1	Razumijevanje načina rada i ograničenja anti-virusnog softvera.
		2.3.2	Skeniranje određenog pogona, mape, datoteke anti-virusnim softverom. Raspored skeniranja korištenjem anti-virusnog softvera.
		2.3.3	Razumijevanje pojma karantene i učinka stavljanja u karantenu zaraženih/sumnjivih datoteka.
		2.3.4	Razumijevanje važnosti preuzimanja i instaliranja ažuriranja, datoteka s antivirusnim definicijama.
3 Sigurnost mreže	*3.1 Mreže*	3.1.1	Razumijevanje pojma mreže i prepoznavanje uobičajenih vrsta mreža kao što su: lokalna (LAN), prostorna (WAN), virtualna privatna mreža (VPN).
		3.1.2	Razumijevanje uloge mrežnog administratora u utvrđivanju autentičnosti, upravljanju autorizacijom i pristupnim pravima unutar mreže.
		3.1.3	Razumijevanje funkcije i ograničenja vatrozida (firewall).
	3.2 Povezivanje na mrežu	3.2.1	Prepoznavanje mogućnosti za povezivanje na mrežu kao što su: kabel, bežično.
		3.2.2	Razumijevanje posljedica na sigurnost pri spajanju na mrežu kao što su: štetan softver, neovlašteni pristup podacima, čuvanje privatnosti.
	3.3 Bežična sigurnost	3.3.1	Prepoznavanje važnosti zahtijeva za lozinkom pri pristupu bežičnoj mreži.
		3.3.2	Prepoznavanje različitih tipove bežične sigurnosti kao što su: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).
		3.3.3	Biti svjestan da korištenje nezaštićene bežične mreže omogućava prisluškivačima pristup podacima.
		3.3.4	Povezivanje na zaštićenu/nezaštićenu bežičnu mrežu.
	3.4 Kontrola pristupa	3.4.1	Razumijevanje svrhe mrežnog računa i kako mu treba pristupati korištenjem korisničkog imena i lozinke.
		3.4.2	Prepoznavanje dobre politike lozinki, kao što su: ne dijeliti lozinke, redovito ih mijenjati, odgovarajuća dužina lozinke, kombiniranje odgovarajućih slova, brojeva i posebnih znakova.
		3.4.3	Poznavanje uobičajenih biometrijskih sigurnosnih tehnika za kontrolu pristupa kao što su: otisak prsta, skeniranje oka.
4 Sigurno pregledavanje Web-a	*4.1 Pregledavanje Web-a*	4.1.1	Biti svjestan da određene aktivnosti na mreži (kupovina, financijske transakcije) treba poduzimati samo na sigurnim web stranicama.
		4.1.2	Prepoznavanje sigurnih web mjesta kao što su: https, simbol lokota.
		4.1.3	Biti svjestan pharming-a.
		4.1.4	Razumijevanje pojma digitalni certifikat. Provjera valjanosti certifikata.
		4.1.5	Razumijevanje pojma jednokratne lozinke.
		4.1.6	Izbor postavki za omogućavanje, onemogućavanje automatskog dovršetka, automatskog spremanja pri popunjavanju obrasca.
		4.1.7	Razumijevanje pojma kolačić (cookie).
		4.1.8	Izbor odgovarajućih postavki za preuzimanje, blokiranje kolačića.
		4.1.9	Brisanje privatnih podataka iz preglednika kao što su: povijest pregledavanja, privremeno spremljene internetske datoteke, lozinke, kolačići, podatci o automatskom dovršetku.
		4.1.10	Razumijevanje svrhe, funkcije i vrste softvera za kontrolu sadržaja kao što su: softver za internet filtriranje, roditeljski nadzor.

KATEGORIJA	VJEŠTINA	OZN.	ZADATAK
	4.2 Socijalne mreže	4.2.1	Razumijevanje važnosti ne otkrivanja povjerljivih informacija na socijalnim mrežama.
		4.2.2	Biti svjestan potrebe da se na računu socijalne mreže primjenjuju odgovarajuće postavke privatnosti.
		4.2.3	Poznavanje potencijalnih opasnosti pri korištenju socijalnih mreža kao što su: kibernetičke prijetnje (cyber bullying), njega (grooming), pogrešne / opasne informacije, lažni identiteti, lažne web veze ili poruke.
5 Komunikacija	*5.1 E-pošta*	5.1.1	Razumijevanje svrhe šifriranja, dešifriranja elektroničke pošte.
		5.1.2	Razumijevanje pojma digitalni potpis.
		5.1.3	Stvaranje i dodavanje digitalnog potpisa.
		5.1.4	Biti svjestan mogućnosti primanja lažne i neželjene e-pošte.
		5.1.5	Razumijevanje pojma pecanje (phishing). Poznavanje zajedničkih karakteristike pecanja kao što su: korištenje imena legitimnih tvrtki, ljudi, lažnih web veza.
		5.1.6	Biti svjestan opasnosti zaraze računala štetnim softverom pri otvaranju privitaka e-pošte koji sadržavaju makronaredbu ili izvršnu datoteku.
	5.2 Istovremene poruke	5.2.1	Razumijevanje pojma izravne poruke (instant messaging - IM) i njegovo korištenje.
		5.2.2	Razumijevanje sigurnosnih ranjivosti IM-a kao što su: štetni softver, pristup kroz zadnja vrata (backdoor), pristup datotekama.
		5.2.3	Poznavanje metoda za osiguranje tajnosti pri korištenju IM-a kao što su: šifriranje, ne otkrivanje važnih informacija, ograničavanje dijeljenja datoteka.
6 Upravljanje sigurnošću podataka	*6.1 Sigurnost i rezervne kopije podataka*	6.1.1	Poznavanje načina za osiguranje fizičke sigurnosti uređaja kao što su: popis lokacija opreme i dijelova, korištenje kablovskih brava, kontrola pristupa.
		6.1.2	Biti svjestan važnosti posjedovanja procedure za kreiranje sigurnosne kopije u slučaju gubitka: podataka, financijskih evidencija, web favorita / povijesti.
		6.1.3	Poznavanje značajki postupka za kreiranje sigurnosne kopije kao što su: redovitost / frekvencija, raspored, mjesto pohrane.
		6.1.4	Stvaranje sigurnosne kopije podataka.
		6.1.5	Obnavljanje i provjera valjanosti sigurnosne kopije podataka
	6.2 Sigurno uništavanje	6.2.1	Razumijevanje razloga za trajno brisanje podataka s pogona ili uređaja.
		6.2.2	Poznavanje razlike između brisanja i trajnog uništavanja podataka.
		6.2.3	Poznavanje uobičajenih metoda za trajno uništavanje podataka kao što su: rezanje, uništavanje pogona/medija, demagnetizacija, korištenje uslužnih programa za uništavanje podataka.