ICDL MODUL IT Sigurnost

Syllabus verzija 2.0

Cilj

Dokument detaljno opisuje nastavni program za ICDL modul IT sigurnost ver. 2.0. Kroz rezultate učenja, nastavni program opisuje znanja i vještine koje kandidat treba imati. Nastavni program je osnovica za praktično - primijenjeni test ovog modula

.

Izjava o odricanju odgovornosti

ECDL Fondacija uložila je najveći mogući napor kako 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 bilo 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 i prilagodba: HRVATSKI INFORMATIČKI ZBOR (HIZ), © 2020

HRVATSKI INFORMATIČKI ZBOR
10000 ZAGREB, Ilica 191e/II

Tel: +385 1 2222 722
E-mail: hiz@hiz.hr, info@ecdl.hr
URL: www.hiz.hr, www.ecdl.hr

Modul IT Sigurnost definira osnovne pojmove i vještine na kojima se temelji sigurno korištenje ICT u svakodnevnom životu i korištenje odgovarajućih tehnika i aplikacija za održavanje sigurnih mrežnih veza, pažljivo korištenje Interneta, te prikladno upravljanje podacima i informacijama.

Ciljevi modula

Uspješni kandidati moraju biti osposobljeni:

- Razumjeti važnost čuvanja i sigurnosti podataka, te utvrditi zajedničke principe njihove zaštite.
- Prepoznati prijetnje osobnoj sigurnosti od krađe identiteta i potencijalne prijetnje podacima korištenjem računalstva u oblaku.
- Moći koristiti lozinke i šifriranje za zaštitu datoteka i podataka.
- Razumjeti prijetnju zlonamjernog softvera i moći zaštititi računalo, uređaj ili mrežu od napada.
- Prepoznati zajedničke mrežne i bežične vrste sigurnosti i biti u mogućnosti koristiti osobni vatrozid i osobne vruće točke.
- Zaštititi računalo ili uređaj od neovlaštenog pristupa i moći sigurno upravljati i ažurirati lozinke.
- Koristiti odgovarajuće postavke web preglednika i razumjeti kako autentificirati web stranice i sigurno pregledavati WEB.
- Razumjeti pitanja sigurnosti komunikacija koja mogu nastati korištenjem e-pošte, društvenih mreža, glasovnog protokola putem Interneta i trenutnih poruka s mobilnih uređaja.
- Izraditi sigurnosnu kopiju i vratiti podatke u lokalne i oblačne lokacije, te izbrisati i raspolagati podacima i uređajima.

KATEGORIJA	VJEŠTINA	OZN.	ZADATAK
1 Sigurnost - pojmovi	*1.1 Prijetnje podacima*	1.1.1	Razlikovati podatke i informacije.
		1.1.2	Razumjeti pojam kibernetičkog kriminala, hakiranje.
		1.1.3	Prepoznati zlonamjerne, slučajne prijetnje podacima od pojedinaca, pružatelja usluga, vanjskih organizacija.
		1.1.4	Prepoznati prijetnje podacima kod izvanrednih okolnosti poput požara, poplave, rata, zemljotresa.
		1.1.5	Prepoznati prijetnje podacima korištenjem računalstva u oblaku poput: upravljanja podacima, te potencijalnog gubitka privatnosti.
	1.2 Vrijednost informacija	1.2.1	Razumjeti osnovne karakteristike informacijske sigurnosti poput: povjerljivosti, integriteta, dostupnosti.
		1.2.2	Razumjeti razloge zaštite osobnih podataka kao što su: izbjegavanje krađe identiteta, prijevara, održavanja privatnosti.
		1.2.3	Razumjeti razloge zaštite podataka na računalima na radnom mjestu i uređajima, poput: sprečavanja krađe, lažne uporabe, slučajnog gubitka podataka, sabotaže.
		1.2.4	Identificirati zajedničke principe zaštite podataka / privatnosti, zadržavanja i kontrole kao što su: transparentnost, zakonitost, razmjernost.
		1.2.5	Razumjeti pojmove subjekata podataka i kontrolora podataka, te kako se na njih primjenjuju načela zaštite podataka, privatnosti i kontrole.
		1.2.6	Razumjeti važnost pridržavanja smjernica i pravila za korištenje ICT i kako im pristupiti.
	1.3 Osobna sigurnost	1.3.1	Razumjeti pojam socijalnog inženjeringa i njegove posljedice kao što su: neovlašteni pristup računalu i uređajima, neovlašteno prikupljanje podataka, prijevare.
		1.3.2	Identificirati metode socijalnog inženjeringa kao što su: telefonski pozivi, phishing, virenje preko ramena.
		1.3.3	Razumjeti pojam krađe identiteta i njegove posljedice: osobni, financijski, poslovni, pravni.
		1.3.4	Identificirati metode krađe identiteta kao što su: pretraživanje odbačenih informacija, neovlašteno kopiranje, pretvaranje.
	1.4 Sigurnost datoteka	1.4.1	Razumjeti učinak omogućavanja / deaktiviranja postavki sigurnosti makronaredbi.
		1.4.2	Razumijeti prednosti i ograničenja šifriranja. Biti svjesni važnosti ne otkrivanja ili gubitka lozinke za šifriranje, ključa, certifikata.
		1.4.3	Šifrirati datoteku, mapu, uređaj.
		1.4.4	Postaviti lozinku za datoteke poput: dokumenata, proračunskih tablica, komprimiranih datoteka.
2 Štetan softver	*2.1 Tipovi i metode*	2.1.1	Razumjeti pojam zlonamjernog softvera. Prepoznati različite načine na koje se zlonamjerni softver može sakriti na računalima i uređajima kao što su: trojanski konji, rootkiti, stražnja vrata.
		2.1.2	Prepoznati vrste zaraznog zlonamjernog softvera i razumjeti kako djeluju: virusi, crvi.
		2.1.3	Prepoznati vrste krađe podataka, zlonamjernog softvera za stvaranje / iznuđivanje i razumjeti kako djeluju: neželjeni oglasi, prijetnje, špijunski softver, botnet, evidentiranje pritiska na tipke, brojčanici.
	2.2 Zaštita	2.2.1	Razumjeti kako djeluje antivirusni softver i njegova ograničenja.
		2.2.2	Razumjeti zašto antivirusni softver treba biti instaliran na računala i uređaje.
		2.2.3	Razumjeti važnost redovitog ažuriranja poput: antivirusnog programa, web preglednika, programskih dodataka, aplikacija, operacijskog sustava.
		2.2.4	Skenirati određene uređaje, mape, datoteke pomoću antivirusnog softvera. Probati skeniranje pomoću antivirusnog softvera.
		2.2.5	Razumjeti rizike upotrebe zastarjelog i nepodržanog softvera poput: povećane prijetnje od zlonamjernog softvera, nekompatibilnost

KATEGORIJA	VJEŠTINA	OZN.	ZADATAK
	2.3 Rješavanje i uklanjanje	2.3.1	Razumijeti pojam karantene i učinak karantene zaraženih / sumnjivih datoteka.
		2.3.2	Karantena, brisanje zaraženih / sumnjivih datoteka.
		2.3.3	Razumjeti da se napad zlonamjernog softvera može dijagnosticirati i riješiti pomoću mrežnih resursa kao što su: web stranice operacijskog sustava, antivirusnih programa, dobavljača softvera za web preglednike, web stranica nadležnih tijela.
3 Sigurnost mreže	*3.1 Mreže i veze*	3.1.1	Razumjeti pojam mreže i prepoznati uobičajene vrste mreža kao što su: lokalna mreža (LAN), bežična lokalna mreža (WLAN), širokopojasna mreža (WAN), virtualna privatna mreža (VPN).
		3.1.2	Razumjeti kako povezivanje s mrežom ima posljedice na sigurnost poput: zlonamjernog softvera, neovlaštenog pristupa podacima, održavanja privatnosti.
		3.1.3	Razumjeti ulogu mrežnog administratora u upravljanju autentifikacijom, autorizacijom računa korisnika na mreži, nadgledanjem i instaliranjem relevantnih sigurnosnih zakrpa i ažuriranja, nadziranjem mrežnog prometa i u postupanju sa zlonamjernim softverom otkrivenim na mreži.
		3.1.4	Razumijeti funkciju ograničenja vatrozida u osobnom, radnom okruženju.
		3.1.5	Uključiti, isključiti osobni vatrozid. Omogućiti blokiranje pristupa aplikaciji, usluzi / značajkama putem osobnog vatrozida.
	3.2 Bežična sigurnost	3.2.1	Prepoznati različite mogućnosti bežične sigurnosti i njihova ograničenja kao što su: privatnost žičane ekvivalentne zaštite (WEP), zaštićeni Wi-Fi pristup (WPA) / zaštićen Wi-Fi pristup 2 (WPA2), filtriranje pristupa, pristup mediju (MAC), skriveni identifikator servisnog skupa (SSID).
		3.2.2	Razumjeti kako uporaba nezaštićene bežične mreže može dovesti do napada poput: prisluškivanja, otmica mreže, čovjek u sredini.
		3.2.3	Razumjeti pojam osobne pristupne točke (hotspot) .
		3.2.4	Omogućiti, onemogućiti sigurnu osobnu pristupnu točku i sigurno povezivanje, isključivanje uređaja.
4 Kontrola pristupa	*4.1 Metode*	4.1.1	Identificirati mjere za sprečavanje neovlaštenog pristupa podacima kao što su: korisničko ime, lozinka, PIN, šifriranje, višefaktorska provjera identiteta.
		4.1.2	Razumijevanje pojma jednokratne lozinke i uobičajene primjene.
		4.1.3	Razumijevanje pojma mrežnog računa.
		4.1.4	Razumjeti kako mrežnom računu treba pristupiti preko korisničkog imena i lozinke i zaključati, odjaviti uređaj kada se ne koristi.
		4.1.5	Identificirati uobičajene biometrijske sigurnosne tehnike koje se koriste u kontroli pristupa kao što su: otisak prsta, skeniranje očiju, prepoznavanje lica, geometrije ruku.
	4.2 Upravljanje lozinkama	4.2.1	Prepoznati dobra pravila o lozinkama, kao što su: odgovarajuća dužina lozinke, odgovarajućih slova, brojeva i posebnih znakova, ne dijeljenje lozinki, redovito mijenjanje, različite lozinke za različite usluge.
		4.2.2	Razumjeti funkciju ograničenja softvera za upravljanje lozinkama.
5 Sigurna upotreba WEB-a	*5.1 Postavke preglednika*	5.1.1	Odabrati odgovarajuće postavke za omogućavanje, onemogućavanje automatskog popunjavanja i automatskog spremanja podataka prilikom popunjavanja obrazaca.
		5.1.2	Izbrisati privatne podatke iz preglednika kao što su: povijest pregledavanja, povijest preuzimanja, spremljene internetske datoteke, lozinke, kolačići, automatsko kompletiranje podataka.
	Sigurno pregledavanje	5.2.1	Imati na umu da se određene mrežne aktivnosti (kupovina, bankarstvo) moraju poduzimati samo na sigurnim web stranicama koristeći sigurnu mrežnu vezu.
		5.2.2	Identificirati načine za potvrdu autentičnosti web stranice kao što su: kvaliteta i vrijednost sadržaja, važeći URL, podaci tvrtke ili vlasnika, kontaktni podaci, sigurnosni certifikat, provjera vlasnika domene.
		5.2.3	Razumjeti pojam omogućavanja redirekcije.
		5.2.4	Razumjeti funkciju i vrste softvera za kontrolu sadržaja kao što su: internetski softver za filtriranje sadržaja, softver za roditeljski nadzor.

KATEGORIJA	VJEŠTINA	OZN.	ZADATAK
6 Komunikacije	*6.1 Elektronička pošta*	6.1.1	Razumjeti svrhu šifriranja, dešifriranja e-pošte.
		6.1.2	Razumjeti pojam digitalnog potpisa.
		6.1.3	Identificirati moguću lažnu e-poštu, neželjenu e-poštu.
		6.1.4	Utvrditi uobičajene karakteristike krađe identiteta kao što su: korištenje naziva legitimnih organizacija, osoba, lažnih web veza, logotipa i marke, poticanja otkrivanja osobnih podataka.
		6.1.5	Biti svjesni kako prijaviti pokušaje krađe identiteta legitimne organizacije, nadležnim vlastima.
		6.1.6	Biti svjesni opasnosti od zaraze računala ili uređaja zlonamjernim softverom, otvaranjem privitka e-pošte koji sadrži makronaredbu ili izvršnu datoteku.
	6.2 Društvene mreže	6.2.1	Razumjeti važnost ne objavljivanja povjerljivih ili osobnih podataka na web lokacijama društvenih mreža.
		6.2.2	Biti svjestan potrebe za primjenom i redovitim pregledom odgovarajućih postavki računa na društvenim mrežama, kao što su: privatnost računa, lokacija.
		6.2.3	Primjena postavki računa na društvenim mrežama: privatnost računa, lokacija.
		6.2.4	Razumjeti potencijalne opasnosti pri korištenju web stranica društvenih mreža poput: cyber maltretiranja, dotjerivanja, zlonamjernog otkrivanja osobnog sadržaja, lažnog identiteta, lažnih ili zlonamjernih veza, sadržaja, poruka.
		6.2.5	Imati na umu mogućnost prijave neprimjerenog korištenja ili ponašanja društvenih mreža davatelju usluga nadležnim tijelima.
	VoIP i Instant poruke	6.3.1	Razumjeti sigurnosne ranjivosti trenutnih poruka (IM) i razgovora preko IP (VoIP) poput: zlonamjernog softvera, pristupa na stražnja vrata, pristupa datotekama, prisluškivanja.
		6.3.2	Prepoznati metode osiguranja povjerljivosti kod korištenja IM i VoIP kao što su: šifriranje, neotkrivanje važnih podataka, ograničavanja dijeljenja datoteka.
	6.4 Mobilnost	6.4.1	Razumjeti moguće posljedice upotrebe aplikacija iz neslužbenih trgovina aplikacijama ao što su: mobilni zlonamjerni softver, nepotrebno korištenje resursa, pristup osobnim podacima, loša kvaliteta, skriveni troškovi.
		6.4.2	Razumjeti izraz dozvola za korištenje podataka.
		6.4.3	Imati na umu kako mobilne aplikacije mogu skinuti privatne podatke s mobilnog uređaja kao što su: kontaktni podaci, povijest, lokacija, slike.
		6.4.4	Biti svjestan hitnih i predostrožnih mjera u slučaju gubitka uređaja kao što su: daljinsko isključivanje, daljinsko brisanje, lociranje uređaja.
7 Upravljanje sigurnošću podataka	*7.1 Sigurnost i rezervne kopije podataka*	7.1.1	Prepoznati načine osiguranja fizičke sigurnosti računala i uređaja kao što su: ne biti bez nadzora, mjesto i detalji opreme loga, koristiti kabelske brave, kontrolu pristupa.
		7.1.2	Prepoznati važnost postupka izrade sigurnosne kopije u slučaju gubitka podataka s računala i uređaja.
		7.1.3	Identificirati značajke postupka izrade sigurnosnih kopija kao što su: pravilnost / učestalost, raspored, mjesto pohrane, kompresija podataka..
		7.1.4	Izraditi sigurnosnu kopiju podataka na lokaciji kao što su: lokalni uređaj, vanjski uređaj /medij, usluga u oblaku.
		7.1.5	Vraćanje podataka sa sigurnosne kopije na: lokalni disk, vanjski uređaj / medij, oblak.
	7.2 Sigurno brisanje i uništavanje	7.2.1	Razlikovati između brisanja i trajnog brisanja podataka.
		7.2.2	Razumjeti razloge za trajno brisanje podataka s uređaja.
		7.2.3	Imati na umu kako brisanje sadržaja možda neće biti trajno na uslugama poput: web mjesta društvene mreže, bloga, internetskog foruma, oblaka
		7.2.4	Identificirati uobičajene metode trajnog brisanja podataka kao što su: uništavanje, uništavanje uređaja / medija, demagnetizacije, korištenja alata za uništavanje podataka.