ECDL Foundation

# ECDL- IT sigurnost

## Nastavni plan (Syllabus) Verzija 1.0

# Modul 7–IT sigurnost

U modulu 7 IT sigurnost su navedeni koncepti i veštine koje se odnose na razumevanje bezbednog korišćenja IKT u svakodnevnom životu. Nastavni plan obuhvata korišćenje relevantnih tehnika i aplikacija za održavanje bezbedne konekcije na mrežu, bezbedno i sigurno korišćenje interneta, kao i upravljanje podacima i informacijama na odgovarajući način.

# Ciljevi modula

Kandidat bi trebalo da:

- Razume ključne koncepte koji se odnose na važnost bezbednosti informacija i podataka, fizičku sigurnost, privatnost i krađu identiteta
- Zaštiti računar, uređaj ili mrežu od zlonamernih programa i neovlašćenih pristupa
- Razume razne vrste mreža, konekcija i specifična pitanja vezana za mrežu uključujući i zaštitni zid (firewall)
- Pretražuje veb i bezbedno komunicira putem interneta
- Razume sigurnosna pitanja vezana za komunikaciju, uključujući e-mail i instant poruke
- Pravi kopiju podataka (back up), povrati (restore) podatke na odgovarajući i bezbedan način i da bezbedno raspolaže podacima i uređajima

| POGLAVLJE | OBLAST | OZNAKA | CILJEVI |
|---|---|---|---|
| **1. Koncepti bezbednosti** | *1.1Podaci* | 1.1.1 | Praviti razliku između podataka i informacija. |
| | | 1.1.2 | Razumeti pojam sajber kriminal |
| | | 1.1.3 | Razumeti razliku između termina hakovanje, krekovanje i etičko hakovanje. |
| | | 1.1.4 | Prepoznati pretnje podacima kao što su: vatra, poplava, rat i zemljotres. |
| | | 1.1.5 | Prepoznati pretnje podacima od strane zaposlenih, servis provajdera i pojedinaca iz spoljnog okruženja. |
| | *1.2 Važnost informacija* | 1.2.1 | Razumeti razloge za zaštitu ličnih podataka: krađa identiteta i prevara. |
| | | 1.2.2 | Razumeti razloge za zaštitu oseljivih poslovnih informacija: krađa ili zloupotrebe detalja klijenata i finansijskih informacija. |
| | | 1.2.3 | Identifikovati mere za sprečavanje neovlašćenog pristupa podacima, kao što su šifrovanje (enkripcija) i lozinke. |
| | | 1.2.4 | Razumeti osnovne karakteristike bezbednosti informacija kao što su: poverljivost, integritet i dostupnost. |
| | | 1.2.5 | Identifikovati vrste zaštite podataka i privatnosti, kontrolu pristupa podacima isl. u vašoj zemlji. |
| | | 1.2.6 | Razumeti važnost kreiranja i pridržavanja smernica i politike korišćenja IKT. |
| | *1.3 Lična sigurnost* | 1.3.1 | Razumeti termin socijalni inženjering i implikacije kao što su: prikupljanje informacija, prevare, pristup sistemu računara. |

| POGLAVLJE | OBLAST | OZNAKA | CILJEVI |
|---|---|---|---|
| | | 1.3.2 | Identifikovati metode socijalnog inženjeringa kao što su: telefonski pozivi, phishing, „surfovanje preko ramena“ (shoulder surfing) . |
| | | 1.3.3 | Razumeti značenje i implikacije termina krađa identiteta: ličnog, finansijskog, poslovnog i pravnog. |
| | | 1.3.4 | Identifikovati metode krađe identiteta kao što su: information diving („kopanje po podacima“), skimming(„skidanje“ podataka sa magnetne trake), pretexting („Izmišljeni scenario“) |
| | *1.4 Bezbednost fajlova* | 1.4.1 | Razumeti uticaj uključivanja/isključivanja makro naredbi. |
| | | 1.4.2 | Postaviti lozinke za fajlove kao što su: dokumenta, kompresovani fajlovi, tabelarne kalkulacije. |
| | | 1.4.3 | Razumeti prednosti i ograničenja šifrovanja (enkripcije). |
| **2. Zlonamerni programi** | *2.1Definicija i funkcija* | 2.1.1 | Razumeti pojam zlonamerni program (malware). |
| | | 2.1.2 | Prepoznati različite vrste prikrivenih zlonamernih programa kao što su: trojans, rootkits i back doors. |
| | *2.2 Vrste* | 2.2.1 | Prepoznati vrste zlonamernih programa kao što su virusi i crvi. |
| | | 2.2.2 | Prepoznati vrste krađe podataka i zlonamernih programa za iznudu kao što su: adware (programi za oglašavanje), spyware (špijunski programi), botnets, keystroke logging i diallers („birači“). |
| | *2.3Zaštita* | 2.3.1 | Razumeti način rada i ograničenja antivirusnog programa. |
| | | 2.3.2 | Skenirati specifične diskove (drives), foldere, fajlove koristeći antivirus program. Zakazati skeniranje antivirus programa. |
| | | 2.3.3 | Razumeti termin „karantin“ i njegov uticaj na zaražene/sumnjive fajlove. |
| | | 2.3.4 | Razumeti važnost redovnog ažuriranja antivirus programa. |
| **3. Bezbednost mreže** | *3.1Mreže* | 3.1.1 | Razumeti termin mreža i razumeti vrste mreža kao što su: LAN, WAN i VPN. |
| | | 3.1.2 | Razumeti ulogu administratora mreže |
| | | 3.1.3 | Razumeti funkciju i ograničenja zaštitnog zida (firewall). |
| | *3.2Način povezivanja na mrežu* | 3.2.1 | Prepoznati opcije za povezivanje na mrežu - putem kabla ili bežično. |
| | | 3.2.2 | Razumeti kako povezivanje na mrežu može uticati na bezbednost: zlonamerni programi, nedozvoljeni pristup podacima, zaštita privatnosti. |
| | *3.3 Sigurnost bežičnih mreža* | 3.3.1 | Prepoznati važnost zaštite bežične mreže. |
| | | 3.3.2 | Prepoznati različite načine zaštite bežične mreže kao što su WEP, WPA, MAC. |

| POGLAVLJE | OBLAST | OZNAKA | CILJEVI |
|---|---|---|---|
| | | 3.3.3 | Biti svestan da korišćenje nezaštićene bežične mreže može dovesti do neovlašćenog pristupa vašim podacima. |
| | | 3.3.4 | Pristup zaštićenoj/nezaštićenoj bežičnoj mreži. |
| | *3.4 Kontrola pristupa* | 3.4.1 | Razumeti svrhu naloga na mreži i pristup korišćenjem korisničkog imena i lozinke. |
| | | 3.4.2 | Razumeti važnost i ispravan način kreiranja lozinke - lozinka treba da sadrži slova,brojeve i znakove isl; treba je redovno menjati, ne treba je deliti ni sa kim. |
| | | 3.4.3 | Identifikovati sigurnosne tehnike u kontroli pristupa kao što su: otisci prstiju ili skeniranje zenice oka. |
| **4. Sigurno korišćenje veba** | *4.1 Veb pretraživanje* | 4.1.1 | Razumeti da se onlajn aktivnosti, kao što je kupovina ili finansijske transakcije, vrše preko sigurnih veb stranica. |
| | | 4.1.2 | Identifikovati sigurne vebsajtove: https, lock symbol isl |
| | | 4.1.3 | Razumeti vrste sajber napada |
| | | 4.1.4 | Razumeti termin digitalni sertifikat. Proveriti valjanost digitalnog sertifikata |
| | | 4.1.5 | Razumeti termin jednokratna lozinka. |
| | | 4.1.6 | Izabrati odgovarajuća podešavanja za omogućavanje i onemogućavanje automatskog unosa i automatskog čuvanja podataka prilikom popunjavanja obrasca. |
| | | 4.1.7 | Razumeti termin „kolačić“ (cookie) |
| | | 4.1.8 | Izabrati odgovarajuća podešavanja za dozvolu ili blokiranje kolačića (cookies). |
| | | 4.1.9 | Obrisati lične podatke iz veb čitača kao što je: istorija pretraživanja, keširani internet fajlovi, kolačići, automatski unos podataka. |
| | | 4.1.10 | Razumeti svrhu, fukncju i vrste programa za kontrolu sadržaja: program za internet filtriranje, programi za roditeljsku kontrolu. |
| | *4.2 Društvene mreže* | 4.2.1 | Razumeti zašto ne treba postavljati lične i privatne podatkena društvenim mrežama. |
| | | 4.2.2 | Razumeti da je potrebno primeniti odgovarajuća podešavanja privatnosti na nalozima društvenih mreža. |
| | | 4.2.3 | Razumeti potencijalne opasnosti pri korišćenju društvene mreže kao što je: uznemiravanje putem interneta, lažni identiteti, zaraženi linkovi ili poruke isl. |
| **5. Komunikacije** | *5.1E-mail poruke (Elektronska pošta)* | 5.1.1 | Razumeti svrhu šifrovanja (enkripcije) i dešifrovanja (decrypting) e-mail poruka. |
| | | 5.1.2 | Razumeti termin digitalni potpis. |
| | | 5.1.3 | Napraviti i dodati digitalni potpis. |
| | | 5.1.4 | Biti svestan mogućnosti primanja lažne i neželjene pošte. |
| | | 5.1.5 | Razumeti termin i karakteristike Phishinga(pokušaj preuzimanja informacija) kao što je korišćenje imena ugledne kompanije, ljudi i lažnih linkova. |

| POGLAVLJE | OBLAST | OZNAKA | CILJEVI |
|---|---|---|---|
| | | 5.1.6 | Biti svestan potencijlnih opasnosti usled otvaranja priloga koji sadrže makro naredbe ili izvršne fajlove. |
| | *5.2Instant poruke* | 5.2.1 | Razumeti termin i svrhu IM – Instant poruka. |
| | | 5.2.2 | Razumeti potencijalne opasnosti prilikom razmene instant poruka kao što su: zlonamerni programi (malware), backdoor pristup, pristup fajlovima isl. |
| | | 5.2.3 | Prepoznati metode obezbeđivanja poverljivosti prilikom razmene IM kao što su: šifrovanje (enkripcija), ne objavljivanje važnih informacija i ograničenja u deljenju fajlova. |
| **6. Upravljanje sigurnošću podataka** | *6.1Sigurnost i pravljenje sigurnosne kopije podataka* | 6.1.1 | Prepoznati načine za obezbeđivanje fizičke sigurnosti uređaja - korišćenje brava za kablove, kontrola pristupa isl |
| | | 6.1.2 | Prepoznati važnost procedure pravljenja kopije podataka u slučaju gubljenja podataka, finansijskih izveštaja, istorije pretraživanja isl. |
| | | 6.1.3 | Identifikovati karakteristike pravljenja kopije podataka kao što su: frekventnost, lokacija za čuvanje podataka, zakazivanje pravljenja kopije. |
| | | 6.1.4 | Pravljenje sigurnosne kopije podataka. |
| | *6.2Trajno uništavanje podataka* | 6.2.1 | Razumeti razlog za trajno brisanje podataka sa diskova ili uređaja. |
| | | 6.2.2 | Razlikovati brisanje i trajno uništavanje podataka. |
| | | 6.2.3 | Identifikovati metode trajnog uništavanja podataka kao što su: korišćenje sekača papira, uništavanje diskova/medija, razmagnetisavanje, korišćenje pomoćnog programa za uništavanje podataka. |