IT Security onlajn obuka

IT Security onlajn obuka upoznaće Vas sa bezbednosnim rizicima korišćenja računara, interneta, društvenih mreža, elektronske pošte, kao i sigurnom upravljanju i zaštiti ličnih i poslovnih podataka. Naučićete osnovne principe sajber bezbednosti i dobićete veće samopouzdanje u svakodnevnim poslovnim aktivnostima.

Ciljevi onlajn obuke

Polaznik će naučiti da:

- Razume važnost zaštite podataka i identifikuje uobičajene principe zaštite podataka i kontrole privatnosti.
- Prepozna pretnje po ličnu bezbednost zbog krađe identiteta i potencijalne pretnje podacima u računarskom oblaku – Cloud-u.
- Bude sposoban da koristi lozinke i šifrovanje za zaštitu fajlova i podataka.
- Razume pretnju od malvera (*malware*) i bude spreman da preduzme osnovne mere za zaštitu računara i drugih uređaja od napada.
- Prepoznaje uobičajene mrežne i bežične bezbednosne rizike i koristi lični zaštitini zid (*firewall*).
- Zaštiti računar ili uređaj od neovlašćenog pristupa i bude u mogućnosti da bezbedno ažurira lozinke.
- Koristi odgovarajuća podešavanja veb pregledača (*web browser*), prepoznaje sigurne veb lokacije i bezbedno pregleda veb sadržaje.
- Razume sigurnosne probleme u komunikaciji, koji mogu nastati korišćenjem e-pošte, društvenih mreža, VoIP, instant poruka i mobilnih uređaja.
- Pravi rezervnu kopiju podataka (*backup*), povrati (*restore*) podatke na odgovarajuće lokacije, briše i odlaže podatke i uređaje na sigurno.

Program obuke

1. Koncepti bezbednosti

1.1 Podaci

1.1.1 Razlika između podatka i informacije

1.1.2 Sajber kriminal, hakovanje, krekovanje i etičko hakovanje

1.1.3 Prepoznati pretnje podacima od strane zaposlenih, servis provajdera i pojedinaca iz spoljnog okruženja

1.1.4 Pretnje podacima kao što su: vatra, poplava, rat i zemljotres

1.1.5 Pretnje podacima u oblaku (Cloud) poput: kontrole podataka, potencijalni gubitak privatnosti

1.2 Važnost informacija

1.2.1 Razlozi za zaštitu ličnih podataka: krađa identiteta i prevara

1.2.2 Razlozi za zaštitu osetljivih poslovnih informacija: krađa, prevara ili zloupotrebe detalja klijenata i finansijskih informacija

1.2.3 Mere za sprečavanje neovlašćenog pristupa podacima, kao što su šifrovanje (enkripcija) i lozinke

1.2.4 Osnovne karakteristike bezbednosti informacija kao što su: poverljivost, integritet i dostupnost

1.2.5 Vrste zaštite podataka i privatnosti, kontrola pristupa podacima u našoj zemlji

1.2.6 Važnost kreiranja i pridržavanja smernica i politike korišćenja IKT

1.2.7 GDPR - General Data Protection Regulation

1.3 Lična sigurnost

1.3.1 Socijalni inženjering i njegove implikacije, kao što su: prikupljanje informacija, pristup računarskoj mreži, prevare (fraud)

1.3.2 Metode socijalnog inženjeringa kao što su: telefonski pozivi, smishing, phishing, shoulder surfing

1.3.3 Značenje i implikacije termina krađa identiteta: ličnog, finansijskog, poslovnog i pravnog

1.3.4 Metode krađe identiteta kao što su: information diving, skimming, pretexting

1.4 Bezbednost fajlova

1.4.1 Efekti uključivanja/isključivanja makro naredbi

1.4.2 Prednosti i ograničenja šifrovanja (enkripcije). Važnost čuvanja ili gubitka lozinke, ključa, sertifikata

1.4.3 Šifrovati fajlove, foldere, drajv

1.4.4 Postaviti lozinke za fajlove kao što su: dokumenta, tabelarne kalkulacije, kompresovane fajlove

2. Zlonamerni programi

2.1 Vrste i metode

2.1.1 Zlonamerni programi (malware): trojanci, rootkits i back doors

2.1.2 Zlonamerni programi (malware): virusi i crvi

2.1.3 Metode krađe podataka i malvera za iznudu kao što su: adware, spyware, botnets, ransomware, keystroke logging i diallers

2.1.4 Ransomware

2.1.5 Botnets i DDoS

2.2 Zaštita

2.2.1 Način rada i ograničenja antivirusnih programa

2.2.2 Razumeti da antivirusni softver treba instalirati na računare i druge uređaje

2.2.3 Skenirati specifične diskove (drives), foldere, fajlove koristeći antivirus program

2.2.4 Razumeti termin ''karantin'' i njegov uticaj na zaražene/sumnjive fajlove

2.2.5 Rizik korišćenja zastarelog softvera bez podrške i važnost redovnog ažuriranja antivirus programa

2.3 Rešavanje i uklanjanje

2.3.1 Efekat stavljanja zaraženih/sumnjivih fajlova u karantin i njihovo brisanje

2.3.2 Razumeti da se napad malvera može dijagnostikovati i spečiti pomoću mrežnih (online) resursa

3. Bezbednost mreže

3.1 Mreže i konekcije

3.1.1 Računarske mreže i vrste mreža: LAN, WLAN, WAN, VPN

3.1.2 Uticaj povezivanja na mrežu na bezbednost: zlonamerni programi, pristup podacima, zaštita privatnosti

3.1.3 Uloga administratora mreže

3.1.4 Funkcija i ograničenja zaštitnog zida (firewall) u ličnom radnom okruženju

3.1.5 Uključiti i isključiti lični zaštitni zid (firewall)

3.2 Sigurnost bežičnih mreža (Wireless Security)

3.2.1 Načini zaštite bežične mreže: WEP, WPA, WPA2, MAC filtering, SSID hiding

3.2.2 Biti svestan da korišćenje nezaštićene bežične mreže može dovesti do

neovlašćenog pristupa vašim podacima, prisluškivanja, preuzimanja mreže ili postavljanja nekoga između

3.2.3 Personal hotspot

3.2.4 Uključiti i isključiti bezbedni personal hotspot, konektujte i diskonektujte uređaje

4. Kontrola pristupa

4.1 Metode – načini

4.1.1 Mere za sprečavanje neovlašćenog pristupa podacima, kao što su: korisničko ime, lozinka, PIN, šifrovanje, višefaktorska autentifikacija

4.1.2 Pojam jednokratne lozinke i njene tipične upotrebe

4.1.3 Razumeti svrhu mrežnog naloga (korisničko ime i lozinka)

4.1.4 Pristup mrežnom nalogu putem korisničkog imena i lozinke

4.1.5 Biometrijske sigurnosne tehnike koje se koriste u kontroli pristupa

4.2 Menadžment lozinki

4.2.1 Dobra politika lozinki

4.2.2 Razumeti funkcije i ograničenja softvera za upravljanje lozinkama

5. Sigurno korišćenje veba

5.1 Podešavanje Veb pregledača (browser-a)

5.1.1 Izabrati odgovarajuća podešavanja za omogućavanje i onemogućavanje automatskog dovršavanja i čuvanja podataka prilikom popunjavanja obrasca

5.1.2 Izbrisati privatne podatke iz pregledača, kao što su: istorija pregledanja, istorija preuzimanja, keširani internet fajlovi, lozinke, kolačići, podaci o automatskom dovršavanju

5.2 Sigurno pregledanje interneta (secure browsing)

5.2.1 Imati na umu da određene mrežne aktivnosti (kupovina, bankarstvo, ...) treba obavljati samo na sigurnim veb stranicama pomoću sigurne mreže

5.2.2 Načini za potvrđivanje autentičnosti veb stranice, kao što su: kvalitet sadržaja, valuta, važeći URL, podaci o preduzeću ili vlasniku, kontakt podaci, bezbednosni sertifikat, potvrđivanje vlasnika domena

5.2.3 Pharming

5.2.4 Funkcije i vrste softvera za kontrolu sadržaja: roditeljska kontrola i filtriranje interneta

6. Komunikacije

6.1 E-mail

6.1.1 Svrha šifrovanja (enkripcije) i dešifrovanja (decrypting) e-mail poruka

6.1.2 Digitalni potpis

6.1.3 Lažna i neželjena pošta

6.1.4 Phishing (pecanje) - metoda krađe identiteta

6.1.5 Prijava pokušaja krađe identiteta nadležnim organima

6.1.6 Opasnosti od zaraze računara i drugih uređaja malverom, usled otvaranja priloga koji sadrže makro naredbe ili izvršne fajlove

6.2 Društvene mreže

6.2.1 Opasnost od postavljanja ličnih i privatnih podataka na društvenim mrežama

6.2.2 Podešavanje privatnosti i lokacija na nalozima društvenih mreža

6.2.3 Potencijalne opasnosti pri korišćenju društvene mreže kao što su: uznemiravanje putem interneta, lažni identiteti, grooming, zlonamerno otkrivanje ličnih informacija

6.2.4 Prijava neprimerenog ponašanja i upotrebe društvenih mreža pružaocu internet usluga i nadležnim organima

6.3 VoIP i instant poruke

6.3.1 Razumeti termine i svrhu VoIP i IM – Instant poruka

6.3.2 Potencijalne opasnosti prilikom razmene IM i VoIP

6.3.3 Metode obezbeđivanja poverljivosti prilikom razmene IM i VoIP

6.4 Mobilne komunikacije

6.4.1 Moguće implikacije korišćenja aplikacija iz lažnih internet prodavnica

6.4.2 Pojam application permissions

6.4.3 Imati na umu da mobilne aplikacije mogu iz mobilnog telefona izvući privatne informacije, kao što su: kontakti, lokacije kretanja, slike, ...

6.4.4 Hitne mere predostrožnosti, ako se mobilni telefon izgubi, kao što su: lociranje uređaja, daljinsko isključivanje, daljinsko brisanje

7. Upravljanje sigurnošću podataka

7.1 Sigurnost i pravljenje sigurnosne kopije podataka (back up data)

7.1.1 Fizička sigurnost računara i drugih uređaja: nadzor, evidencija lokacije i detalja opreme, brave za kablove, kontrola pristupa i slično

7.1.2 Važnost rezervne kopije podataka u slučaju gubitka podataka sa računara ili uređaja.

7.1.3 Karakteristike sigurnosne kopije podataka kao što su: frekventnost, raspored, lokacija za skladištenje, kompresija podataka

7.1.4 Rezervne kopije podataka na različitim lokacijama: lokalni drajv, eksterni drajv, cloud kopija

7.1.5 Vraćanje podataka (restore) sa rezervnih kopija

7.2 Sigurnosno trajno brisanje i uništavanje podataka

7.2.1 Razlikovati brisanje i trajno uništavanje podataka

7.2.2 Razlozi za trajno brisanje podataka sa diskova ili uređaja

7.2.3 Imati na umu da brisanje sadržaja možda neće biti trajno-konačno na sajtovima društvenih mreža, blogovima, forumima i cloud servisima

7.2.4 Metode trajnog uništavanja podataka kao što su: uništavanje diskova/medija, razmagnetisavanje, korišćenje pomoćnog programa za uništavanje podataka.