Program seminara
''Bezbedno korišćenje interneta, društvenih mreža i onlajn komunikacije''

1. Kontrola pristupa

1.1 Metode – načini

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

1.1.2 Pojam jednokratne lozinke i njene tipične upotrebe

1.1.3 Razumeti svrhu mrežnog naloga (korisničko ime i lozinka)

1.1.4 Pristup mrežnom nalogu putem korisničkog imena i lozinke

1.1.5 Biometrijske sigurnosne tehnike koje se koriste u kontroli pristupa

1.2 Menadžment lozinki

1.2.1 Dobra politika lozinki

1.2.2 Razumeti funkcije i ograničenja softvera za upravljanje lozinkama

2. Sigurno korišćenje veba

2.1 Podešavanje Veb pregledača (browser-a)

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

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

2.2 Sigurno pregledanje interneta (secure browsing)

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

2.2.2 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

2.2.3 Pharming

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

3. Komunikacije

3.1 E-mail

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

3.1.2 Digitalni potpis

3.1.3 Lažna i neželjena pošta (spam)

3.1.4 Phishing (pecanje) - metoda krađe identiteta

3.1.5 Prijava pokušaja krađe identiteta nadležnim organima

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

3.2 Društvene mreže

3.2.1 Opasnost od postavljanja ličnih i privatnih podataka na društvenim mrežama

3.2.2 Podešavanje privatnosti i lokacija na nalozima društvenih mreža

3.2.3 Potencijalne opasnosti pri korišćenju društvenih mreža kao što su: uznemiravanje putem interneta, lažni identiteti, grooming, zlonamerno otkrivanje ličnih informacija

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

3.3 VoIP i instant poruke

3.3.1 Razumeti termine i svrhu VoIP i IM – Instant poruka

3.3.2 Potencijalne opasnosti prilikom razmene IM i VoIP

3.3.3 Metode obezbeđivanja poverljivosti prilikom razmene IM i VoIP

3.4 Mobilne komunikacije

3.4.1 Moguće implikacije korišćenja aplikacija iz lažnih internet prodavnica

3.4.2 Pojam application permissions

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

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

4. Upravljanje sigurnošću podataka

4.1 Sigurnost i pravljenje sigurnosne kopije podataka (backup data)

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

4.1.2 Važnost rezervne kopije podataka u slučaju gubitka podataka sa računara ili uređaja

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

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

4.1.5 Vraćanje podataka (restore) sa rezervnih kopija

4.2 Sigurnosno trajno brisanje i uništavanje podataka

4.2.1 Razlikovati brisanje i trajno uništavanje podataka

4.2.2 Razlozi za trajno brisanje podataka sa diskova ili uređaja

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

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