Upute za etičko ponašanje na webu i sigurnost od phishing napada

---

1. Što je phishing napad?

Phishing je oblik cyber prijevare gdje napadači koriste lažne e-mailove, web-stranice ili poruke kako bi vas prevarili da otkrijete svoje osobne podatke (lozinke, brojeve kreditnih kartica, podatke za prijavu na sveučilišne sustave i sl.). Napadači se mogu predstavljati kao vaši kolege, IT podrška ili pouzdane organizacije kako bi vas naveli na neoprezne postupke.

Najčešće metode phishing napada uključuju:

- **E-mail prijevare** – Lažne poruke koje izgledaju kao da dolaze iz pouzdanog izvora.
- **Lažne web-stranice** – Stranice koje imitiraju prave stranice banaka, sveučilišta ili servisa poput Googlea.
- **SMS phishing** – Prijevare putem poruka na mobilnim telefonima.

---

2. Kako prepoznati sumnjive e-mailove?

- **Nepoznat ili neobičan pošiljatelj** – Ako ne prepoznajete adresu pošiljatelja, budite oprezni.
- **Hitnost i prijetnje** – Ako e-mail tvrdi da morate hitno poduzeti akciju (npr. "Vaš račun će biti obrisan!"), provjerite autentičnost prije klikanja na bilo kakve poveznice.
- **Gramatika i pravopis** – Phishing e-mailovi često sadrže gramatičke pogreške i čudne izraze.

- **Sumnjive poveznice** – Prije klika na link, pređite mišem preko njega (bez klikanja) kako biste vidjeli stvarnu adresu na koju vodi.
- **Neočekivani privici** – Ako e-mail sadrži prilog koji niste očekivali, ne otvarajte ga.
- **Neobične poruke kolega ili profesora** – Ako primite poruku od poznate osobe, ali vam se čini neobična, provjerite telefonskim pozivom ili osobnim kontaktom.

---

3. Pravila sigurnog ponašanja na internetu

- **Ne klikajte na nepoznate ili sumnjive poveznice!** Ako dobijete e-mail s poveznicom koja izgleda sumnjivo, prvo provjerite s IT službom sveučilišta.
- **Koristite jake lozinke** – Lozinke trebaju biti složene, unikatne i redovito mijenjane.
- **Ne dijelite svoje podatke putem e-maila** – Prava IT podrška nikada neće tražiti vaše lozinke ili osjetljive podatke putem e-maila.
- **Provjerite adresu web-stranice** – Ako vas e-mail vodi na stranicu koja izgleda kao službena, provjerite adresu (URL). Lažne stranice često imaju sitne izmjene u nazivu domene.
- **Koristite dvofaktorsku autentifikaciju (2FA)** – Google nudi 2FA koji dodatno osigurava vaš račun.
- **Budite oprezni s javnim Wi-Fi mrežama** – Izbjegavajte prijavu na osjetljive račune putem nesigurnih mreža.
- **Redovito ažurirajte softver** – Sigurnosna ažuriranja sustava i aplikacija štite vas od najnovijih prijetnji.
- **Instalirajte antivirusni softver** – Kvalitetan antivirus može blokirati zlonamjerne napade i upozoriti vas na sumnjive aktivnosti.

---

4. Što učiniti ako sumnjate na phishing?

- **Ne klikajte na poveznicu i ne otvarajte privitke!**

- **Odmah prijavite IT službi sveučilišta.**
- **Ako ste kliknuli na sumnjivu poveznicu, odmah promijenite lozinku i prijavite incident.**
- **Upozorite kolege i prijatelje da ne otvaraju slične poruke.**
- **Blokirajte i označite sumnjive e-mailove kao "Phishing" u Gmailu** kako bi se spriječilo daljnje širenje napada.

---

5. Dodatni savjeti za digitalnu sigurnost

- **Budite skeptični prema neočekivanim zahtjevima za osjetljive informacije.**
- **Koristite različite lozinke za različite servise.**
- **Redovito provjeravajte svoje račune** i pratite neovlaštene prijave.
- **Obrazujte se o sigurnosnim prijetnjama** – Napadi se stalno razvijaju, pa je važno pratiti novosti u cyber sigurnosti.
