

SIGURNOST U ONLINE KUPOVINI

Online kupovina donosi mnoge pogodnosti, ali također otvara vrata za različite vrste prijevare i sigurnosnih prijetnji.

Što to točno znači?

Kada kupujemo online, suočavamo se s nizom potencijalnih sigurnosnih prijetnji. Evo nekoliko ključnih aspekata na koje treba obratiti pažnju:

- **Lažne web stranice:** Prijevare putem lažnih web stranica koje izgledaju kao legitimne trgovine, ali zapravo služe za krađu Vaših osobnih i finansijskih podataka. Ove stranice često nude nevjerojatno niske cijene kako bi privukle kupce.
- **Nezaštićene transakcije:** Sigurnost transakcija je ključna. Koristite samo sigurne web stranice koje imaju SSL certifikat (oznaka „https“ ili ikona **lokota** u adresnoj traci) kako biste osigurali da su Vaši podaci zaštićeni (kriptirani) tijekom prijenosa.
- **Krađa identiteta:** Prilikom unosa osobnih podataka na sumnjivim web stranicama, riskirate krađu identiteta. Ovi podaci mogu biti zloupotrijebljeni za razne prijevare.
- **Malware i phishing:** Otvaranje sumnjivih poveznica (linkova) ili preuzimanje datoteka iz neprovjerenih izvora može rezultirati infekcijom Vašeg uređaja malicioznim softverom ili Vas pretvoriti u metu phishing napada.

Što ja mogu učiniti?

Kako biste se zaštitili tijekom online kupovine, slijedite ove preporuke:

- **Provjerite web stranice:** Kupujte samo od poznatih i pouzdanih trgovina. Provjerite recenzije drugih kupaca i tražite kontakt informacije na web stranici. Ponude koje se čine nevjerojatno dobre, često su samo dobar mamac za prijevarne radnje krađe novaca ili podataka. Jedan od alata za inicijalnu provjeru web stranice je <https://www.virustotal.com/gui/home/url>, koji Vam može dati osnovne informacije o tome je li ista bila prijavljivana kao maliciozna.
- **Koristite sigurne načine plaćanja:** Kupujte od trgovaca koji koriste 3D Secure uslugu sigurnog plaćanja (*Visa Secure ili MasterCard Identity Check*). Za dodatnu sigurnost, razmotrite korištenje usluga posrednika u plaćanju (npr. *PayPal*).
- **Redovito ažurirajte uređaje:** Držite svoj operativni sustav, antivirusni softver i web preglednike ažuriranim kako biste zaštitili svoj uređaj od najnovijih prijetnji.
- **Snažne i jedinstvene zaporkе:** Za korisničke račune koristite složene lozinke koje se sastoje od kombinacije slova, brojeva i simbola te koristite različite lozinke za različite račune.
- **Razdvojite poslovnu i privatnu komunikaciju:** Ne koristite službenu opremu (prijenosno računalo, mobitel), poslovne kontakt podatke (email, telefon, mobitel) ili korisničke račune za provođenje privatne online kupovine. Također, na privatnim korisničkim računima ne koristite istu lozinku kao na poslovnim korisničkim računima.
- **Budite oprezni s e-mailovima:** Ne otvarajte linkove ili preuzimajte privitke iz nepoznatih e-mailova koji tvrde da su od trgovina ili banaka. Ako sumnjate, posjetite web stranicu prodavatelja samostalnim upisom adrese web lokacije u preglednik, umjesto otvaranja

Važno je znati da banke putem elektroničke pošte i SMS poruka nikad od svojih klijenata neće tražiti:

- PIN kartice ili autentifikacijskog uređaja (token, mobitel i sl.)
- CVC/CVV kartice
- Aktivacijske ili pristupne kodove za internet ili mobilno bankarstvo
- Instalaciju alata poslanog putem e-mail poruke ili SMS-a
- Presliku osobnih dokumenata

Sigurnost u online kupovini zahtijeva oprez i pridržavanje najboljih praksi. Pridržavanjem ovih savjeta, možete značajno smanjiti rizik od prijevara i zaštititi svoje osobne i financijske podatke.