

Online kupovina donosi mnoge pogodnosti, ali također otvara vrata za različite vrste prijevare i sigurnosnih prijetnji. Bilo da kupujete osobne ili poslovne proizvode, važno je znati kako sigurno navigirati digitalnim tržištem.

## 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 financijskih podataka. Ove stranice često nude nevjerovatno 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 malicioznom softverom ili Vas pretvoriti u metu phishing napada.

## Što ja mogu učiniti?

- **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 nevjerovatno dobre, često su samo dobar mamac za prijevarene 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:** 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 lozinke:** 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 linkova iz e-maila.

**Zaključak**

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.

Lijep pozdrav,  
Croatia banka d.d.