

## Zaštitite svoje osobne podatke

Razvoj i korištenje naprednih tehnologija i usluga korisnicima donosi brojne pogodnosti, no istodobno se povećava i rizik od zlorabe te su korisnici usluga suočeni s nizom potencijalno opasnih elektroničkih sadržaja. Različiti pokušaji prijeara svakodnevna su pojava na Internetu, stoga je potrebno voditi računa o zaštiti osobnih podataka kako oni ne bi završili u „pogrešnim rukama“ i na taj način prouzročili štetu korisnicima.

Jedan od najčešćih oblika prijeara je tzv. „phishing“. Najčešće je riječ o elektroničkoj pošti koja se šalje s krivotvorene adrese, a kroz sadržaj poruke pokušava se manipulirati korisnicima i navesti ih na dostavljanje osobnih podataka, poput korisničkog imena, lozinke, pina, podataka vezanih uz kreditne kartice te ostalih osobnih i povjerljivih podataka. Prikupljanjem osobnih podataka prevaranti imaju mogućnost ostvarivanja materijalne koristi, što korisnicima čiji su podaci kompromitirani može zadati mnoge poteškoće.

Osim putem e-pošte, phishing napadi mogu se provoditi i putem drugih kanala komunikacije, primjerice putem instant poruka (ICQ, Skype), društvenih mreža i slično.

Hrvatski Telekom veliku pažnju poklanja sigurnosti svojih korisnika te im nudi različite oblike internetske zaštite, poput firewalla, antivirusne te antispam zaštite. No, neovisno o primijenjenoj tehnologiji zaštite, uporaba internetskih usluga prvenstveno nalaže dodatan oprez i pozornost korisnika. Stoga je primarno postići sigurnost u korištenju internetskih usluga, u skladu s trendovima njihovog razvoja, kroz edukacije i podizanje razine svijesti javnosti.

U slučaju dobivanja sumnjive elektroničke pošte, savjet korisnicima je da ni u kojem slučaju ne dostavljaju svoje osobne podatke, ne slijede linkove i ne otvaraju priloge koji se nalaze u elektroničkoj poruci, ukoliko nisu u potpunosti sigurni u vjerodostojnost pošiljatelja.

U slučaju primanja sumnjivih e-mail poruka, korisnici takve slučajeve mogu prijaviti na e-mail adresu: [abuse@t-com.hr](mailto:abuse@t-com.hr)

### Kako prepoznati phishing e-mail:

- **Gramatičke greške:** Phishing e-mail poruke često sadrže gramatičke greške jer oni koji ih šalju ne troše mnogo vremena na ispravljanje grešaka, kao što to rade legitimne tvrtke, a često se koriste i automatiziranim alatima za prevođenje teksta (npr. Google prevoditelj). Stoga se phishing poruke općenito doimaju jako neprofesionalnima, osobito ako su na hrvatskom jeziku.
- **Lažne poveznice (linkovi):** Poveznice u phishing porukama često su izrađene na način da se tekst poveznice i URL (adresa na koju poveznica pokazuje) ne poklapaju. Nikad ne slijedite poveznice u sumnjivim porukama. Umjesto toga, postavite pokazivač miša iznad poveznice bez klikanja. Kod većine modernih e-mail programa, u dnu prozora ili iznad pokazivača miša prikazat će se stvarna adresa na koju poveznica pokazuje.
- **Prijetnje ili nagrade:** Kako bi motivirali korisnika da što prije učini ono na što ga se navodi u poruci, kriminalci se često služe prijetnjama ili nagradama. Primjeri prijetnji su zaključavanje korisničkog računa, ukidanje prava na uslugu ili čak zakonske posljedice. Nagrade najčešće uključuju novac (nagrade na lutriji, pokloni, povrati poreza i slično).
- **Oponašanje poznatih tvrtki ili institucija:** Phishing poruke često izgledaju kao da su poslone od strane poznatih tvrtki, internetskih servisa ili državnih i međunarodnih tijela. Krivotvorena adresa pošiljatelja („from“ polje) i vizualni identitet (logotip, font i slično) samo su neke od tehnika za zavaravanje korisnika. Budući da renomirane tvrtke i institucije nikada od korisnika ne traže osobne podatke na ovaj način, lako je prepoznati da je riječ o prijeari.
- **Upozorenja programa:** Moderni e-mail programi i web preglednici (npr. Internet Explorer, Firefox, Chrome) imaju ugrađene mehanizme za prepoznavanje prevarantskih sadržaja. Prigodom otvaranja poruke ili posjeta web stranici, program može korisniku ispisati sigurnosno upozorenje ako postoji mogućnost da se radi o phishingu ili drugoj vrsti opasnosti. Iako vrlo korisni, ovakvi mehanizmi nisu savršeni i nije uputno u potpunosti se na njih osloniti.