**Datum: 16.11.2021.**  **SAOPŠTENJE ZA MEDIJE**

**Najčešće internet zloupotrebe kojih se trebate čuvati**

*Prepoznajte pokušaje prevare, vodite računa o zaštiti ličnih podataka i bezbjednosti*

Upotreba interneta u posljednje dvije godine je rapidno porasla a uporedo sa tim, nažalost i broj pokušaja prevara internet korisnika lažnim e-mail porukama, oglasima, nagradnim igrama, prilikama za laku zaradu ili nekim oblicima prijetnje. U nastavku vam navodimo najčešće pokušaje prevare i kako da ih prepoznate:

**Phishing e-mail**

Ukoliko primite e-mail sumnjivog sadržaja u kojem se od vas traži da izvršite ažuriranja svojih podataka, da kliknete na neki link ili da otvorite prilog poruke, ne slijedite uputstva već e-mail obrišite.

U drugom slučaju, rizikujete da preuzmete zlonamjeran softver na svoj uređaj ili da budete upućeni na neki phishing sajt, gdje će se od vas tražiti da unesete svoje lozinke, broj bankovne kartice ili druge lične podatke.

Lažne poruke se mogu prepoznati po e-mail adresi pošiljaoca a često i po nizu pravopisnih i gramatičkih grešaka u samoj poruci.

**Lažne nagradne igre**

Poruke i objave ovakvog sadržaja najčešće predstavljaju prevare uz lažno predstavljanje i neovlašćeno korištenje grafičkog identiteta. U sadržaju poruke korisnicima se lažno nude pokloni ili učestvovanje u različitim nagradnim igrama ukoliko posjete određene internet adrese.

Ukoliko vam se negdje ponudi nagradna igra za koju se tvrdi da je organizuje kompanija m:tel, savjetujemo vam da prvo provjerite da li informacija o takvoj nagradnoj igri postoji na našim zvaničnim stranicama: [www.mtel.ba](http://www.mtel.ba), [www.blog.mtel.ba](http://www.blog.mtel.ba) ili na m:tel Facebook stranici [www.facebook.com/mtelbih](http://www.facebook.com/mtelbih).

**Pop-up reklame unutar aplikacija**

Agresivno prikazivanje reklamnih poruka i oglasa su karakteristične za aplikacije koje najčešće nemaju neku korisnost već im je cilj da prikažu poruke kad god se uređaj uključi. Te poruke takođe mogu da sadrže link ka sumnjivim web sajtovima ili da navedu korisnika da generiše međunarodni saobraćaj.

Budete oprezni sa aplikacijama koje želite da instalirate, pregledajte utiske drugih korisnika i provjerite koje dozvole traže pri instalaciji.

Takođe, kao zaštitu koristite antivirusni softver koji će blokirati maliciozne aktivnosti, kao što je [Siguran NET](https://sigurannet.mtel.ba/) koji je na raspolaganju m:tel korisnicima mobilne telefonije.

Pored internet prevara, kao korisnik mobilne telefonije obratite pažnju i na klasične pokušaje prevare:

**SMS zloupotrebe**

Lažnim SMS porukama je cilj da se pokuša zbuniti korisnik kako bi pomislio da mu se javlja neko njemu poznat. U pitanju je lažno predstavljenje u kojem se najčešće traži dopuna prepaid računa ili se šalje link na lažnu web stranu sa zahtjevom za unosom bankovnog računa.

**Propušteni pozivi sa nepoznatih ili neuobičajenih brojeva**

Ukoliko dobijete propušten poziv sa nepoznatih međunarodnih brojeva, ne pozivajte brojeve sa ovim numeracijama kako biste izbjegli moguće nepotrebne troškove.

Podsjećamo da se dolazni pozivi za m:tel korisnike kada se nalaze u svojoj matičnoj m:tel mobilnoj mreži ne naplaćuju, bez obzira odakle je poziv upućen.

Za sve nedoumice, pozive ili poruke sa neuobičajenih brojeva, pozovite m:tel korisničku podršku na besplatan broj 066 10 10 10 za prepaid korisnike ili 0800 50 000 za sve postpaid korisnike. Brojevi su na raspolaganju svim našim korisnicima 24 sata svakog dana.