



VARNI NA SPLETU

PREPOZNAJTE SPLETNE PREVARE!

Prevare se pojavljajo odkar pomnimo, v zadnjem času pa so v porastu spletne goljufije, ki ciljajo na pridobitev vašega denarja, občutljivih podatkov ali dragocenih finančnih informacij.

Nekaj tipičnih primerov prevar:

- Klicatelj, ki se predstavlja kot »uslužbenec banke ali tehnične podpore«, vam predlaga namestitev programa za oddaljen dostop, z namenom posodobitve vaše bančne aplikacije.
- Nerealno nizke ponudbe za najem avtodoma, nakup oblačil priznane blagovne znamke ipd.
- Elektronska sporočila s povezavo na neznano sumljivo spletno stran.
- Naslov članka: »Borut Pahor in Luka Dončić predlagata, kako zaslužiti s kriptovalutami!«
- Sogovornik v klepetu vam obljublja, da boste nasledili njegovo premoženje.
- Na vašem transakcijskem računu so se znašla sredstva neznanega izvora.



**ŽRTEV PREVARE LAHKO POSTANE VSAK OD NAS,
ZATO PREVIDNOST NIKOLI NI ODVEČ.**

ZAŠČITITE SE PRED PREVARAMI!

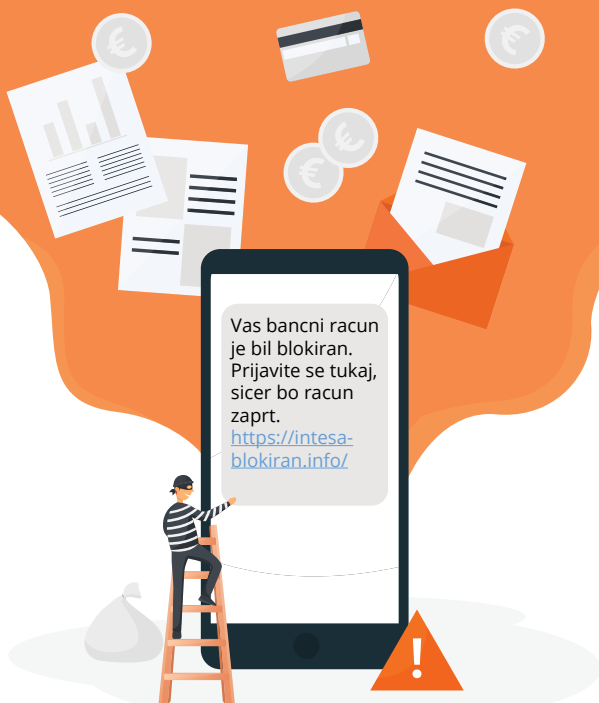
- Ne odgovarjajte na klice in sporočila SMS z **neznanih telefonskih števil**.
- Če prejmete sumljivo elektronsko sporočilo, **ne klikajte na povezave**, ne prenašajte priponk ter nanj ne odgovarjajte.
- Če ste v dvomih o avtentičnosti sporočila, se o verodostojnosti pošiljatelja prepričajte na njegovi spletni strani ali ga kontaktirajte.
- Bodite sumničavi do ponudb, ki obljublajo varno naložbo, zajamčene donose in velik dobiček.
- **Nikomur ne dovolite dostopa** do svoje spletne ali mobilne banke.
- **Ne razkrivajte** številke PIN vaših kartic ali gesel spletnih računov ter ne pošiljajte kopij osebnih dokumentov.
- Sprotno in dosledno preverjajte stanje in transakcije na vašem bančnem računu.
- Oddaljen dostop do računalnika dovolite samo znanim in preverjenim osebam, s katerimi poslovno sodelujete in je to ustaljena praksa.
- Če ste že bili udeleženi v prevari, bodite previdni, saj vas bodo prevaranti verjetno ponovno kontaktirali.
- Ne odstranjujte varnostnih nastavitev na telefonih in tablicah.
- Na računalniku si nastavite geslo, ki je daljše od 16 znakov in ga zamenjajte vsaj vsakih 90 dni. Na mobilnih telefonih in tablicah **uporabite gesla ali biometrične metode**, ki so na voljo.
- Poskrbite, da **nepooblaščen**e osebe **nimajo dostopa** do vašega digitalnega potrdila in zasebnega ključa ali osebnega gesla. Če posumite na zlorabo, nemudoma kontaktirajte overitelja, ki je digitalno potrdilo izdal, in svojo banko.



ČE POSTANETE ŽRTEV PREVARE ...

... NE BODITE V ZADREGI,
AMPAK KAR SE DA HITRO UKREPAJTE!

- **Takoj prekinite vse stike.**
- Če je mogoče, shranite vso komunikacijo, npr. sporočila v klepetu, elektronska sporočila, seznam klicev.
- Vložite prijavo na policijo.
- Sporočite prevaro spletnemu mestu, kjer se je prevarant prvič obrnil na vas.
- Če ste posredovali podatke o vašem transakcijskem računu, kontaktirajte vašo banko. V Intesi Sanpaolo Bank smo vam na voljo na **brezplačni telefonski številki 080 13 18**.



OB SUMU NA PREVARO V SPLETNI ALI MOBILNI BANKI ...



SPLETNA IN MOBILNA BANKA ZA FIZIČNE OSEBE

- Če se prevara dogaja v spletni banki, se **takoj prijavite v vašo mobilno banko**. Na ta način boste prevarantom prekinili sejo v spletni banki.
- Za zaščito pred prevaro lahko mobilno banko načrtno zaklenete (3x vnesete napačno kodo PIN) ali pa izvedete Izbris uporabnika.

Če sumite, da ste bili žrtev (spletne) prevare, lahko reklamacijo ali sum neupravičene transakcije prijavite:

- skrbniku osebno v poslovalnici oziroma na e-naslov skrbnika,
- prek e-pošte na naslov info@intesasanpaolobank.si.



SPLETNA IN MOBILNA BANKA ZA PRAVNE OSEBE

Če sumite, da ste bili žrtev (spletne) prevare, lahko reklamacijo ali sum neupravičene transakcije prijavite:

- skrbniku osebno v poslovalnici oziroma na e-naslov skrbnika,
- prek Poslovne Banke IN,
- prek e-pošte na naslov info@intesasanpaolobank.si.

SKRIBNO RAVNAJTE S PLAČILNIMI KARTICAMI!



Poleg spletne in mobilne banke so plačilne kartice ključna ranljiva točka, prek katerih prevaranti lahko pridejo do vašega denarja. Enako velja tudi za vaš telefon ali drugo napravo, na kateri imate naložene digitalizirane kartice.

- Plačilno kartico in mobilno napravo, na kateri imate naložene digitalizirane plačilne kartice, **ne puščajte brez vašega nadzora.**
- **Številke PIN ne zapisujte nikamor**, še posebej pa je ne hranite skupaj s plačilno kartico.
- **Številke plačilne kartice** in drugih z njo povezanih podatkov **ne razkrivajte nikomur**, tudi če vas povpraša po njih.
- Ne nasedajte elektronskim, telefonskim ali drugim sporočilom, četudi navidezno prihajajo od banke (npr. da je bila vaša kartica zlorabljenjena in morate vnesti podatke v varnostne spletne obrazce ...).
- Vključite si prejemanje varnostnih sporočil SMS ali drugo storitev takojšnjega obveščanja, ki vam jih banka omogoča.
- Redno spremljajte promet na kartici prek mobilne ali spletne banke. **Neznane transakcije takoj sporočite vaši banki, sum kraje kartice pa nemudoma prijavite policiji** – tudi, če ste v tujini.

KARTICO BLOKIRAJTE TAKOJ, KO ZAZNATE ZLORABO!
Prijava izgube ali kraje kartice 24/7: +386 56 66 12 56

Za več informacij obišči našo spletno stran: www.intesasanpaolobank.si/varni-na-spletu



www.intesasanpaolobank.si



08/2024

Banka Intesa Sanpaolo d. d., Pristaniška ulica 14, 6502 Koper, Slovenija, matična številka: 5092221000, ID za DDV: SI98026305, registrski organ: Okrožno sodišče v Kopru, osnovni kapital: 22.173.218,16 EUR, BIC: BAKOSI2X, transakcijski račun: SI56 1011 1102 0304 044.