Spletne prevare

Kako se zaščititi

Marko Marković

Idrija, 24.02.2026

NLB

Najpogostejše pasti, v katere se lahko ujamete

Spletne prevare

Marko Marković

Idrija, 24.02.2025

NLB

PRED SPLETNO GOLJUFIJO SE LAHKO UBRANIŠ LE TAKO, DA JO PREPOZNAŠ.

Spletne goljufije se nenehno spreminjajo in prilagajajo novim tehnologijam. Njihove oblike postajajo vse bolj prefinjene, zato njihova žrtev lahko postane prav vsakdo izmed nas. S hitrim tehnološkim razvojem in digitalizacijo se pojavljajo tudi nove oblike kibernetskih groženj. Zato je ključno, da se nenehno izobražujemo o novih vrstah spletnih goljufij ter razvijamo veščine za varno uporabo tehnologij.

Kaj je spletna prevara?

Vas nekdo prosi za PIN, geslo ali številko kartice?

Gre za poskus prevare. NLB teh podatkov nikoli ne zahteva po telefonu, e-pošti ali SMS-u.

Vas vabijo v sumljivo spletno trgovino?

Klik na napačno povezavo vas lahko drago stane – lahko vam ukradejo podatke plačilne kartice ali vas prepričajo v nakup neobstoječega izdelka. Vedno preverite naslov spletne strani in pošiljatelja povezave.

Želite visok zaslužek brez tveganja?

Prevaranti vas skušajo prepričati s ponudbami, kjer lahko "v kratkem času zaslužite veliko denarja" – brez tveganja. A v resnici vam želijo izmakniti denar ali osebne podatke.

Zahtevajo od vas hitro ukrepanje?

"Takoj ukrepajte, sicer boste izgubili denar!" je priljubljena taktika prevarantov. Vzemite si čas za premislek - resna banka vas nikoli ne sili v hiter odziv.

Kako se lahko zaščitite?

- **Ne delite osebnih podatkov**

NLB jih od vas nikoli ne bo zahtevala preko e-pošte ali telefona.

- **Preverjajte pošiljatelje in povezave**

Klikajte le na znane, preverjene naslove.

- **Ne nasedajte “predobrim” ponudbam**

Visok zaslužek brez tveganja je skoraj vedno znak za alarm

- **Uporabljajte licenčno programsko opremo**

S tem si zagotovite redne posodobitve, tehnično podporo in večjo zaščito pred zlonamerno programsko

- **Nameščajte aplikacije samo iz uradnih trgovin**

Na nalagajte nepoznanih mobilnih aplikacij (npr. AnyDesk, TeamViewer,…).

- **Spremljajte stanje na računu**

Redno spremljajte stanje na vašem računu, saj se zlorabe lahko zgodijo tudi z zamikom

- **Vklopite potisna obvestila in SMS alarme**

Tako boste takoj obveščeni o dogajanju na računu.

- **Namestite uradno pridobljen protivirusni program**

Le uradno pridobljeni programi omogočajo učinkovito zaščito pred virusi, vohunsko programsko opremo in drugimi kibernetskimi grožnjami.

Ključne številke na dlani

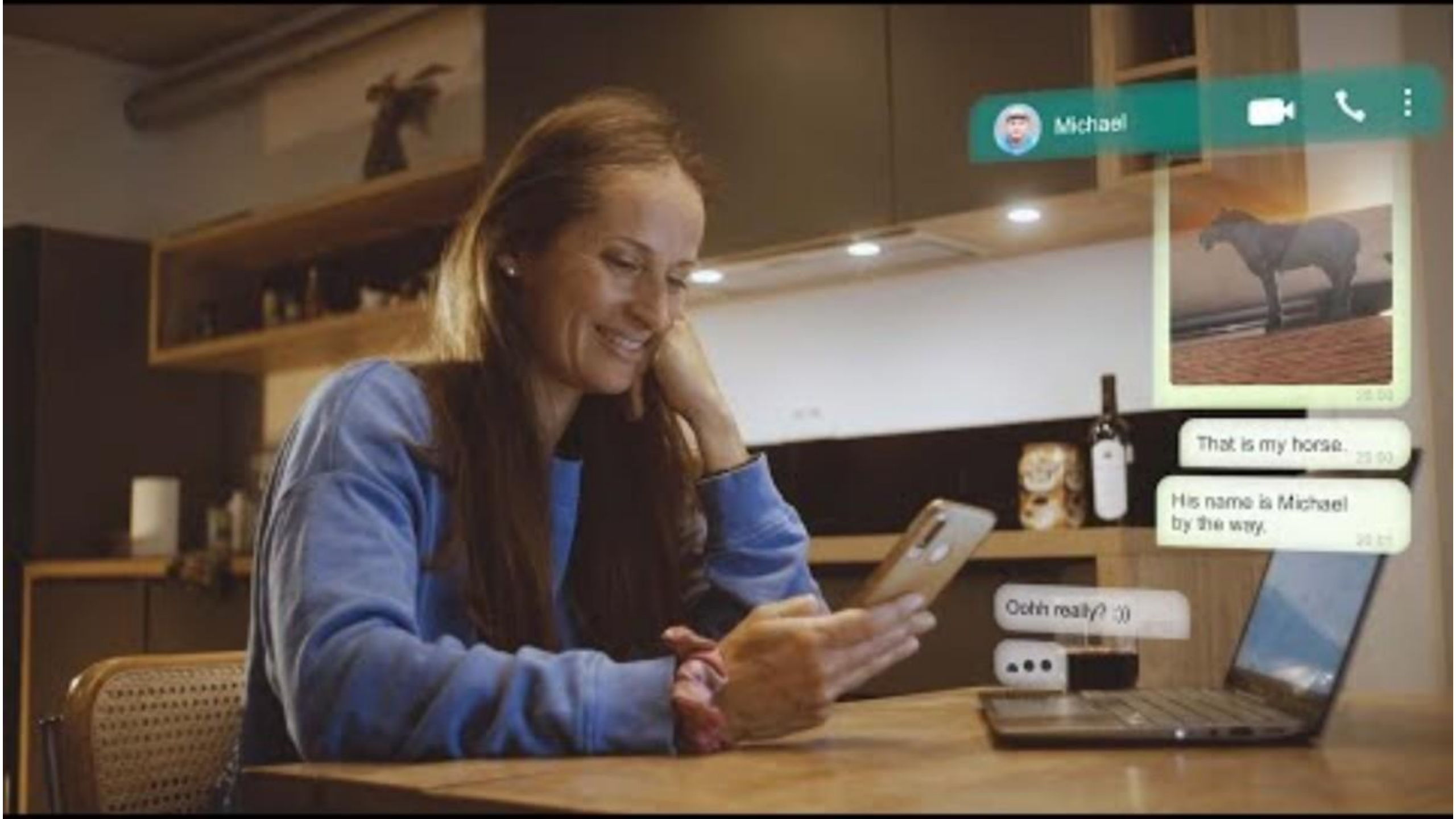
6196 incidentov, od tega 778 zahtevnejših,

35-odstotni porast incidentov in 44-odstotni porast prejetih prijav,

1995 primerov phishinga,

1100 zlonamernih domen,

Celoten znesek prijav kaznivih dejanj spletnih goljufij v letu 2025 je znašal 40,4 milijona evrov, kar je kar 33-odstotni porast v primerjavi z letom 2024.


Michael
That is my horse.
His name is Michael by the way.
Oohh really? :))

Ste prepričani, da bi prepoznali spletno prevaro?

Prevare s skrito naročnino

Kako deluje prevara?

Zasledite privlačen oglas ali objavo na družabnih omrežjih, ki obljublja izdelek za nizko ceno ali celo brezplačno. Po kliku ste preusmerjeni na stran s kvizom ali kratkim preizkusom, ne glede na odgovore pa prejmete »posebno ponudbo«. Za »dostavo« ali »aktivacijo« ponudbe je potrebno vnesti osebne podatke in podatke plačilne kartice. V drobnem tisku je skrito, da gre za preizkusno obdobje, po katerem se začne mesečno zaračunavanje – pogosto med 30 in 60 EUR. Odjava je skoraj nemogoča, pomoč uporabnikom pa pogosto neodzivna

Na kaj morate biti pozorni?

Na zelo ugodne ponudbe, ki obljubljajo skoraj nemogoče. Na obvezno vnašanje podatkov plačilne kartice za »brezplačen« izdelek. Na drobni tisk – tam se ponavadi skriva podatek, da gre za naročnino.

Kako se zaščitite?

Ne vnašajte podatkov plačilne kartice, če niste prepričani o legitimnosti spletne strani. Kritično presojajte oglase z neverjetnimi ponudbami in brezplačnimi izdelki. Če ste že posredovali podatke in so vam obračunali storitev, poskusite prekiniti naročnino. Če to ni mogoče, čimprej kontaktirajte banko.

Ste prepričani, da bi prepoznali spletno prevaro?

Kaj je phishing?

Phishing je spletna prevara, pri kateri prevaranti želijo pridobiti vaše osebne podatke, kot so gesla, številke bančnih kartic ali druge občutljive informacije. Najpogosteje se to zgodi prek e-pošte, sporočil ali lažnih spletnih strani, ki izgledajo kot resnične. Kako prepoznati phishig Nepričakovano sporočilo: Če prejmete e-pošto ali sporočilo od banke, podjetja ali znanca, ki ga ne pričakujete, bodite previdni.

Lažni alarmi:

Pogosto sporočila trdijo, da je vaš račun blokiran, in zahtevajo, da "takoj ukrepate". Sumljivi naslovi: Prevaranti uporabljajo naslove, ki so podobni resničnim, vendar imajo majhne napake (npr. "banka-sigurnost.com" namesto "banka.si").Povezave in priponke: Nikoli ne klikajte sumljivih povezav ali ne odpirajte priponk, ki jih ne pričakujete.

Kaj lahko storite:

Ne hitite: Če niste prepričani, ne ukrepajte takoj. Posvetujte se s kom, ki mu zaupate. Preverite vir: Pokličite podjetje ali osebo, ki naj bi vam poslala sporočilo, in preverite, če je resnično. Zaščitite svoje geslo: Nikoli ne vpisujte gesla na straneh, ki niso uradne. Posodobite naprave: Poskrbite, da imate na računalniku ali telefonu nameščene najnovejše posodobitve in protivirusni program.

Zapomnite si, da vas banke ali uradne ustanove nikoli ne bodo prosile za osebne podatke ali gesla prek e-pošte ali sporočil. Če ste v dvomih, raje ne naredite nič in poiščite pomoč!

Ste prepričani, da bi prepoznali spletno prevaro?

Kako zlonamerne aplikacije na telefonu beležijo vsak vaš dotik telefona?

Zlonamerne aplikacije, ki jih prenesete iz nepreverjenih virov (ne iz uradnih trgovin, kot so Google Play, App Store ali App Gallery), so lahko zelo nevarne. Take aplikacije lahko beležijo vse, kar počnete na napravi – vaše gesla, uporabniška imena, prebirajo vaše e-pošte, SMS sporočila in celo prestrezajo enkratna gesla za dostop do spletne banke.

Kaj lahko naredijo?

Popoln nadzor: Zlonamerne aplikacije lahko prevzamejo popoln nadzor nad vašo napravo, tudi če je zaslon zaklenjen. Dostop do spletne banke: S pomočjo teh aplikacij goljufi lahko vdrejo v vašo spletno ali mobilno banko in ukradejo denar.

Kako se zaščititi?

Prenesite aplikacije samo iz uradnih trgovin: Aplikacije vedno nameščajte iz zaupanja vrednih virov, kot so Google Play, App Store ali App Gallery. Preverite dovoljenja: Preden aplikaciji odobrite dostop, preverite, katere dostope zahteva. Aplikacijam ne dovolite dostopa do funkcije za dostopnost (ang. accessibility).

Bodite pozorni na sumljive zahteve: Če aplikacija zahteva preveč dovoljenj ali dostop do podatkov, ki jih ne potrebuje, je to lahko znak prevare. Če niste prepričani, ali je aplikacija varna, se raje posvetujte z nekom, ki mu zaupate. Nikoli ne nameščajte aplikacij, ki niso iz uradnih virov, saj lahko resno ogrozite svojo varnost.

Pomembne informacije o zlorabah

Pomembne koristne povezave

Na televizijah, družabnih omrežjih in plakatih ste gotovo opazili zelo jasno sporočilo: Pazi.se, ki je tudi naslov posebne spletne strani https://www.pazi.se.

V primeru spletne zlorabe, naj žrtev zlorabe nemudoma kontaktira banko, saj lahko blokiramo kartice ali digitalno bančništvo. Prav tako naj zlorabo seveda prijavi policiji. Ostali nasveti so navedeni na naši namenski spletni strani: https://www.nlb.si/osebno/varnost

Hvala za pozornost.

Za vse, kar sledi.

Marko.markovic@nlb.si 041 667 930

NLB