

**Odgovori Združenja bank na novinarska vprašanja glede spletnih prevar**

**Vprašanja**:

1. Katere so trenutno najbolj pogoste prevare - prek SMS sporočil ali pa prek e-mail naslovov, ko se goljufi predstavljajo kot banka? In za kakšne prevare konkretno gre?
2. Opazil sem, da določene banke opozarjajo tudi na previdnost pri nalaganju denarja v različne naložbe, tudi kriptovalute, saj se lahko zgodi, da gre za lažne ponudnike?
3. Za konec pa še, katera so glavna navodila glede previdnosti, da ne pride do spletnih prevar, in kako ukrepati, v kolikor se to vendarle zgodi?

**Odgovori ZBS:**

1. Banke in hranilnice se ne glede na to, da phishing napadi niso nekaj novega, še vedno zelo pogosto srečujejo prav s poskusi phishing incidentov, ki predstavljajo napade z lažnim predstavljanjem, najpogosteje preko elektronskih sporočil, ki poskušajo prejemnika prepričati v razkritje občutljivih podatkov (gesel, podatkov glede kreditnih kartic…). Spomnimo, lani od aprila dalje je bilo v Sloveniji beležiti več valov phishing napadov na slovenske uporabnike pod krinko plačila za dostavo paketa. V začetku lanskega leta so nekatere banke zaznale tudi več napadov na svoje komitente, pri čemer so napadalci povezave na lažne spletne strani pošiljali v SMS sporočilih, ki so bila poslana na naključne telefonske številke. Nenazadnje je treba omeniti še ciljane phishing napade na zaposlene v bankah in hranilnicah oz. podjetjih, pri čemer so elementi sporočila vsebovali tudi navidezno resnične podatke o banki ali hranilnici oz. podjetju. SI-CERT je tako lani obravnaval 488 zadev (predlani 301 tovrstnih primerov), povezanih z phishing sporočili, in 202 zadev, povezanih s phishing spletnimi mesti (predlani 134).

Banke in hranilnice v tem trenutku nimajo evidentiranih incidentov oškodovanja strank, četudi je zgoraj opisanih poskusov napadov tudi letos kar nekaj. Banke in hranilnice si zato vsled varnega poslovanja neprestano prizadevajo za ustrezno obveščanje svojih strank in informacije glede poskusov prevar nemudoma delijo s SI-CERTom, ki je slovenski nacionalni odzivni center za kibernetsko varnost. Tesno sodelujejo tudi s policijo.

1. Združenje bank Slovenije je v prejšnjem tednu ponovno povzelo obvestilo policije, v katerem policija opozarja na porast oškodovanja državljanov Slovenije, ki še vedno nase dajo lažnim spletnim platformam z obljubami visokih donosov iz naslova investicijskih vlaganj. Konkretni podatki kažejo, da je sicer problematika začela izstopati že v letu 2020, ko je bilo obravnavanih 83 zadev s skupnim oškodovanjem v višini več kot dva milijonov evrov. Letos pa je bilo samo do konca meseca avgusta obravnavanih že 115 zadev s skupnim oškodovanjem v višini več kot pet milijonov evrov.

Poudarki iz obvestila policije:

Za tovrstne goljufije je značilno, da storilci na spletu ponujajo različne oblike lahkega zaslužka, pri čemer potencialne oškodovance privabljajo z možnostjo vlaganja sredstev v različne oblike naložb (virtualne valute, zlato, sklade ipd.) in z obljubami o nerealno visoki donosnosti (tudi po več odstotkov dnevno).

Oškodovanci svoja denarna sredstva v višini več tisoč ali celo več deset tisoč evrov vlagajo v lažnive naložbene produkte. Do tega lahko pride na različne načine, in sicer:

* na podlagi oglasa na družbenih medijih, ki ponuja možnost zanesljivega, hitrega in visokega zaslužka;
* na podlagi stika, ki ga goljufi v nadaljevanju vzpostavijo s potencialnimi oškodovanci po telefonu ali elektronski pošti; v nekaterih primerih kontaktne podatke pridobijo preko obrazca, ki ga oškodovanec izpolni na spletu, ali iz javno dostopnih podatkov, obstajajo pa tudi primeri, ko goljufi kličejo na naključne telefonske številke;
* brez predhodne preveritve (preko spleta, po telefonu ali osebno), ali je v ozadju produkta dejansko ponudnik naložbenih storitev ali pa gre samo za zlorabo imena ali oznake uveljavljenih ponudnikov investicijskih storitev oz. za izmišljenega ponudnika;
* oškodovanci si po navodilu goljufa na svoj računalnik namestijo program za oddaljen dostop (običajno Anydesk), s čimer storilcem omogočijo v celoti upravljati s svojim računalnikom;
* goljufi postanejo njihovi "osebni asistenti" in prek oddaljenega dostopa na lažni investicijski platformi v imenu oškodovanca odprejo trgovalni račun ter denarnice za virtualne valute;
* oškodovanci nepoznanim osebam zaupajo geslo spletne banke, podatke o plačilnih karticah in druge bančne podatke; nato goljufi opravijo prenakazilo denarja na račune v tujini z namenom nakupa virtualnih valut;
* goljufi v profilih lažnih investicijskih platform prikazujejo visoke donose, ki pa v resnici sploh ne obstajajo, saj njihovih vložkov ne investirajo v produkte, temveč jih odtujijo s transakcijami v druge virtualne denarnice.

Če ugotovite, da ste svoja sredstva investirali v produkt, ki ne omogoča izplačila vloženih sredstev, ste bili najverjetneje žrtev goljufije, zato svetujemo, da zadevo nemudoma prijavite na najbližji policijski enoti ali na spletnem mestu policije: [Vloga za naznanilo kaznivega dejanja policiji](https://e-uprava.gov.si/podrocja/vloge/vloga.html?id=377).

**3.** Varnostna in previdnostna opozorila, ki jih velja upoštevati pri uporabi spletnih aplikacij, so naslednja:

* Vsi uporabniki interneta morate vedeti, da ste s poslovanjem preko interneta izpostavljeni varnostnim tveganjem, ki se jim s poznavanjem varnega poslovanja lahko izognete oziroma omejite škodo ob ugotovljeni morebitni zlorabi. Žal ne obstaja en sam opozorilni znak, ki bi z gotovostjo kazal na spletno prevaro.
* Pred prvim nakupom oziroma po menjavi plačilne kartice preverite, ali lahko spletni nakup potrdite z uporabo močne avtentikacije.
* Pri spletnem nakupovanju si vzemite čas in natančno preverite spletno trgovino in samega trgovca, saj nas to lahko obvaruje pred kasnejšo finančno škodo v obliki nedostavljenega izdelka ali zlorabe sredstev s kreditne kartice.
* Velja namreč, da so vse lažne spletne trgovine zasnovane po istem kopitu; izdelki priznanih blagovnih znamk so na voljo po izjemno nizkih cenah, dostava je brezplačna na vse konce sveta, vsi artikli so na zalogi, ni pa nobenih podatkov o samem podjetju, ki stoji za trgovino. Uporabniki zato pred nakupom vselej preverite vse navedene kontaktne podatke, ali je na voljo podpora prek telefona, elektronske pošte ali je na strani zgolj kontaktni obrazec. Obvezno preverite podatke o domeni na strani https://whois.domaintools.com/, vse pogoje plačila, vračila in dostave. Nizke cene in 70-odstotni popusti so pogosto znak sumljivega spletnega poslovanja.
* Če na spletni strani ne najdemo podatkov o trgovcu, npr. sedeža podjetja, matične številke, je to prvi znak, da morate biti pozorni. Velja tudi, da nakupe pri slovenskem trgovcu oz. znotraj EU ščiti enotna evropska potrošniška zakonodaja in da se v primeru težav lahko obrnemo na Tržni inšpektorat oz. Evropski potrošniški center. Pri opravljenih nakupih izven EU (največkrat je to Kitajska) pa smo brez pravic in prepuščeni dopisovanju s trgovcem. Seveda v primeru lažne spletne trgovine trgovec sploh ne obstaja, ampak smo nasedli le lepim slikam na spletni strani.
* Če boste koristili plačila na spletnih prodajnih mestih v tujini preverite ali imate urejeno potrjevanje spletnih plačil skladno z zahtevami močne avtentikacije (za trgovce znotraj EU) in varnostnim standardom 3D Secure, ki jih prepoznate po logotipu »MasterCard SecureCode« oz. »Mastercard ID Check« ali »Verified by Visa« oz. »Visa Secure«.
* Če boste koristili plačila na spletnih prodajnih mestih v tujini, preverite ali imate urejeno potrjevanje spletnih plačil skladno z zahtevami močne avtentikacije in varnostnim standardom 3D Secure.
* Če spletna stran ne uporablja varnostne zaščite 3-D secure in niste prepričani glede varnosti/verodostojnosti spletne strani, kjer želite opraviti plačilo, tega ne storite, dokler se ne prepričate, da je storitev varna.
* Če je v preteklosti veljalo prepričanje, da je **HTTPS** popolnoma varna povezava, ker je šifrirana, pa se je treba zavedati, da **ni vsemogočni znak varnosti,** saj lahko predstavlja tunel, kjer nihče ne vidi podatkov vaše kreditne kartice in na drugi strani tunela čaka goljuf, ki bo vaše podatke prejel in jih zlorabil. Zato vnesite podatke kreditne kartice le, ko ste preverili, kdo dejansko stoji za spletno trgovino, torej kdo bo podatke obdeloval.
* Nikoli ne dostopajte do spletne strani na internetu preko povezave, ki ste jo prejeli v e-sporočilu ali sporočilu SMS/ MMS oziroma na takih spletnih straneh v obrazce ne vnašajte osebnih podatkov.
* Bodite pazljivi na objave na socialnih omrežjih, e-sporočila, ki jih niste zahtevali ali iskali, ali na klice, pri katerih vas sprašujejo po osebnih podatkih in med njimi po številkah plačilnih kartic. Te podatke hranite varno in jih na tak način ne razkrijte.
* V primeru, da trgovec nakup ali vpogled v artikle ali zalogo pogojuje z namestitvijo aplikacije, tega ne storite, saj se tovrstne aplikacije lahko izkoristijo za prestrezanje kartičnih podatkov oziroma potrditvenih (SMS) sporočil.
* Sicer bodite pazljivi pri razkrivanju kakršnih koli osebnih podatkov na spletu in socialnih omrežjih.
* Obvezno poskrbite, da je tudi naprava, preko katere opravljate spletni nakup ustrezno zaščitena pred vdori, zlorabami in zlonamerno programsko opremo oziroma redno skrbite za varnostne popravke in nadgradnje vaših elektronskih naprav, s katerimi plačujete. Redno preverjajte posebne – nove informacije in napotke, kako zaščititi vaš osebni računalnik in naprave ter sebe pri uporabi spletnih strani na internetu.
* Posebej bodite pozorni, kdaj in za kakšne namene uporabljate javne dostopne točke (knjižnice, kavarne) ali katerikoli osebni računalnik, ki ni vaš in nad katerim nimate nadzora. Pred odhodom vedno preverite, če ste pobrisali za seboj vse osebne in občutljive podatke. Navodila, kako zbrisati zgodovino in kaj se v njej shranjuje, so objavljena na spletnih straneh spletnih brskalnikov.
* Nikoli ne zapustite računalnika, ko ste varno povezani na spletno stran trgovca. Prepričajte se tudi, da ste se pravilno odjavili, ko ste končali nakup in če je bila predhodno potrebna prijava. Prijava na trgovčevo spletno prodajno mesto namreč običajno ni neposredno povezana z neposredno uporabo kartice oziroma se podatke o kartici večinoma vnaša sproti ali na ločenih spletnih straneh (npr. 3D Secure). Zato je odjava pomembna v primerih, ko ob registraciji kartico povežemo z uporabniškim računom (npr. Ali Express).
* Vklopite si prejemanje varnostnih SMS sporočil ali drugo storitev takojšnjega obveščanja, ki jih omogoča vaša banka ali hranilnica. Tako boste obveščeni o plačilih ali dvigih gotovine na bančnem avtomatu z vašo plačilno kartico. Če veste, da plačilne kartice niste uporabili, vas bo varnostno SMS ali drugo takojšnje sporočilo opozorilo, da se z vašo plačilno kartico dogaja nekaj nenavadnega. V tem primeru morate takoj obvestiti svojo banko, hranilnico ali procesni center, ki bodo izvedli ustrezne preventivne ukrepe ter preprečili nadaljnjo zlorabo kartice.
* Redno spremljajte vaše transakcije s plačilno kartico prek varnostnih SMS oz. drugih takojšnjih obvestil, spletne/mobilne banke ali izpiskov prometa, ki vam jih pošlje banka ali hranilnica. Če opazite transakcije, ki jih niste opravili, o tem takoj obvestite svojo banko ali hranilnico. O morebitni zlorabi obvestite tudi policijo; incident pa lahko tudi sami prijavite na SI-CERT.

Združenje bank Slovenije
Ljubljana, 27. september 2021