PRIROČNIK
VARNEGA SPLETNEGA POSLOVANJA

NovaKBM

VSAK LAHKO POSTANE ŽRTEV PREVARE

Porast uporabe digitalnih kanalov komuniciranja odpira novo polje izpostavljenosti uporabnikov, ki ga s pridom izkoriščajo predvsem spletni goljufi. Z izrazom spletne prevare razumemo kakršno koli shemo goljufij, kjer se uporabljajo e-pošta, spletna mesta, klepetalnice. Pravzaprav so to vse goljufije, ki jih prevaranti storijo s pomočjo interneta, z namenom finančno ogoljufati potencialne žrtve. Prevaranti s pomočjo spletne komunikacije zavedejo svoje žrtve - z goljufivimi prošnjami, da žrtev izvede transakcijo, največkrat v tujino.

Bolj kot je družabno omrežje popularno, večjo možnost in potencial imajo goljufi, da to virtualno druženje, pogovarjanje, spoznavanje, povezovanje izkoristijo za izvajanje finančnih prevar. Ne smemo zanemariti dejstva, da digitalne platforme uporabljajo tudi starejši, ki jim je to okolje novo in ne poznajo vseh njegovih pasti.

V Novi KBM smo v zadnjem času zaznali povečanje prevar z vnaprejšnjim plačilom stroškov. Tudi o teh prevarah si lahko več preberete v nadaljevanju. Zaznali smo tudi povečanje prevar pri podjetnikih, in sicer prevaro, ki jo imenujemo vrivanje v poslovno komunikacijo. Goljufi vdrejo v elektronsko pošto podjetja ali njihovega poslovnega partnerja iz tujine, spremljajo komunikacijo in spremenijo številko računa za plačilo. Denar tako namesto na račun prodajalca odteče na račun goljufov.

S spremljanjem sumljivih transakcij, ki v Novi KBM poteka v Oddelku za preprečevanje prevar, se s pomočjo sistemov za avtomatizirano spremljavo zlorab tvorijo alarmi. Te sisteme v Novi KBM uporabljamo predvsem za odkrivanje kartičnih zlorab.

V Oddelku za preprečevanje prevar alarme skrbno spremljamo in morebitno možnost zlorabe preverimo pri uporabniku. S stranko se pogovorimo, preverimo, kako je do zlorabe prišlo in jo seveda skušamo preprečiti v prihodnje. V primeru potrjene zlorabe imetniku kartico zablokiramo in naročimo na stroške banke novo. Pomembno je opozoriti na uporabo varnostnih SMS sporočil. SMS sporočilo je v bistvu alarm, ki ga uporabnik prejme ob vsaki transakciji po njegovih karticah (plačilo, prenos, dviga denarja ...). Gre za dodatni varnostni element poslovanja, saj je stranka hitro obveščena, če nekdo nepooblaščeno uporablja njena sredstva. Prav hitra identifikacija prevare omogoča hitro ukrepanje, ki je bistveno pri preprečevanju kartičnih zlorab.

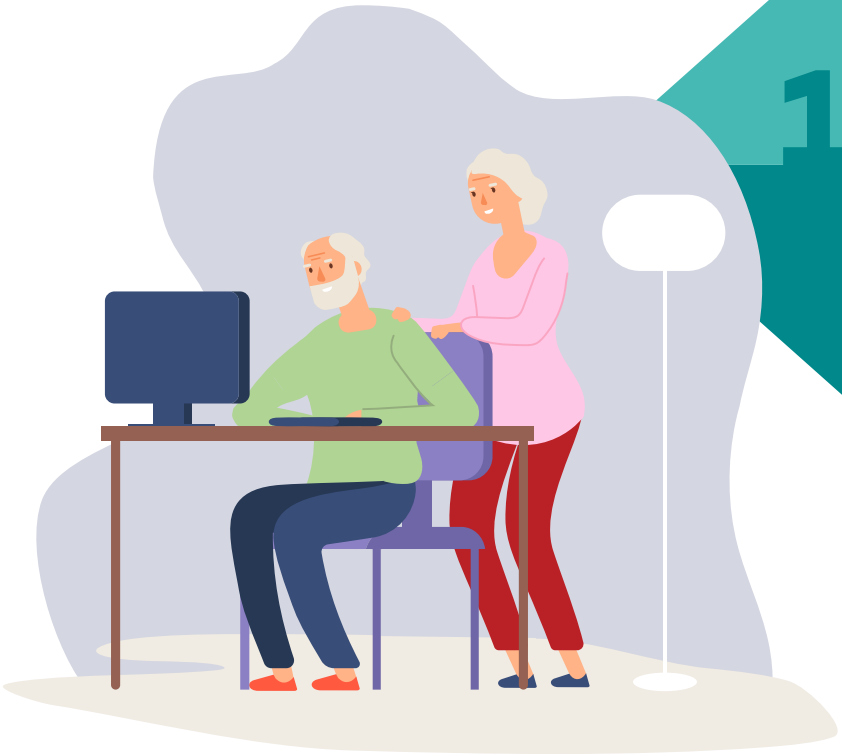
Banka nakazila stranke ne more preprečiti, zato poudarjamo pomen ozaveščanja strank. Vsak je lahko žrtev spletne prevare, zato je pomembno, da se o njih pogovarjamo in širimo zmožnost strank prevaro pravočasno prepoznati. Velikokrat pomaga pogovor, stranki pojasnimo okoliščine, saj gre velikokrat za ljudi, ki o novodobnih prevarah ne vedo veliko. Prisluhnite dobronamernim nasvetom, ki jih dobite v poslovalnici. S takšnim pristopom smo v Novi KBM preprečili že kar nekaj prevar ali pa zaustavili nadaljnje pošiljanje sredstev. Naši bančniki na okencih že zelo dobro ozaveščeni o prevarah, jih hitro prepoznajo in opozorijo stranko še preden opravi nakazilo.

V nadaljevanju vam opisujemo prevare, ki smo jih zaznali v naši banki. Svetujemo vam, kako se zaščitite. Naš cilj je vaše varno spletno poslovanje.

Aleš Ritonja, vodja Oddelka za preprečevanje prevar

1

FINANČNE ZLORABE IN STAROSTNIKI



Za finančno zlorabo pri starostnikih je značilno, da so storilci teh prevar bodisi starostnikovi otroci, vnuki oziroma drugi družinski člani, ki izkoristijo osebni odnos z žrtvijo.

Največkrat gre za neupravičene dvige sredstev z računa, opravljanje transakcij z bančno kartico, tudi odtujitev ostalega premoženja, in sicer brez privolitve in vedenja starostnika. Veliko je primerov prisile k podpisu oporoke ali kreditne pogodbe, ki lahko močno obremeni starostnikovo pokojnino.
Starostnik lahko postane žrtev finančne, čustvene ali psihične zlorabe ter raznih oblik zanemarjanja.

KAKO PREPOZNATI PREVARO?

Tovrstne zlorabe so pogoste, vendar jih je zelo težko prepoznati. Zunanji opazovalec mora biti zelo pozoren in ozaveščen, da prepozna tovrstno prevaro in zazna indice, da je nekaj narobe. Vsekakor pa je alarmanten vsak odstop od ustaljenega poslovanja starejše osebe.

KAJ LAHKO STORITE SAMI?

Če ste skrbnik starostnika ali pa pomagate pri finančnih zadevah vašemu svojcu, vam svetujemo, da si uredite primeren status in vsa potrebna pooblastila za poslovanje s starostnikovim računom oziroma da poslujete preko svoje pooblaščenske kartice.

Naši zaposleni vam bodo v pomoč pri urejanju potrebnih pooblastil, lahko pa pokličete tudi v kontaktni center Nove KBM, kjer vam bomo z veseljem prisluhnili.

SPLETNE PREVARE PRI KREDITIH – NE NASEDITE TUDI VI !

Če vam neznanec preko spleta ponuja kredit pod izredno ugodnimi pogoji in od vas zahteva, da pred izplačilom kredita plačate razne stroške odobritve, zavarovanja ... gre zelo verjetno za prevaro.

V banki obravnavamo veliko prevar, ki so povezane s pridobitvijo (lažnih) kreditov preko spleta. Ponudniki ponujajo izredno ugodne kreditne pogoje, hkrati pa od vas zahtevajo vnaprejšnje plačilo raznih stroškov. Vsakršno sodelovanje s takšnimi ponudniki vam odsvetujemo.

Žrtve goljufov so največkrat kreditojemalci, ki so v finančni stiski in so neuspešno želeli pridobiti kredit v banki.

POSTOPEK PREVARE

Ponudbo za "ugoden" kredit prejmete na vaš elektronski naslov ali preko družbenih omrežij (npr. facebook). Podjetja, ki to storitev ponujajo, so praviloma iz tujine, komunikacija pa poteka v polomljeni slovenščini.

1. Od vas zahtevajo, da jim posredujete svoje osebne podatke, podatke o ročnosti in znesku kredita – enako, kot to zahteva banka ob odobravanju bančnih kreditov.
2. Prevaranti od vas zahtevajo, da plačate določen znesek vnaprej. Znesek, ki je zahtevan kot plačilo vnaprej, prevaranti poimenujejo kot plačilo zavarovanja za kredit, plačilo odobritve kredita, plačilo davka, raznih pristojbin ipd.
3. Zahtevanemu nakazilu naj bi sledilo izplačilo kredita na vaš račun, kar pa se seveda ne zgodi.
4. Ves vaš nakazan denar je izgubljen, ponudnik kredita pa se ne javlja več.

KAKO PREPOZNATI PREVARO?

Svetujemo vam, da ste zelo previdni in ne sklepate takih poslov. Bodite pozorni na:

- zahtevo po vnaprejšnjem plačilu stroškov,
- elektronski naslov ponudnika kredita – običajno je sklenjen pri brezplačnih ponudnikih (@gmail.com, @yahoo.com, @hotmail.com ...),
- način prejema ponudbe (splet, elektronska pošta, facebook ipd.),
- komunikacijo v polomljeni slovenščini.

Če naletite na tako ponudbo, čim prej obvestite policijo.
O možnosti preklica že izvedenega nakazila, mnenje in nasvet smo za vas dosegljivi na **prevare@nkbm.si**.

3

LJUBEZENSKE PREVARE

Če se na spletu pogovarjate z vdovcem, ameriškim vojakom, ki vam bo poslal paket družinskega bogastva in vas prosi za pomoč pri plačilu carine, potem ste zelo verjetno žrtev ljubezenske prevare.

Pri ljubezenski prevari neznana oseba z vami naveže stik – v večini primerov preko družbenih omrežjih ali elektronske pošte. Razvije se zaupanja vreden odnos in oseba od vas kmalu zahteva pomoč v obliki nakazil denarnih sredstev.

POSTOPEK PREVARE

1. Preko družbenih omrežij, elektronske pošte ali drugih spletnih mest se začne z vami pogovarjati neznana oseba, ki si želi prijateljskega ali romantičnega razmerja.
2. V večini primerov se oseba predstavi kot vdovec/vdova, ameriški vojak/vojakinja, zdravnik/zdravnica, novinar/novinarka. Pogosto se osebe zaradi službenih obveznosti nahajajo nekje v tujini (npr. na misiji).
3. Način komunikacije je izredno prijazen, prijateljski in razumevajoč. Zgodba, ki vam jo neznana oseba predstavi, je zelo čustvena, podkrepljena z različnimi fotografijami. Pri vas vzbudijo občutek, da ste v tej osebi našli partnerja ali prijatelja, ki ste ga tako dolgo iskali.
4. Cilj prevarantov je, da vas pripeljejo do točke, ko ste pripravljeni storiti vse, da bi tega partnerja oziroma prijatelja pripeljali v vaše življenje (običajno se nahajajo v oddaljenih krajih, na različnim "misijah", (npr. vojaških, novinarskih, humanitarnih in podobno).
5. Ko vzpostavijo zaupanja vreden odnos, pričnejo z zaprosili za denar, ker so v težavah ali so v težavah njihovi družinski člani.
6. Po prvem nakazilu denarja se zgodbe zapletejo in zahteva po denarju se veča (npr. paket, ki so vam ga poslali, je zadržan na carini in sedaj morate plačati še stroške carine itn.).
7. V kolikor posumite v resničnost zgodbe in denarja več ne nakažete, lahko pričnejo z raznimi grožnjami (da bodo obvestili domače, da ste sodelovali pri pranju denarja in/ali bodo obvestili oblasti). Pomembno je, da se na takšne grožnje ne odzivate!

KAKO PREPOZNATI PREVARO?

- Kontakt vzpostavi oseba, ki je ne poznate in s katero nimate skupnih prijateljev ali poznanstev. Predstavi se s polnim imenom in običajno gre za vdovce/vdove z otroki ali ločenci z otroki.
- Sprašujejo vas o vašem finančnem položaju (koliko imate privarčevanih sredstev, ali ste kreditno sposobni, ali si lahko denar od koga izposodite).
- Izogibajo se video komunikaciji (video klici preko aplikacij). Poslane fotografije si ne sledijo v logičnem zaporedju in/ali so v nasprotju z naravnimi značilnostmi lokacije.
- Ko želijo, da jim nakažete denar, želijo da denar nakažete na drug račun, in sicer osebi, ki so jo v zgodbi predstavili kot zaupanja vredno osebo.
- V večini primerov komunikacija poteka v polomljeni slovenščini, saj prevaranti za prevod v slovenščino uporabljajo na spletu dostopne prevajalnike.

4

BODITE POZORNI, KOMU ZAUPATE SVOJE PODATKE (PHISHING SPOROČILA)

Če prejmete elektronsko sporočilo, v katerem od vas zahtevajo vnos kartičnih podatkov ali drugih gesel, tega ne storite. Podatke boste posredovali neposredno prevarantu.

Bodite izredno pozorni, če od neznanca ali podjetja prejmete elektronsko sporočilo, v katerem od vas zahtevajo vnos osebnih podatkov, podatkov kartice ali raznih gesel. Zelo verjetno je, da gre za **t. i. phishing prevaro.**

POSTOPEK PREVARE

1. Prejmete elektronsko sporočilo, ki je videti kot pristno sporočilo osebe ali znanega podjetja. Pošiljatelj vas nagovarja, da za dodatne informacije ali za povračilo denarja kliknete na povezavo.
2. Pošiljatelj vas poskuša zvabiti na lažno stran banke ali spletne trgovine pod pretvezo, da se morate zaradi preverjanja podatkov ali dodatnih ugodnosti prijaviti in preveriti podatke.
3. Če na tej lažni, t. i. "phishing" strani vpišete številko bančne kartice ali geslo za dostop, **podatke posredujete prevarantu.**

KAKO SE LAHKO IZOGNETE PHISHINGU?

- Če prejmete sumljivo elektronsko ali SMS sporočilo, sporočila ne odpirajte in ga izbrišite.
- Poskrbite, da je na vašem računalniku nameščena protivirusna programska oprema in da je le-ta posodobljena.
- Nikoli ne odgovarjajte na elektronsko pošto, ki od vas zahteva **osebne podatke, podatke vaše kartice, gesla ipd.**
- Ko se prijavite na spletne strani, ki imajo opraviti z vašimi finančnimi podatki, spletni naslov (www....) obvezno vtipkajte neposredno v naslovno vrstico.
- Ne pošiljajte in ne prejemajte osebnih in občutljivih podatkov, kadar ste povezani z javnim Wi-Fi omrežjem, razen če uporabljate varno spletno stran.
- **Pozor!** Prevaranti vam lahko pošljejo sporočilo v imenu znanega podjetja. Na tak način vas poskušajo pretentati, da gre za verodostojno sporočilo.

TRGOVANJE Z VREDNOSTNIMI PAPIRJI IN KRIPTOVALUTAMI

5

Bodite izredno pozorni pri trgovanju z vrednostnimi papirji in kriptovalutami! Posebej, če se s tem srečujete prvič. Tudi svet trgovanja je poln prevarantov, vi pa lahko ostanete brez vloženih sredstev. Žrtve so pogosto oškodovane tudi za več deset tisoč evrov!

Čeprav so novice v povezavi z bajnimi zaslužki malce potihnile, pa žal prevaram v svetu kriptovalut še ni videti konca. Opažamo, da so žrtve goljufov običajno začetniki na tem področju, ki so jih prepričali lažni oglasi.

Torej, **ne verjemite** lažnim oglasom, kjer goljufi zlorabljajo podobe znanih oseb, ki dajejo neresnične izjave. Ti oglasi so zelo pogosti na družbenih omrežjih (npr. facebook), včasih pa se pojavijo tudi med novicami na spletu in prav zato izgledajo še bolj verodostojni.

Vedno gre za obljube o bajnih zaslužkih - goljufi si vzamejo veliko časa in vam po telefonu ali v klepetu natančno obrazložijo potek trgovanja s kriptovalutami. S tem si želijo pridobiti vašo pozornost in zaupanje. Včasih vas lahko preseneti tudi telefonski klic (po navadi iz tujine) – tudi takemu klicu **ne nasedajte.** Svetujemo vam, da se na neznane klice iz tujine ne oglašate in da ste previdni, katere podatke zaupate neznanemu sogovorniku (ne zaupajte svojih osebnih in predvsem bančnih podatkov – npr. številka bančne kartice).

Včasih goljufi ob prvem vplačilu omogočijo prenakazilo nekega manjšega zneska, žrtvam tudi omogočijo vpogled na trgovalni račun in celo prikazujejo naraščanje premoženja. Zgodba je vedno enaka – ko gre za večje zneske, vam dostop in vsa izplačila onemogočijo – tako namesto obljubljenega bajnega zaslužka ostanete brez vsega.

V zadnjem času so žrtve predvsem **starejši in nevešči trgovanja** s kriptovalutami. Če se tudi sami prvič srečujete s tem področjem, preberite, česa v nobenem primeru ne smete storiti pri trgovanju s kriptovalutami:

OPOZORILA ZA ZAČETNIKE V SVETU KRIPTOVALUT

- Nikomur ne zaupajte dostopnih podatkov vašega trgovalnega niti osebnega računa.
- Ne dovolite, da drugi odprejo račun na vaše ime.
- Neznancem ne dovolite oddaljenega dostopa do vašega računalnika.
- Za običajno trgovanje s kriptovalutami morate sami odpreti trgovalni račun na enem od legitimnih portalov.
- Nikoli ne nasedajte oglasom, ki ponujajo ogromne zaslužke.
- Nikoli ne nasedajte oglasom, ki so napisani v polomljeni slovenščini.
- Ne nasedajte ponudbam, ki so časovno omejene.
- Bodite pozorni, kadar vam obljubljajo varne naložbe (brez tveganja), zagotovljene donose in velike zaslužke.
- Bodite pozorni, kadar posredniki nastopajo zelo agresivno (vas pogosto kontaktirajo, pozivajo k hitremu nakupu ipd.).

Tisti, ki redno trgujejo s kriptovalutami, nikoli ne nasedajo oglasom.

6

DENARNE MULE

Ste kdaj prejeli elektronsko sporočilo neznanca, v katerem so vas v zameno za nagrado prosili za pomoč pri prenosu denarja? Bodite pazljivi.

KAJ SO DENARNE MULE?

Denarne mule oziroma prenašalci denarja lahko vede ali nevede postanete tudi vi. Gre za primere, ko vas neznanci oziroma razna podjetja prepričajo, da na svoj račun prejmete nakazilo ukradenega ali nezakonito pridobljenega denarja in ga nato nakažete naprej.

POZOR! Prevaranti vam lahko predstavijo lažno zgodbo in največkrat sploh ne boste vedeli, da gre v resnici za nezakonito pridobljen denar.

POSTOPEK PREVARE

1. Prevaranti vas “uporabijo” ali “najamejo” kot denarno mulo.
2. Komunikacija se začne po elektronski pošti, preko spletnih mest za iskanje zaposlitev ali drugih spletnih oglasov.
3. Prevaranti vas prosijo, da jim pomagate pri prenosu denarja.
4. Prevaranti vam v zameno za prenos denarja ponudijo provizijo oziroma nagrado.

POZOR! Neznancem ne zaupajte svojih osebnih in bančnih podatkov. Če boste neznancu zaupali številko svojega bančnega računa in številko svoje bančne kartice, bo lahko ta preko vašega računa izvajal nezakonite prenose denarja – in vaš račun bo postal t. i. denarna mula. Ker bo prevarant razpolagal sl podatki vašega bančnega računa, bo vedel, kam lahko nezakonito pridobljena sredstva nakaže. S pomočjo aplikacij za prenos denarja in podatkov vaše bančne kartice, bo denar prenakazal v katero koli državo na svetu - ne da bi vi vedeli, da se na vašem računu kaj dogaja.

KAKO PREPOZNATI PREVARO?

- Neznanec od vas zahteva vaše osebne in bančne podatke.
- Nekdo vas prosi za pomoč pri prenosu denarnih sredstev in želi, da se prenos izvede preko vašega računa.
- Neznanec od vas zahteva, da prejeta sredstva nakažete na vam neznan račun.
- V nekaterih primerih neznanec želi nadzor nad vašim računom. Nikoli nikomur ne dajajte vstopnih podatkov do vašega računa.

7

NIGERIJSKA PREVARA

Če vam neznanec sporoča: da ste po daljnem sorodniku iz tujine podedovali hišo na obali ali da vas je neznana oseba naključno izbrala in vam bo podarila svoje premoženje v vrednosti 1.000.000 EUR ali da ste srečni nagrajenec nagradne igre in da boste prejeli nagrado v vrednosti 25.000.000.000 EUR, je sporočilo prelepo, da bi bilo resnično. Ne nasedite, gre za prevaro.

POSTOPEK PREVARE

1. Preko elektronske pošte ali družbenega omrežja prejmete sporočilo. Prevarant vam sporoči izredno dobre novice.
2. Prevarant vas prosi za vaše osebne in bančne podatke, saj vam želi nakazati veliko vsoto denarja (nagrada, dediščina ipd.).
3. Če se odzovete na zahteve prevaranta, vam odgovori, da morate **vnaprej poravnati razne stroške** – po navadi gre za stroške odprtja računa, plačilo zavarovanja, plačilo odvetnika, plačilo davka ipd.
4. Če izvedete prvo nakazilo, se bodo pojavile zahteve po dodatnih nakazilih.
5. Prevaranti bodo resničnost zgodbe poskušali podkrepiti z raznimi dokumenti.
6. Čeprav boste poravnali vse stroške, **obljubljene nagrade/dediščine ne boste prejeli.**

POZOR! Neznancem ne zaupajte svojih osebnih in bančnih podatkov. Če boste neznancu zaupali številko svojega bančnega računa in številko svoje bančne kartice, bo lahko ta preko vašega računa izvajal nezakonite prenose denarja – in vaš račun bo postal t. i. denarna mula. Ker bo prevarant razpolagal sl podatki vašega bančnega računa, bo vedel, kam lahko nezakonito pridobljena sredstva nakaže. S pomočjo aplikacij za prenos denarja in podatkov vaše bančne kartice, bo denar prenakazal v katero koli državo na svetu - ne da bi vi vedeli, da se na vašem računu kaj dogaja.

KAKO PREPOZNATI PREVARO?

- Najočitnejši znak je polomljena slovenščina, zato je besedilo tudi težje razumljivo. Besedilo je prevedeno s strojnim prevajalnikom in je polno slovničnih napak.
- Znak prevare je tudi, da vam nekdo ponuja veliko vsoto denarja oziroma zatrjuje, da ste prejeli nagrado (čeprav v nagradni igri sploh niste sodelovali).
- Pojavi se zahteva po plačilu raznih stroškov vnaprej – torej preden prejmete obljubljeno nagrado/dediščino morate poravnati razne stroške.

DOSTOP NA DALJAVO

Neznancem ne omogočajte oddaljenega dostopa do svojega računalnika.

PREVARA STROKOVNJAKOV ZA TEHNIČNO PODPORO

Pri prevari strokovnjakov za tehnično podporo gre za prevaro, kjer vas pokliče neznanec in se predstavi kot strokovnjak tehnične podpore (npr. podjetja Microsoft). Pove vam, da so na vašem računalniku zaznali določene težave in da jih bodo odpravili. Pogosto od vas zahtevajo oddaljen dostop do vašega računalnika.

POSTOPEK PREVARE

1. Prejmete telefonski klic neznanca. Klicatelj trdi, da kliče iz tehnične podpore določenega podjetja (npr. Microsoft).
2. Klicatelj pojasni, da so na vašem računalniku zaznali določene težave oziroma napake.
3. Klicatelj zahteva, da na računalniku odprete določene programe, ki prikazujejo razne napake, ki pa v resnici ne vplivajo na pravilno delovanje vašega računalnika.
4. Od vas zahtevajo prenos določenega programa, s katerim bi vam pomagali odpraviti težave. Običajno gre za programe, ki tretji osebi omogočijo dostop do vašega računalnika – klicatelju tako omogočite popoln nadzor nad vašim računalnikom.
5. Računalnik vam prikazuje lažne znake okužbe – od vas zahtevajo osebne podatke in podatke o bančni kartici za nakup programske opreme, s katero bi težave odpravili.
6. Če ne želite vpisati svojih osebnih in bančnih podatkov, lahko prevaranti preko oddaljenega dostopa tudi izbrišejo posamezne sistemske datoteke oz. računalnik zablokirajo na tak način, da morate ob ponovnem zagonu vpisati geslo, ki pa ga ne poznate. Če podatke vseeno posredujete, težav ne boste odpravili, ampak vam bodo goljufi pobrali ves razpoložljiv denar na bančni kartici, vaš računalnik pa bo treba popraviti.

POZOR! Klici prihajajo iz tujine, vendar se prevaranti za izvajanje prevare poslužujejo različnih načinov potvarjanja telefonskih številk, ki so lahko videti kot lokalne. Zato vam svetujemo previdnost pri vseh sumljivih klicih tehnične podpore, tudi če ti prihajajo iz lokalnih omrežnih skupin.

NA KAJ BODITE POZORNI?

- Neznancem ne omogočajte oddaljenega dostopa do računalnika.

Zaposleni v tehnični podpori od vas nikoli ne bodo zahtevali podatkov vaše bančne kartice.

LAŽNE SPLETNE TRGOVINE

Pri spletnem nakupovanju si vzemite čas - natančno preverite spletno trgovino in se obvarujete pred kasnejšo finančno škodo. Posebej bodite pozorni na izredno ugodne ponudbe.

POSTOPEK PREVARE

1. Prevarant vzpostavi lažno spletno trgovino oziroma spletno stran, ki je videti resnična.
2. Izdelek kupite in plačate.
3. Naročenega blaga nikoli ne prejmete.

KAKO PREPOZNATI PREVARO?

- Izdelki priznanih blagovnih znamk so na voljo po izjemno nizkih cenah.
- Dostava je brezplačna po vsem svetu.
- Vsi artikli so na zalogi.
- Ne najdete nobenih podatkov o podjetju, ki stoji za trgovino.

KAJ LAHKO STORIM?

Pred nakupom 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.