

GOLJUFIJA S KOMPROMITIRANIM RAČUNOM DIREKTORJA/PODJETJA

Do takih prevar pride, ko goljuf zaposlenega, pooblaščenega za izvajanje plačil, z zvijačo zavede, da plača lažni račun ali izvede nepooblaščno nakazilo s poslovnega bančnega računa.

KAKO DELUJE?

Slepar, ki se predstavlja kot eden vodilnih v podjetju (npr. generalni ali finančni direktor), pokliče ali pošlje e-poštno sporočilo.

Organizacijo dobro pozna.

Zahteva nujno plačilo.

Uporablja izraze, kot so: »zaupnost« »podjetje vam zaupa«, »trenutno nisem na voljo«.

Sklicuje se na občutljive okoliščine (npr. davčni pregled, združitev ali pripojitev podjetja).

Pogosto so zahteve za mednarodna plačila bankam zunaj Evrope.

Zaposleni nakaže sredstva na račun, ki je pod nadzorom sleparja.

Navodila, kako ravnati, bodo morda pozneje posredovala druga oseba ali bodo poslana po e-pošti.

Od zaposlenega zahteva, da ne uporabi ustaljenih postopkov za pridobivanje dovoljenj.

KATERI SO PREPOZNAVNI ZNAKI?

- Nezahtevana e-poštna sporočila/telefonski klici.
- Višji nadrejeni, s katerim običajno niste v stiku, se obrne neposredno na vas.
- Zahteva za absolutno zaupnost.
- Pritisk in občutek nujnosti.
- Nenavadna zahteva, ki je v nasprotju z običajnimi notranjimi postopki.
- Grožnje ali nenavadno laskanje/obljube nagrad.

KAJ LAHKO STORITE?

KOT PODJETJE

Zavedajte se tveganj in poskrbite, da bodo tudi zaposleni seznanjeni s to vrsto goljufije in jo poznali.

Zaposlene spodbujajte, da so previdni glede zahtev za plačila.

Uvedite notranje protokole glede plačil.

Uvedite postopek za preverjanje verodostojnosti zahtev za plačila, prejeta po e-pošti.

Vzpostavite postopke poročanja za ukrepanje v primeru goljufij.

Preglejte informacije, objavljene na spletnem mestu podjetja, jih omejite in bodite previdni pri uporabi družbenih omrežij.

Nadgradite in posodobite tehnično varnost.



V primerih goljufij se vedno obrnite na policijo, tudi če niste bili žrtev.

KOT ZAPOSLENI

Strogo izvajajte uveljavljene varnostne postopke za plačila in nabavo. **Ne preskočite nobenega koraka in se ne vdajte pritiskom.**

Pri ravnanju z občutljivimi informacijami/nakazili denarja vedno **skrbno preverite e-poštne naslove.**

Če imate kakršen koli dvom glede naloga za nakazilo, **se obrnite na sodelavca, ki se dobro spozna na to.**

Nikoli ne odpirajte sumljivih povezav ali prilog, prejetih po e-pošti. Bodite zlasti previdni pri odpiranju zasebne e-pošte v službenih računalnikih.

Omejite informacije in bodite previdni pri uporabi družbenih omrežij.

Izogibajte se razkrivanju informacij o hierarhiji podjetja ter varnostnih in drugih postopkih.



Če prejmete sumljivo e-poštno sporočilo ali klic, vedno obvestite oddelek za IT.

NALOŽBENE PREVARE

Pogoste gre pri naložbenih prevarah za na videz dobičkonosne naložbene priložnosti, kot so delnice, obveznice, kriptovalute, žlahtne kovine, nepremičninske naložbe v tujini ali alternativni viri energije.

KATERI SO PREPOZNAVNI ZNAKI?

- Obljublajo vam hiter donos in zagotovljeno varnost naložbe.
- Ponudba je na voljo samo za omejen čas.

- Stalno prejimate nezahtevane klice.



- Ponudba je na voljo samo vam in od vas se zahteva, da je ne razkrijete drugim.

KAJ LAHKO STORITE?

- Vedno poiščite objektivni finančni nasvet, preden izročite denar ali se podate v naložbo.
- Zavrnite nezahtevane klice, povezane z naložbenimi priložnostmi.
- Bodite sumničavi do ponudb, ki obljublajo varne naložbe, zagotovljen donos ali velike dobičke.
- Na prevare bodite pozorni tudi vnaprej. Če ste že vložili sredstva v goljufijo, je verjetno, da vas bodo sleparji znova ciljali ali vaše podatke prodali drugim kriminalcem.
- Obrnite se na policijo, če kar koli sumite.

PONEVERBA RAČUNOV

- Na podjetje se obrne nekdo, ki trdi, da zastopa dobavitelja/ponudnika storitev/upnika.
- Uporabi lahko kombinacijo pristopov: telefon, pismo, e-pošta ipd.
- Slepjar zahteva, da se bančne podrobnosti za plačila (torej podrobnosti o bančnem računu prejemnika plačila) prihodnjih računov spremenijo. Predlagani novi račun je pod nadzorom sleparja.



KAJ LAHKO STORITE?

Poskrbite, da bodo **zaposleni seznanjeni s to vrsto goljufije in jo poznali** ter bodo vedeli, kako se ji izogniti.

Uvedite **postopek za preverjanje** verodostojnosti zahtev za plačila.

Preverite vse zahteve, ki naj bi bile od vaših upnikov, zlasti če zahtevajo spremembo svojih bančnih podatkov za prihodnje račune.

Ne uporabite podatkov za stik v pismu/faksu/e-poštnem sporočilu z zahtevo za spremembo. Namesto tega uporabite podatke iz **prejšnje korespondence**.

Določite **imenovano enotno točko za stik** s podjetji, katerim redno izvajate plačila.

KOT PODJETJE



Osebj, ki je odgovorno za plačevanje računov, dajte navodila, da **vedno preveri**, ali je v njih kaj nenavadnega.

Preglejte informacije, objavljene na spletnem mestu podjetja, zlasti pogodbe in dobavitelje. Poskrbite, da bodo zaposleni omejili, kaj v družbenih omrežjih razkrivajo o podjetju.

Za plačila nad določenim zneskom **določite postopek za potrditev** pravilnega bančnega računa in prejemnika (npr. sestanek s podjetjem).

Ko je račun plačan, **pošljite prejemniku e-poštno obvestilo o tem**. Navedite ime banke prejemnika in zadnje štiri številke številke posameznega računa, določenega za to, da zagotovite varnost.

KOT ZAPOSLENI



Omejite informacije, ki jih v družbenih omrežjih razkrivate o svojih zaposlenih.



V primerih goljufij se vedno obrnite na policijo, tudi če niste bili žrtev.

PREVARE PRI SPLETNEM NAKUPOVANJU

Spletne ponudbe so pogosto dober nakup, vendar pazite na prevare.



Posebna ponudba
PONUDBA ZA VEČERJO

70%

KAJ LAHKO STORITE?

- Uporabljajte domače spletne trgovine, če je le mogoče – najverjetneje boste lažje rešili morebitne težave.
- Izdelek, ki ga kupujete, temeljito preučite – pred nakupom preberite mnenja.
- Uporabljajte kreditne kartice – tako imate več možnosti za povračilo denarja.
- Plačujte samo z uporabo varnih plačilnih storitev – ali prodajalec zahteva plačilo z nakazilom ali storitvijo za prenos denarja? Razmislite še enkrat!
- Plačujte samo, če imate vzpostavljeno varno internetno povezavo – ne uporabljajte brezplačnega ali javnega omrežja Wi-Fi.
- Plačujte samo z varno napravo – poskrbite, da bosta vaš operacijski sistem in varnostna programska oprema posodobljena.
- Bodite pazljivi pri oglasih, ki ponujajo neverjetne ponudbe ali čudežne izdelke – če je slišati preveč dobro, da bi lahko bilo resnično, verjetno tudi je!
- Ali se odpira pojavno okno z obvestilom, da ste prejeli nagrado? Premislite dvakrat. Morda boste zadeli samo zlonamerno programsko opremo.
- Če izdelka ne dobite, se obrnite na prodajalca. Če ni odgovora, se obrnite na banko.



Vsak sum goljufije vedno prijavite policiji, tudi če niste bili žrtev.

E-POŠTNA SPOROČILA Z LAŽNIM PREDSTAVLJANJEM BANK

Pojem »lažno predstavljanje« se nanaša na sleparska e-poštna sporočila, ki prejemnike poskušajo pretentati, da razkrijejo svoje osebne, finančne ali varnostne podatke.

KAKO DELUJE?

Ta e-poštna sporočila:

so lahko **videti** enaka korespondenci, ki jo pošiljajo prave banke;

posnemajo logotipe, postavitev in slog pravih e-poštnih sporočil;

zahtevajo, da prenesete priloženi dokument ali kliknete povezavo;

uporabljajo način naslavljanja, ki ustvarja pritisk in občutek nujnosti.

KAJ LAHKO STORITE?

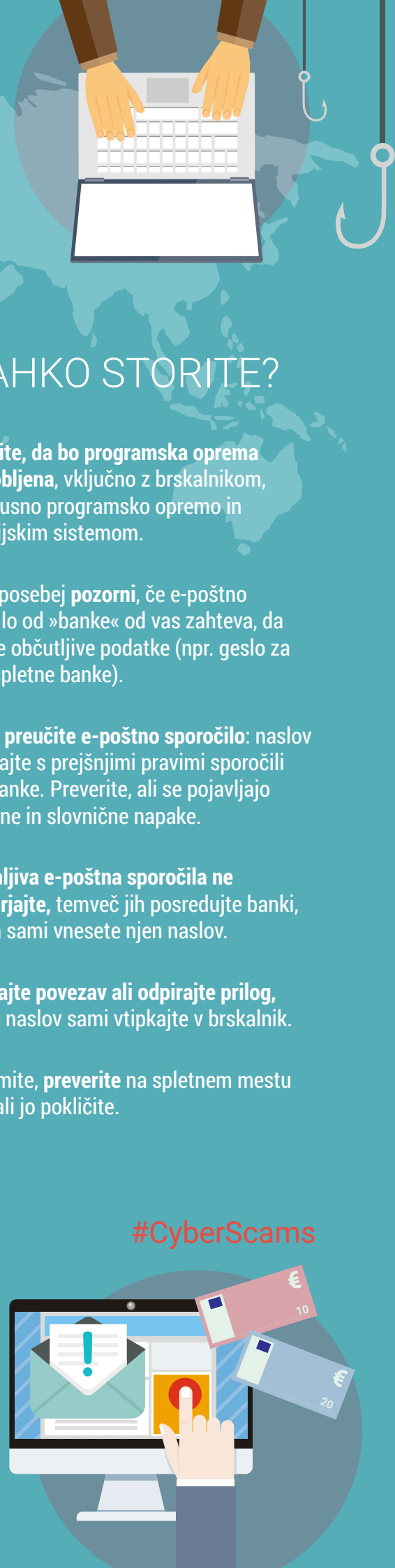
- > Poskrbite, da bo programska oprema **posodobljena**, vključno z brskalnikom, protivirusno programsko opremo in operacijskim sistemom.
- > Bodite posebej **pozorni**, če e-poštno sporočilo od »banke« od vas zahteva, da pošljete občutljive podatke (npr. geslo za račun spletne banke).
- > **Skrbno preučite e-poštno sporočilo**: naslov primerjajte s prejšnjimi pravih sporočili svoje banke. Preverite, ali se pojavljajo črkovalne in slovnične napake.
- > Na sumljiva e-poštna sporočila **ne odgovarjajte**, temveč jih posredujte banki, tako da sami vnesete njen naslov.
- > **Ne klikajte povezav ali odpirajte prilog**, temveč naslov sami vtipkajte v brskalniki.
- > Če dvomite, **preverite** na spletnem mestu banke ali jo pokličite.



Spletni kriminalci se zanašajo na dejstvo, da so ljudje zaposleni in da so tovrstna sporočila na prvi pogled videti verodostojna.



Bodite previdni pri uporabi mobilne naprave. Poskus lažnega predstavljanja bo morda težje prepoznati v telefonu ali tabličnem računalniku.



#CyberScams

LJUBEZENSKA PREVARA

Sleparji ciljajo žrtve na spletnih mestih za zmenke, lahko pa za vzpostavljjanje stika uporabijo tudi družbena omrežja ali e-pošto.



KATERI SO PREPOZNAVNI ZNAKI?



KAJ LAHKO STORITE?

- **Bodite zelo previdni** glede tega, koliko osebnih podatkov razkrijete v družbenih omrežjih in spletnih mestih za zmenke.
- **Vedno upoštevajte tveganja.** Goljufi so prisotni tudi na najuglednejših spletnih mestih.
- **Ne hitite** in postavljajte vprašanja.
- **Preučite** fotografijo in profil osebe ter preverite, ali sta bila že uporabljena drugje.
- **Bodite pozorni** na črkovalne ali slovnične napake ter nedoslednosti v tem, kar vam pove, in opravičila, kot je to, da ne dela kamera.
- **Ne razrivajte** ničesar, kar bi vas lahko spravilo na slab glas in bi lahko bilo uporabljeno za izsiljevanje.
- Če se dogovorite za osebno srečanje, **družinskim članom in prijateljem povejte**, kam greste.
- **Pazite se zahtev za denar.** Nikoli ne pošiljajte denarja in ne razkrivajte podrobnosti kreditnih kartic, spletnih računov ali kopij osebnih dokumentov.
- Ne pošiljajte vnaprejšnjih plačil.
- **Ne nakazujte denarja** za koga drugega: pranje denarja je kaznivo dejanje.

ALI STE ŽRTEV?

Naj vas ne bo sram.

Takoj prekinite vsakršen stik.

Če je mogoče, shranite vso korespondenco, kot so klepetna sporočila.

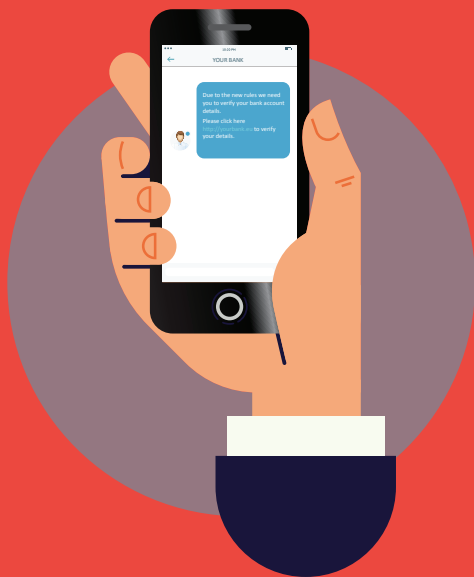
Prijavite policiji.

Prijavite spletnemu mestu, na katerem ste imeli prvi stik s prevarantom.

Če ste razkrili podatke o računu, se obrnite na banko.

SMS-JI Z LAŽNIM PREDSTAVLJANJEM BANK

Pošiljanje SMS-jev z lažnim predstavljanjem (angl. »smishing«) je način, s katerim poskušajo sleparji prek sporočila SMS pridobiti osebne, finančne ali varnostne podatke.



KAKO DELUJE?

V sporočilu SMS bo običajno zahteva, da kliknete povezavo ali pokličete telefonsko številko, da »potrdite«, »posodobite« ali »znova aktivirate« svoj račun. Vendar pa povezava vodi na lažno spletno mesto, telefonska številka pa je od sleparja, ki se predstavlja kot verodostojno podjetje.

KAJ LAHKO STORITE?

- **Ne klikajte povezav, prilog ali slik**, ki jih prejmete v nezahtevanih sporočilih SMS, ne da bi prej preverili pošiljatelja.
- **Ne hitite.** Vzemite si čas in preverite vse potrebno, preden se odzovete.
- **Nikoli ne odgovarjajte na sporočilo SMS**, ki zahteva vaš PIN, geslo za spletno banko ali kakršne koli druge varnostne poverilnice.
- Če menite, da ste morda odgovorili na lažno predstavljanje prek sporočila SMS in razkrili svoje bančne podrobnosti, **se takoj obrnite na svojo banko.**

LAŽNA SPLETNA MESTA BANK

E-poštna sporočila z lažnim predstavljanjem banke običajno vsebujejo povezave, ki vas usmerijo na lažno spletno mesto banke, na katerem morate razkriti finančne in osebne podatke.



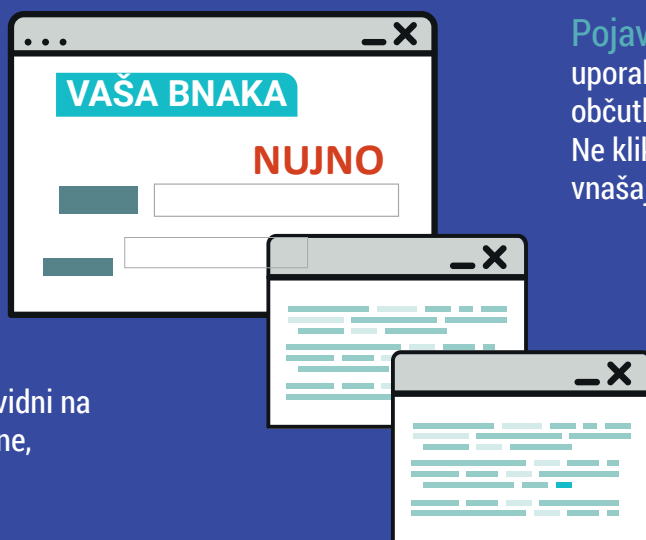
KATERI SO PREPOZNAVNI ZNAKI?

Lažna spletna mesta bank so videti skoraj tako kot prava. Taka spletna mesta pogosto uporabljajo pojavno okno s pozivom, da vnesete bančne poverilnice. Prave banke ne uporabljajo takih oken.

Za ta spletna so značilne te lastnosti:

Nujnost: takih sporočil na pravih spletnih mest bank ni.

Slabo oblikovanje: bodite previdni na spletnih mestih, ki imajo oblikovne, črkovalne ali slovnične napake.



Pojavna okna: ta se pogosto uporabljajo za zbiranje občutljivih podatkov od vas. Ne klikajte jih in vanje ne vnašajte osebnih podatkov.

KAJ LAHKO STORITE?



Nikoli ne klikajte povezav v e-poštnih sporočilih, ki vodijo do spletnega mesta vaše banke.



Povezavo vedno ročno vnesite ali uporabite obstoječo povezavo na svojem seznamu priljubljenih spletnih mest.



Uporabljajte brskalnik, ki omogoča blokiranje pojavnih oken.



Če gre za kaj res nujnega, vas bo banka o tem obvestila, ko se prijavite v svoj spletni račun.

KLICI BANK Z GLASOVNIM LAŽNIM PREDSTAVLJANJEM

Glasovno lažno predstavljanje (angl. »vishing«) je telefonska prevara, s katero poskušajo sleparji žrtve pripraviti do tega, da jim razkrijejo osebne, finančne ali varnostne podatke ali nakažejo denar.

KAJ LAHKO STORITE?

- **Bodite pozorni** na nezahtevane telefonske klice.
- **Zabeležite si število kličočega** in mu povejte, da ga boste poklicali nazaj.
- **Potrdite njegovo identiteto** tako, da **poiščete telefonsko številko organizacije** in se obrnete neposredno nanjo.
- **Kličočega ne preverjajte s telefonsko številko, ki vam jo je dal** (to je lahko izmišljena ali lažna telefonska številka).
- **Sleparji lahko osnovne podatke o vas poiščejo v spletu** (npr. prek družbenih omrežij). **Ne sklepajte, da je kličoči verodostojen**, samo zato, ker ima vse te podrobnosti.
- **Ne razkrivajte številke PIN kreditne ali debetne kartice ali gesla za spletno banko.** Banka od vas nikdar ne bo zahtevala takih podrobnosti.
- **Ne nakazujte denarja na drug račun na njegovo zahtevo.** Banka tega od vas ne bo nikdar zahtevala.
- Če menite, da gre za lažni klic, **obvestite svojo banko.**



BANK ACCOUNT HACKING

