"DIREKTORSKA" PRIJEVARA

"Direktorska" prijevara događa se kada je zaposlenik koji je ovlašten za provođenje plaćanja prevaren na način da plati lažni račun ili provede neovlašteni prijenos s računa tvrtke.

KAKO SE TO RADI?

Prevarant zove ili šalje poruke predstavljajući se kao direktor ili član uprave tvrtke.

Dobro poznaju organizaciju tvrtke.

Traže hitno provođenje plaćanja.

Koriste fraze kao "povjerljivost", "tvrtka ima povjerenje u vas", "trenutno sam nedostupan".

Kažu da se radi o osjetljivoj situaciji (npr. porezna kontrola, preuzimanje i spajanje poduzeća).

Od zaposlenika se traži da ne slijedi redovne autorizacijske postupke.

Upute o tome kako postupiti mogu se dati kasnije, putem treće osobe ili e-pošte.

Zaposlenik prenosi sredstva na račun koji kontrolira prevarant.

Često se zahtjev odnosi na međunarodna plaćanja bankama izvan Europe.

KAKO PREPOZNATI ZNAKOVE?

- Neočekivani poziv/poruka
- Izravni kontakt od visokog dužnosnika u tvrtki s kojim obično niste u kontaktu
- Zahtijeva se apsolutna povjerljivost
- Pritisak i uvjeravanje u hitnost
- Neuobičajen zahtjev u suprotnosti s internim postupcima
- Prijetnje, neobična laskanja ili obećanja nagrade

ŠTO MOŽETE UČINITI?

KAO TVRTKA

Budite svjesni rizika i pobrinite se da **zaposlenici budu informirani i upoznati**.

Potaknite zaposlenike da budu **oprezni sa svim zahtjevima za plaćanje.**

Provoditi interne protokole vezane uz plaćanja.

Propisati postupak provjere legitimnosti zahtjeva za plaćanjem primljenih putem e-pošte.

Uspostaviti **pravila za izvještaje** o prijevarama.

Pregledajte informacije objavljene na stranicama svoje tvrtke, **ograničite informacije i pripazite** na društvene medije.

Nadogradite i ažurirajte tehničku sigurnost.

Uvijek se obratite policiji u slučaju pokušaja prijevare, čak i ako niste postali žrtvom.

KAO ZAPOSLENIK

Strogo poštujte sigurnosne postupke za plaćanja i nabave. **Ne preskačite niti jedan korak i ne popuštajte pritisku**.

Uvijek **pažljivo provjeravajte adrese e-pošte** kada se radi o osjetljivim informacijama ili prijenosu sredstava.

U slučaju sumnje o nalogu za prijenos, **obratite se nadležnom kolegi**.

Nikad ne otvarajte sumnjive poveznice ili privitke primljene putem e-pošte. Budite posebno oprezni kada čitate svoju privatnu e-poštu na računalima tvrtke.

Ograničite informacije i budite oprezni s obzirom na društvene medije.

Izbjegavajte dijeljenje informacija o internoj organizaciji tvrtke, sigurnosti i procedurama.

Ako primite sumnjivu e-poštu ili poziv, uvijek obavijestite IT odjel.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIJA MUP RH

HRVATSKA UDRUGA BANAKA GIU

#CyberScams

INVESTICIJSKE PRIJEVARE

Najčešće investicijske prijevare uključuju ponude za unosne investicijske mogućnosti kao što su dionice, obveznice, kriptovalute, plemeniti metali, strana zemljišta ili alternativna energija.

KAKO PREPOZNATI ZNAKOVE?

- Obećavaju vam brzu značajnu dobit i uvjeravaju u sigurnost investicije.
- Ponuda je dostupna samo na ograničeno vrijeme.
- Dobivate učestale nenajavljene pozive.
- Ponuda je dostupna samo vama i traže da je ne dijelite s drugima.

ŠTO MOŽETE UČINITI?

- **Uvijek tražite nepristrani financijski savjet** prije nego što date novac ili uložite sredstva.
- **Odbijte nenajavljene pozive** o mogućnostima ulaganja.
- **Budite sumnjičavi** prema ponudama koje obećavaju sigurnu investiciju, zajamčene povrate i veliku dobit.
- **Čuvajte se budućih prijevara.** Ako ste jednom uložili u prijevaru, prevaranti će vas vjerojatno ponovno ciljati ili prodati vaše podatke drugim prevarantima.
- **Obratite se policiji** ako vam je nešto sumnjivo.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIJA MUP

HRVATSKA UDRUGA BANAKA GIU

#CyberScams

PRIJEVARA S RAČUNIMA

KAKO SE TO RADI?

- Tvrtki pristupa netko tko se pretvara da predstavlja dobavljača / davatelja usluga / vjerovnika.
- Može se koristiti kombinacija pristupa: telefon, pismo, e-pošta itd.
- Prevaranti traže da se bankovni podaci o plaćanju (odnosno pojedinosti o bankovnom računu primatelja) budućih računa promijene. Novi navedeni račun kontrolira prevarant.

ŠTO MOŽETE UČINITI?

KAO TVRTKA

Pobrinite se da su **zaposlenici obaviješteni i svjesni** ove vrste prijevare i upućeni u to kako ih izbjeći.

Uputiti osoblje odgovorno za plaćanje računa da ih **uvijek provjeravaju zbog mogućih nepravilnosti**.

Uvesti **postupak za provjeru** legitimiteta zahtjeva za plaćanjem.

Pregledajte informacije objavljene na stranici tvrtke, posebno ugovore i dobavljače. Pobrinite se da vaši zaposlenici paze na ono što dijele o tvrtki na svojim društvenim mrežama.

KAO ZAPOSLENIK

Provjerite sve zahtjeve koji se čine da dolaze od vaših vjerovnika, posebno ako zatraže promjenu bankovnih podataka za buduća plaćanja.

Za isplate iznad određenog praga **uspostavite postupak potvrde** ispravnosti bankovnog računa i primatelja (npr. sastanak s tvrtkom).

Nemojte koristiti detalje kontakta dobivene pismom/faksom/e-poštom koji traže izmjenu. Sigurnije je koristiti one iz **prethodne korespondencije.**

Kada je račun plaćen, **pošaljite e-poruku kako biste obavijestili primatelja**. Navedite naziv banke i posljednje četiri znamenke računa na koji ste uplatili kao mjeru sigurnosti.

Odredite osobe koje će biti jedinstvene kontaktne točke za rad s tvrtkama kojima redovito plaćate.

Ograničite informacije koje dijelite o svom poslodavcu na društvenim medijima.

Uvijek se obratite policiji u slučaju pokušaja prijevare, čak i ako niste postali žrtvom.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIJA MUP

HRVATSKA UDRUGA BANAKA GIU

#CyberScams

PRIJEVARE KOD KUPOVINE ONLINE

Online ponude su često povoljne, ali čuvajte se prijevare.

ŠTO MOŽETE UČINITI?

- **Koristite lokalne online trgovine kada je moguće** - vjerojatnije je da možete riješiti moguće probleme.
- **Potrudite se i istražite** - provjerite recenzije prije kupnje.
- **Koristite kartice** - imate više šanse za povrat novca.

- **Plaćajte samo preko sigurnog pružatelja usluge plaćanja** - traže li uslugu prijenosa sredstava preko banke ili alternativno? Dobro razmislite!
- Plaćajte samo kada ste spojeni na **sigurnu internetsku vezu** - izbjegavajte besplatni ili otvoreni javni WiFi.
- **Plaćajte samo na sigurnom uređaju** - ažurirajte redovno operativni sustav i sigurnosni softver.
- Čuvajte se oglasa koji nude nevjerojatne ponude ili čudotvorne proizvode - **ako se nešto čini predobro da bude istinito, nije istinito!**
- Iskoči vam oglas i kaže da ste osvojili nagradu? **Dobro razmislite**, možda osvojite zlonamjerni softver.
- Ako proizvod ne stigne, kontaktirajte prodavača. Ako ne odgovara, **obratite se svojoj banci**.

Uvijek prijavite svaku sumnju na pokušaj prijevare policiji, čak i ako niste postali žrtvom.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIJA MUP RH

HRVATSKA UDRUGA BANAKA GIU

#CyberScams

"PHISHING" - MREŽNA KRAĐA IDENTITETA

Krađa identiteta se odnosi na lažne poruke e-pošte koje prevare primatelja i navedu ga na dijeljenje osobnih, financijskih ili sigurnosnih podataka.

KAKO SE TO RADI?

Ovakve e-poruke:

mogu izgledati identično onom tipu korespondencije koju banke doista šalju.

repliciraju logotipe, izgled i ton stvarnih e-poruka.

traže da preuzmete priloženi dokument ili kliknete na poveznicu.

koriste izraze koji ostavljaju dojam hitnosti.

ŠTO MOŽETE UČINITI?

- **Redovito ažurirajte softver**, uključujući vaš preglednik, antivirusni i operativni sustav.
- Budite posebno **oprezni** ako se u poruci e-pošte od "banke" od vas traže osjetljivi podaci (npr. zaporku za online račun).
- **Pomno pogledajte e-poštu**: usporedite adresu s prethodnim stvarnim porukama iz vaše banke. Provjerite točnost pravopisa i gramatike.
- **Nemojte odgovarati na sumnjivu e-poruku**, nego je proslijedite svojoj banci tako da sami upišete adresu.
- **Nemojte kliknuti poveznicu ili preuzeti privitak**, nego upišite adresu u preglednik.
- Ako ste u nedoumici, **provjerite** na stranici banke ili nazovite banku.

Počinitelji računalnih kaznenih djela oslanjaju se na činjenicu da su ljudi zauzeti; na prvi pogled, takva lažna e-poruka može se činiti legitimnom.

#CyberScams

Pazite kada koristite mobilni uređaj. Na mobitelu ili tabletu može biti teže razaznati pokušaj krađe identiteta.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIJA MUP

HRVATSKA UDRUGA BANAKA GIU

ROMANTIČNA PRIJEVARA

Prevaranti ciljaju žrtve na stranicama za upoznavanje, no koriste i društvene medije ili e-poštu da uspostave kontakt.

KOJI SU ZNAKOVI?

Netko koga ste nedavno upoznali online iskazuje snažne osjećaje za vas, tražeći privatni razgovor.

Njihove poruke su često loše napisane i nejasne.

VOLJIM TI

Njihov online profil nije u skladu s onim što vam kažu.

Mogu vas tražiti da pošaljete intimne slike ili videozapise o sebi.

€€€

Prvo zadobiju vaše povjerenje. Zatim traže novac, darove ili podatke o bankovnom računu / kreditnoj kartici.

Ako ne pošaljete novac, mogu vas pokušati ucjenjivati. Ako ga pošaljete, tražit će još više.

ŠTO MOŽETE NAPRAVITI?

- **Budite vrlo oprezni** koliko osobnih podataka dijelite na društvenim mrežama i stranicama za upoznavanje.
- **Uvijek budite svjesni rizika.** Preveranti rade i na najrespektabilnijim stranicama.
- **Idite polako** i postavljajte pitanja.
- **Provjerite** fotografiju i profil osobe da vidite jesu li upotrijebljeni negdje drugdje.
- **Pazite** na pravopisne i gramatičke pogreške, nedosljednosti u njihovim pričama i izgovorima da njihova kamera ne radi.
- **Ne dijelite** nikakav kompromitirajućimaterijal koji bi mogao poslužiti za ucjenjivanje.
- Ako se dogovorite za osobni susret, **recite obitelji i prijateljima** kamo idete.
- **Čuvajte se zahtjeva za novcem.** Nikada ne šaljite novac ili podatke o kartici, online računu ili kopije osobnih dokumenata.
- **Izbjegavajte bilo kakva plaćanja unaprijed.**
- **Nemojte slati novac** za nekoga drugoga: pranje novca je kazneno djelo.

POSTALI STE ŽRTVA?

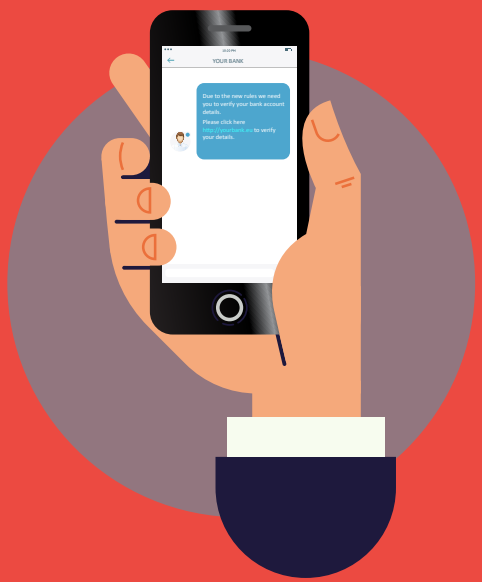
Nemojte se osjećati neugodno!
Odmah prestanite s kontaktom.
Ako možetee, sačuvajte svu komunikaciju, poput chat poruka.
Prijavite sve policiji.
Prijavite web stranici na kojoj je prevarant prvi put došao do vas.
Ako ste dali podatke o svom računu, obratite se banci.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIJA MUP RH | HRVATSKA UDRUGA GIU BANAKA

#CyberScams

KRAĐA IDENTITETA SMS-OM

Smishing (kombinacija riječi SMS i Phishing - krađe identiteta) pokušaj je prevaranata da dođu do osobnih, financijskih ili sigurnosnih podataka putem tekstualne poruke.



KAKO SE TO RADI?

U SMS poruci obično se traži da kliknete poveznicu ili nazovete telefonski broj kako biste "potvrdili", "ažurirali" ili "ponovno aktivirali" svoj račun. Ali ... veza vodi do lažne web stranice, a telefonski broj do prevaranta koji se pretvara da je legitimna tvrtka.

ŠTO MOŽETE UČINITI?

- **Nemojte kliknuti poveznice, privitke ili slike** koje ste primili u SMS porukama s nepoznatog broja bez prethodne provjere pošiljatelja.
- **Ne dajte se požurivati.** Bez žurbe napravite odgovarajuće provjere prije nego što odgovorite.
- **Nikad ne odgovarajte na SMS poruku** koja zahtijeva vaš PIN ili vašu lozinku za online bankarstvo ili bilo koje druge sigurnosne vjerodajnice.
- Ako smatrate da ste nasjeli na smishing poruku i ako ste dali bankovne podatke, **odmah se obratite svojoj banci**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

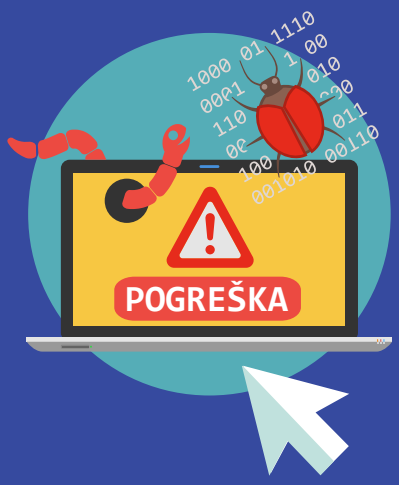
POLICIJA MUP RH

HRVATSKA UDRUGA BANAKA GIU

#CyberScams

LAŽNE STRANICE BANAKA

E-pošta koja naizgled dolazi od banke obično sadrži poveznice koje vode na lažnu stranicu banke, gdje će tražiti da otkrijete svoje financijske i osobne podatke.

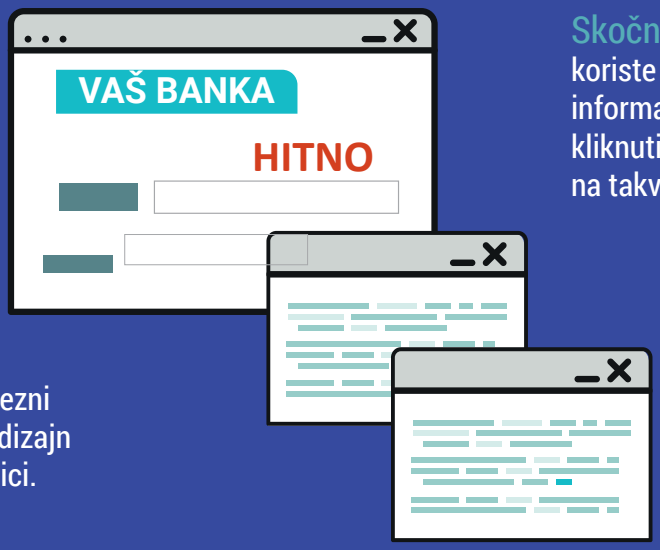


KAKO PREPOZNATI ZNAKOVE?

Lažne stranice banaka izgledaju gotovo identično njihovim pravim stranicama. Na takvim stranicama često će iskočiti prozor koji traži da unesete bankovne vjerodajnice. Stvarne banke ne koriste takve prozore.

Ovakve stranice često prikazuju:

Hitnost: takve poruke nećete pronaći na pravim stranicama banke.



Skočni prozori: obično se koriste za prikupljanje osjetljivih informacija od vas. Nemojte kliknuti i unijeti osobne podatke na takve prozore.

Loš dizajn: budite posebno oprezni sa stranicama koje imaju čudan dizajn ili pogreške u pravopisu i gramatici.

ŠTO MOŽETE UČINITI?

Nikada nemojte kliknuti na poveznice u porukama u kojima se tvrdi da vode do stranice vaše banke.

Uvijek upišite vezu ručno ili koristite postojeću vezu s popisa "favorita".

Koristite preglednik koji omogućuje **blokiranje skočnih prozora**.

Ako vam treba skrenuti pozornost na nešto važno, banka će vas na to upozoriti **kada pristupite svom online računu**.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIJA MUP | HRVATSKA UDRUGA BANAKA GIU

#CyberScams

KRAĐA IDENTITETA POZIVOM

Vishing (kombinacija riječi Voice i Phishing) je telefonska prijevara u kojoj prevaranti pokušavaju navesti žrtvu da otkrije svoje osobne, financijske ili sigurnosne podatke ili da im uplate novčana sredstva.

ŠTO MOŽETE UČINITI?

- **Budite oprezni** kad primite neočekivani telefonski poziv.
- **Uzmite broj pozivatelja** i recite da ćete ih nazvati.
- Da biste potvrdili njihov identitet, **potražite telefonski broj organizacije** i izravno ih kontaktirajte.
- **Nemojte provjeriti pozivatelja koristeći telefonski broj koji su oni naveli** (može biti lažan ili krivotvoren).
- Prevaranti mogu pronaći vaše osnovne podatke online (npr. društvene mreže). **Nemojte pretpostaviti da je pozivatelj legitiman** samo zato što ima takve pojedinosti.
- **Nemojte dijeliti** kartični PIN ili lozinku za online bankarstvo. Vaša banka to nikada neće tražiti.
- **Ne šaljite novac** na neki račun na njihov zahtjev. Vaša banka nikada neće tražiti da to učinite.
- Ako mislite da se radi o lažnom pozivu, **prijavite svojoj banci**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIJA MUP RH

HRVATSKA UDRUGA GIU BANAKA

#CyberScams