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 nepooblaščeno 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).

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

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

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

Pogosto so zahteve za mednarodna plačila bankam zunaj Evrope.

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.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIJA | si-cert Nacionalni odzivni center za kibernetsko varnost

#CyberScams