DIREKTORSKA PREVARA

Direktorska prevara se zgodi, ko prevaranti uslužbenca, pooblaščenega za plačila, prevarajo tako, da plača ponarejen račun ali izvede nepooblaščen prenos iz poslovnega računa.

KAKO POTEKA?

Prevarant pokliče ali pošlje e-pošto in se predstavlja kot izvršni ali finančni direktor podjetja.

Dobro poznajo organizacijo.

Zahtevajo urgentno plačilo.

Uporabljajo izraze kot: »Zaupno«, »Podjetje vam zaupa«, »Trenutno sem nedosegljiv«.

Največkrat je zahtevano plačilo na banke izven Evrope.

Zaposleni prenese sredstva na račun, ki je pod nadzorom prevaranta.

Navodila, kako nadaljevati, sledijo pozneje, s strani tretje osebe ali prek e-pošte.

Zaposlenega prosijo, naj ne uporabi rednih postopkov odobritve.

Sklicujejo se na občutljivo situacijo (npr. davčni nadzor, združitev, prevzem).

KAKŠNI SO ZNAKI?

- Nepričakovana e-pošta/telefonski klic
- Neposreden stik višjega uradnika, s katerim običajno niste v stiku
- Zahteva za popolno zaupnost
- Pritisk in občutek nujnosti
- Nenavadna zahteva v nasprotju z notranjimi postopki
- Grožnje ali nenavadno laskanje/obljube o nagradi

KAJ LAHKO NAREDIMO?

KOT PODJETJE

Zavedajte se tveganj in poskrbite, da bodo tudi **zaposleni obveščeni in ozaveščeni**.

Spodbujajte svoje osebje, **naj previdno pristopajo k zahtevam za plačilo**.

Izvajati notranje protokole v zvezi s plačili.

Izvedite postopek za preverjanje upravičenosti zahtevkov za plačilo, prejetih po e-pošti.

Vzpostavite **rutine poročanja** za upravljanje goljufij.

Preglejte informacije, objavljene na spletnem mestu vašega podjetja, omejite podatke in bodite previdni glede družbenih medijev.

Nadgradite in posodobite tehnično varnost.

V primeru poskusov goljufije se vedno obrnite na policijo, tudi če niste postali žrtev prevare.

KOT ZAPOSLENI

Strogo uporabljajte veljavne varnostne postopke za plačila in javna naročila. **Ne preskočite nobenih korakov in ne popustite pritiskom**.

Pri obravnavi občutljivih informacij/denarnih nakazil vedno **skrbno preverite e-poštne naslove**.

V primeru dvoma glede naloga za prenos se **posvetujte s pristojnim kolegom**.

Nikoli ne odpirajte sumljivih povezav ali prilog, prejetih po e-pošti. Bodite še posebej previdni pri preverjanju zasebne e-pošte v računalnikih podjetja.

Omejite informacije in bodite previdni glede družbenih medijev.

Izogibajte se izmenjavi informacij o hierarhiji, varnosti ali postopkih podjetja.

Če prejmete sumljivo e-pošto ali klic, vedno obvestite ustrezno službo.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO · #CyberScams