

"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".



Često se zahtjev odnosi na međunarodna plaćanja bankama izvan Europe.

Zaposlenik prenosi sredstva na račun koji kontrolira prevarant.

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

Od zaposlenika se traži da ne slijedi redovne autorizacijske postupke.

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

## KAKO PREPOZNATI ZNAKOVE?

- Neočekivani poziv/poruka
- Izravni kontakt od visokog dužnosnika u tvrtki s kojim obično niste u kontaktu
- Zahtjeva 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 TVRRTKA

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 poštujujte 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.