

# CEO PODVOD/BUSINESS EMAIL COMPROMISE (BEC)

CEO podvod/BEC prebieha tak, že zamestnanec oprávnený vykonávať platby je oklamán a uhradí falošnú faktúru alebo vykoná neschválený prevod z firemného účtu.

## AKO TO PREBIEHA?

Podvodník zavolá alebo pošle e-mail, v ktorom predstiera, že má vo firme vysoké postavenie (napr. generálny riaditeľ).



Majú dobrú znalosť o organizácii.



Vyžadujú okamžitú platbu.



Používajú výrazy napr. "Utajené", "Spoločnosť Vám verí", "Momentálne nie som dostupný".



Odvolávajú sa na významnú okolnosť (napr. daňová kontrola, zlúčenie, akvizícia).



Často ide o pokyn na medzinárodnú platbu do banky mimo Európy.



Zamestnanec pošle peniaze na účet, nad ktorým má podvodník kontrolu.



Pokyny o ďalšom postupe môžu prísť neskôr, od tretej osoby alebo e-mailom.

Žiadajú zamestnanca, aby nepostupoval podľa riadnych schvaľovacích postupov.

## AKÉ SÚ TYPICKÉ ZNAKY?

- Neštandardný e-mail/telefonát
- Naliehavosť a dojem neodkladnosti
- Oslovenie pracovníkom, s ktorým nie ste bežne v kontakte
- Neobvyklá žiadosť v rozpore s internými postupmi
- Požiadavka na úplné utajenie
- Vyhrážky alebo neobvyklé povzbudenie/prísľub odmeny

## ČO MÔŽETE UROBIŤ?

### FIRMA

Dajte si pozor na riziká a zariad'te, aby boli zamestnanci informovaní a opatrní.

Upozornite zamestnancov, aby boli obozretní pri žiadostiach o platbu.

Implementujte interné postupy týkajúce sa platieb.

Implementujte postupy na overenie oprávnenosti žiadostí o platbu prijatých e-mailom.

Nastavte procesy nahlásovania podvodov.

Zvážte, aké informácie uvediete na vašej firemnej webovej stránke, obmedzte množstvo informácií a buďte opatrní na sociálnych sieťach.

Modernizujte a aktualizujte technické zabezpečenie.

! Vždy nahláste polícií pokus o podvod, aj keď ste sa nestali obeťou podvodu.

### ZAMESTNANEC

Prísne dodržujte bezpečnostné postupy pri platbách a nákupe. Nevynechajte žiadne kroky a nepodľahnite tlaku.

Keď pracujete s citlivými informáciami/peňažnými prevodmi, vždy starostlivo skontrolujte e-mailové adresy.

Ak máte pochybnosti o platobnom príkaze, poraďte sa s príslušným pracovníkom.

Nikdy neotvárajte podozrivé odkazy alebo prílohy v e-mailoch. Buďte obzvlášť opatrní, ak si kontrolujete váš súkromný e-mail na firemnom počítači.

Obmedzte množstvo informácií a buďte opatrní na sociálnych sieťach.

Nezdieľajte informácie o firemnej štruktúre, bezpečnosti a procesoch.

! Ak dostanete podozrivý e-mail alebo telefonát, vždy informujte IT oddelenie.