

CEO/BEC FRAUD - PODVOD ZNEUŽÍVAJÍCÍ JMÉNO GENERÁLNÍHO ŘEDITELE NEBO FIREMNÍ E-MAIL

K podvodu typu CEO/BEC fraud dochází, pokud je zaměstnanec oprávněný provádět platby podvodně zmanipulován, aby proplatil falešnou fakturu nebo provedl neoprávněný převod z firemního účtu.

JAK TO FUNGUJE?

Podvodník zavolá nebo pošle e-mail a vydává se za vysokého manažera společnosti (např. generálního nebo finančního ředitele).

Mají dobré znalosti o společnosti.

Požadují naléhavé provedení platby.

Používají slova a slovní spojení, jako: "Důvěrnost", "Společnost vám důvěřuje", "Nejsem momentálně k dispozici".



Často se jedná o požadavek na mezinárodní platby bankám mimo Evropu.

Zaměstnanec převede prostředky na účet spravovaný podvodníkem.

Pokyny, jak postupovat, mohou být dány později, třetí osobou nebo e-mailem.

Odvolávají se na choulostivou situaci (např. daňová kontrola, fúze, akvizice).

Požadují, aby zaměstnanec nepostupoval podle zavedených postupů pro schvalování.

JAK TO POZNÁM?

- Nevyžádaný e-mail/telefonát.
- Přímý kontakt ze strany vysokého manažera, se kterým nejste běžně ve styku.
- Žádost o zachování absolutní důvěrnosti.
- Nátlak a pocit naléhavosti.
- Neobvyklá žádost v rozporu s interními postupy
- Zastrasování nebo nezvyklé lichotky/slibování odměn.

CO MŮŽETE DĚLAT?

JAKO OBCHODNÍ SPOLEČNOST

Buďte si vědomi těchto rizik a zajistěte, aby byli také zaměstnanci informováni.

Vyzvěte své zaměstnance, aby k požadavkům na platby přistupovali obezřetně.

Stanovte vnitřní postupy týkající se plateb.

Stanovte postup pro ověření oprávněnosti žádostí o platbu obdržených e-mailem.

Stanovte postupy pro hlášení podvodů.

Zkontrolujte informace uveřejněné na webových stránkách vaší společnosti, omezte informace a přistupujte obezřetně k sociálním médiím.

Aktualizujte vaše technické zabezpečení.

! Pokud dojde k pokusu o podvod, vždy se obraťte na policii, a to i v případě, že jste se nestali obětí podvodu.

JAKO ZAMĚSTNANEC

Důsledně dodržujte nastavené bezpečnostní postupy pro platby a zadávání zakázek. **Nevynechávejte žádné kroky a nepodléhejte tlaku.**

Při zacházení s citlivými informacemi / převody peněz vždy pečlivě kontrolujte e-mailové adresy.

V případě pochybností o platebním příkazu se **poradte s příslušným kolegou.**

Nikdy **neotvírejte podezřelé odkazy nebo přílohy**, které jste obdrželi e-mailem. Buďte zvláště opatrní při otevírání soukromých e-mailů v pracovních počítačích.

Omezte informace sdílené na sociálních sítích a chovejte se obezřetně.

Vyhnete se sdílení informací o organizační struktuře vaší společnosti, bezpečnosti nebo pracovních postupech.

! Pokud obdržíte podezřelý e-mail nebo telefonický hovor, informujte vždy vaše IT oddělení.