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".

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

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.

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
- Zastrašování 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 poraďte s příslušným kolegou.**

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

Omezte informace sdílené na sociálních sítích a **chovejte se obezřetně.**

Vyhněte 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.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE

#CyberScams

INVESTIČNÍ PODVODY

Běžné investiční podvody se mohou týkat výhodných investičních příležitostí do akcií, dluhopisů, kryptoměn, vzácných kovů, zámořských pozemků nebo alternativních energií.

JAK TO POZNÁM?

- Slibují vám rychlé zisky a ujišťují vás, že investice je bezpečná.
- Nabídka je platná pouze na omezenou dobu.
- Máte opakované nevyžádané telefonní hovory.

- Nabídka je určena pouze vám a jste požádáni, abyste ji nesdíleli.

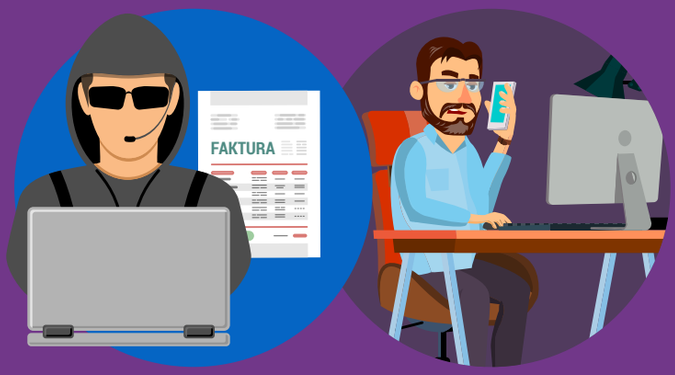
CO MŮŽETE DĚLAT?

- Předtím, než poukážete peníze nebo investujete, **vždy konzultujte s nezávislým finančním poradcem**.
- **Odmítejte nečekané telefonáty,** které se týkají investičních příležitostí.
- **Nedůvěřujte** nabídkám, které slibují bezpečnou investici, zaručené výnosy a velké zisky.
- **Dejte si pozor na budoucí podvody.** Pokud jste již investovali do podvodu, pravděpodobně se na vás podvodníci znovu zaměří nebo prodají vaše údaje jiným zločincům.
- Máte-li podezření, **kontaktujte policii.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE

#CyberScams

PODVODNÁ FAKTURA



JAK TO FUNGUJE?

- Obchodní společnost je oslovena někým, kdo se vydává za zástupce dodavatele/poskytovatele služeb/věřitele.
- Ke kontaktu může být využito různých přístupů: telefon, dopis, e-mail, atd.
- Podvodník požaduje změnu bankovních údajů za účelem platby (tj. údajů o bankovním účtu příjemce platby) u budoucích faktur. Nově navrhovaný účet ovládá podvodník.

CO MŮŽETE DĚLAT?

JAKO OBCHODNÍ SPOLEČNOST

Zajistěte, aby byli zaměstnanci **seznámeni** s podvodem tohoto typu a byli informováni o tom, jak se mu vyhnout.

Informujte pracovníky zodpovídající za úhrady faktur, aby **je prověřovali při zjištění nesrovnalostí.**

Stanovte postup **pro ověření** oprávněnosti žádostí o platbu.

Zkontrolujte informace zveřejněné na webových stránkách společnosti, zejména smlouvy a dodavatele. Zajistěte, aby vaši zaměstnanci na svých profilech na sociálních médiích omezili sdílení informací o společnosti.

JAKO ZAMĚSTNANEC

Ověřte všechny žádosti, které mají pocházet od vašich věřitelů, zejména pokud vás požádají o změnu bankovních údajů u budoucích faktur.

U plateb převyšujících určitou částku **stanovte postup pro potvrzení** správnosti bankovního účtu a příjemce (např. sjednat schůzku se společností).

Nepoužívejte kontaktní údaje z dopisu / faxu / emailu, které požadují změnu. Použijte kontaktní údaje z předchozí korespondence.

O úhradě faktury **e-mailem informujte příjemce.** Uveďte název banky příjemce a poslední čtyři číslice jednotného účtu zřízeného k zajištění bezpečnosti.

Stanovte **jednotná kontaktní místa** se společnostmi s nimiž provádíte pravidelné platby.

Omezte informace, které o svém zaměstnavateli sdílíte na sociálních médiích.

Podezření na pokus o podvod vždy hlaste policii, přestože jste se obětí podvodu nestali.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE

#CyberScams

PODVODY PŘI NAKUPOVÁNÍ NA INTERNETU

Nabídky na internetu představují často výhodnou koupi, ale pozor na podvody.

CO MŮŽETE DĚLAT?

- Pokud je to možné, **využívejte webové stránky tuzemských obchodníků –** je větší pravděpodobnost, že budete moci vyřešit případné problémy.
- **Udělejte si vlastní průzkum** – před nákupem si přečtěte hodnocení.

- **Používejte kreditní karty** – máte větší šanci získat peníze zpět.
- Při placení používejte pouze **zabezpečené platební služby** – je požadována platba prostřednictvím převodu peněz? Rozmyslete si to!
- Plaťte pouze tehdy, máte-li zabezpečené připojení k internetu – vyhněte se používání bezplatných nebo otevřených veřejných Wifi.
- **Plaťte pouze z bezpečného zařízení** – aktualizujte si svůj operační systém a bezpečnostní software.
- Dejte si pozor na reklamy nabízející výhodné koupě nebo zázračné produkty. **Pokud zní nabídka příliš dobře na to, aby to mohla být skutečná, nejspíš nebude!**
- Vyskakovací reklama, která vám oznamuje, že jste získali cenu? **Zamyslete se**, možná jste zrovna vyhráli škodlivý software.
- Pokud produkt nedorazí, kontaktujte prodejce. Pokud vám neodpoví, **kontaktujte svou banku.**

Podezření na pokus o podvod vždy hlaste policii, přestože jste se obětí podvodu nestali.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE

#CyberScams

PHISHINGOVÉ E-MAILY, KTERÉ SE TVÁŘÍ, JAKO BY BYLY ODESLÁNY Z BANKY

Phishing je prováděn prostřednictvím podvodných e-mailů, které od adresátů lákají osobní, finanční nebo bezpečnostních údaje.

JAK TO FUNGUJE?

Tyto e-maily:

mohou vypadat shodně jako korespondence zasílaná skutečnou bankou.

kopírovat loga, strukturu a znění skutečných e-mailů.

požadovat od vás, abyste si stáhli připojený dokument nebo klikli na odkaz.

používat jazyk, který vyvolává pocit naléhavosti.

Kyberzločinci se spoléhají na to, že jsou lidé zaneprázdněni; na první pohled vypadají tyto podvodné e-maily jako pravé.

Mějte se na pozoru pokud používáte mobilní zařízení. Z vašeho telefonu nebo tabletu může být obtížnější zjistit pokus o phishing.

CO MŮŽETE DĚLAT?

- **Aktualizujte svůj software,** včetně svého prohlížeče, antivirového a operačního systému.
- **Mějte se obzvlášť** na pozoru, pokud jste v e-mailu z „banky" žádáni o citlivé informace (např. heslo k vašemu internetovému bankovnictví).
- **Podívejte se na e-mail** pozorně: porovnejte adresu s předchozími skutečnými zprávami ze své banky. Zkontrolujte, zda e-mail neobsahuje gramatické a pravopisné chyby.
- **Neodpovídejte na podezřelý e-mail,** místo toho jej přepošlete své bance na adresu, kterou sami zadáte.
- **Neklikejte na odkaz a nestahujte přílohu,** místo toho zadejte adresu do svého prohlížeče.
- Pokud máte pochybnosti, **ověřte** to na webových stránkách vaší banky nebo do banky zavolejte.

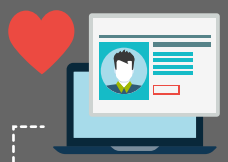
#CyberScams

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE

ROMANCE SCAM

Podvodníci si své oběti vybírají na on-line seznamkách, ale mohou také k navázání kontaktu použít sociální média nebo e-mail.

JAK TO POZNÁM?



Někdo, s kým jste se nedávno setkali online, vám vyzná silné city a požádá vás o soukromý chat.

Jejich zprávy jsou často chybně napsané a jsou nekonkrétní.

Jejich on-line profil neodpovídá tomu, co vám říkají.

Mohou vás požádat o zaslání vašich intimních fotografií nebo videí.

Nejdřív získají vaši důvěru. Potom vás požádají o peníze, dárky nebo o údaje k vašemu bankovnímu účtu/kreditní kartě.

Pokud peníze nepošlete, mohou se vás pokusit vydírat. Pokud je pošlete, budou žádat o další.

STALI JSTE SE OBĚTÍ?

Neciťte se trapně!
Přerušte okamžitě veškeré kontakty.
Pokud je to možné, uschovejte si veškerou komunikaci, například zprávy z chatu.
Podejte stížnost na policii.
Oznamte to správci webové stránky, na níž vás podvodník poprvé kontaktoval.
Pokud jste poskytli údaje o vašem účtu, kontaktujte svou banku.

CO MŮŽETE DĚLAT?

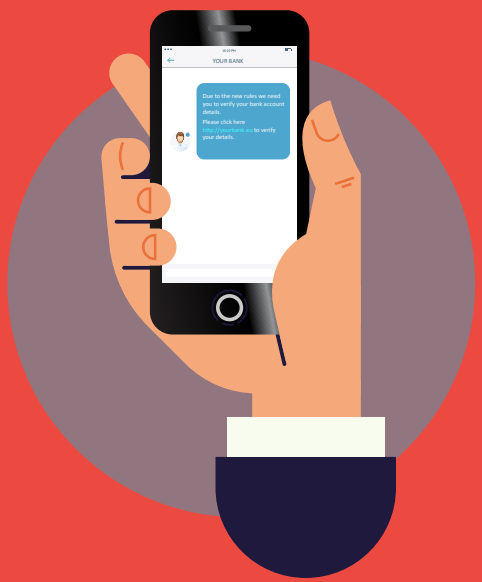
- **Buďte velmi opatrní** v tom, kolik osobních informací sdílíte na sociálních sítích nebo na seznamkách.
- **Vždy zvažte rizika.** Podvodníci se vyskytují i na nejserióznějších stránkách.
- **Postupujte pomalu** a pokládejte otázky.
- **Prozkoumejte** fotografii a profil dané osoby a zjistěte, zdajiž nebyly použity i jinde.
- **Dávejte si pozor** na pravopisné a gramatické chyby, nesrovnalosti v jejich příbězích a výmluvy typu, že jejich kamera nefunguje.
- **Nesdílejte** žádné kompromitující materiály, kterými by vás mohli vydírat.
- Pokud souhlasíte s tím, že se setkáte osobně, **řekněte rodině a přátelům**, kam jdete.
- **Dávejte si pozor na žádosti o peníze.** Nikdy neposílejte peníze, neposkytujte údaje o platební kartě, údaje o internetovém účtu, ani kopie osobních dokladů.
- **Neposílejte jim žádné platby předem.**
- **Nepřevádějte peníze** za nikoho jiného: praní špinavých peněz je trestný čin.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE

#CyberScams

BANKOVNÍ PHISINGOVÉ SMS - SMSISHING

Smishing (kombinace slov SMS a phishing) je pokus podvodníků získat osobní, finanční nebo bezpečnostní informace prostřednictvím textové zprávy.



JAK TO FUNGUJE?

V textové zprávě jste obvykle požádáni, abyste klikli na odkaz nebo zavolali na telefonní číslo pro „ověření“, „aktualizaci“ nebo „opětovnou aktivaci“ svého účtu. Ale... odkaz zavede na falešné webové stránky a telefonní číslo na podvodníka, který se vydává za skutečnou firmu.

CO MŮŽETE UDĚLAT?

- **Neklikejte na odkazy, přílohy nebo obrázky,** které obdržíte v nevyžádaných textových zprávách, aniž byste si předem ověřili odesílatele.
- **Nic neuspěchejte.** Dopřejte si čas než odpovíte a vše náležitě zkontrolujte.
- **Nikdy nereagujte na textovou zprávu,** která požaduje váš PIN kód, heslo k online bankovnictví nebo jiné bezpečnostní údaje.
- Pokud si myslíte, že jste možná odpověděli na smishing SMS a poskytli jste své bankovní údaje, okamžitě **kontaktujte svou banku.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE | #CyberScams

FALEŠNÉ BANKOVNÍ WEBOVÉ STRÁNKY

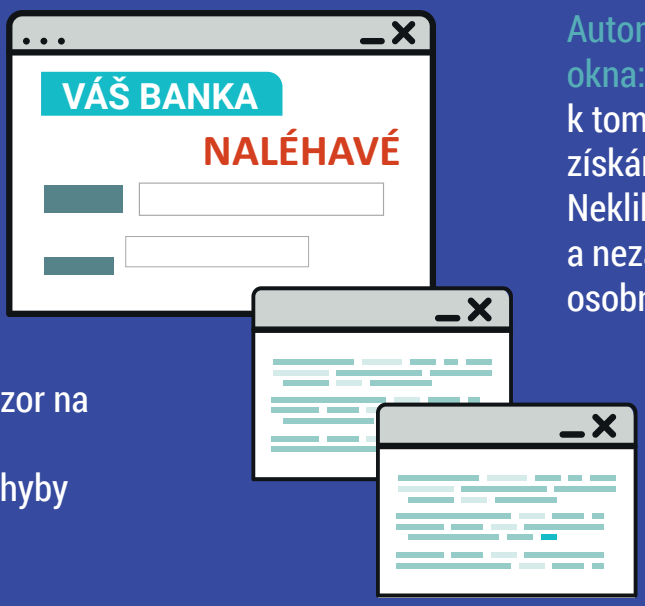
Bankovní phishingové e-maily obvykle obsahují odkazy, které vás zavedou na falešnou bankovní webovou stránku, kde jste požádáni o uvedení svých finančních a osobních údajů.

JAK TO POZNÁM?

Falešné bankovní webové stránky vypadají téměř totožně jako jejich pravá verze. Na těchto webových stránkách se často zobrazí automaticky otevírané okno s žádostí o poskytnutí bankovních údajů. Banky takováto okna nepoužívají.

Tyto webové stránky obvykle obsahují:

Naléhavost: zprávy tohoto typu na důvěryhodných webových stránkách nenajdete.



Automaticky otevíraná okna: obvykle se používají k tomu, aby od vás byly získány citlivé informace. Neklikejte na ně a nezadávejte do nich své osobní údaje.

Chabá úprava: dávejte si pozor na webové stránky, které mají nedostatky v úpravě nebo chyby v pravopisu a gramatice.

CO MŮŽETE DĚLAT?

Nikdy neklikejte na odkazy obsažené v e-mailech, které by vás měly zavést na webovou stránku vaší banky.

Vždy zadávejte odkaz ručně nebo použijte již existující odkaz ze seznamu oblíbených položek.

Používejte vyhledávač, který vám umožní **blokovat automaticky otevíraná okna.**

Pokud něco důležitého skutečně vyžaduje vaši pozornost, budete o tom informováni vaší bankou po **přihlášení se do internetového bankovnictví.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICIE ČESKÉ REPUBLIKY | ČESKÁ BANKOVNÍ ASOCIACE

#CyberScams

VISHING – PHISHING PROSTŘEDNICTVÍM TELEFONÁTU Z ÚDAJNÉ BANKY

Vishing (kombinace slov Voice a Phishing) je pokus o podvod prostřednictvím telefonního hovoru, při kterém se podvodníci snaží získat od oběti finanční nebo bezpečnostní informace nebo ji přimět, aby jim převedla peníze.

CO MŮŽETE DĚLAT?

- **Dávejte si pozor** na nevyžádané telefonní hovory.
- **Vezměte si číslo volajícího** a sdělte mu, že mu zavoláte zpátky.
- Chcete-li prověřit totožnost volajícího, **vyhledejte si telefonní číslo dané společnosti** a kontaktujte ji přímo.
- **Neověřujte si volajícího pomocí telefonního čísla, které vám poskytl** (může být falešné).
- Podvodníci si mohou zjistit základní informace o vás online (např.na sociálních médiích). **Nedomnívejte se, že volající není podvodník** jen proto, že zná tyto údaje.
- **Nesdílejte** číslo PIN své kreditní nebo debetní karty, ani heslo pro online bankovnictví. Vaše banka by vás nikdy nepožádala o takové údaje.
- **Nepřevádějte** na jejich žádost peníze na jiný účet. Vaše banka vás o něco takového nikdy nepožádá.
- Pokud si myslíte, že se jedná o falešný telefonát, **oznamte to své bance.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICIE ČESKÉ REPUBLIKY

ČESKÁ BANKOVNÍ ASOCIACE

#CyberScams