CEO PODVOD/BUSINESS EMAIL COMPROMISE (BEC)

CEO podvod/BEC prebieha tak, že zamestnanec oprávnený vykonávať platby je oklamaný 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).

Žiadajú zamestnanca, aby nepostupoval podľa riadnych schvaľovacích postupov.

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

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

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

AKÉ SÚ TYPICKÉ ZNAKY?

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

ČO MÔŽETE UROBIŤ?

FIRMA

Dajte si pozor na riziká a zariaďte, aby **boli zamestnanci informovaní a opatrní.**

Upozornite zamestnancov, aby boli **obozretní pri žiadostiach o platbu.**

Implementuje interné postupy týkajúce sa platieb.

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

Nastavte **procesy nahlasovania** 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 polícii 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 opatrný, 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.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams

INVESTIČNÉ PODVODY

Obvyklými investičnými podvodmi môžu byť lukratívne investičné príležitosti, napr. akcie, dlhopisy, virtuálne meny, vzácne kovy, investovanie v zahraničí alebo alternatívne zdroje energie.

AKÉ SÚ TYPICKÉ ZNAKY?

- Sľubujú vám rýchlu návratnosť a bezpečné investovanie.
- Ponuka je časovo obmedzená.
- Opakovane dostanete neštandardný telefonát.
- Ponuka je určená len vám a žiadajú vás, aby ste o tom nikomu nehovorili.

ČO MÔŽETE UROBIŤ?

- **Vždy sa poraďte** pred tým, ako dáte niekomu peniaze alebo investujete.
- **Nereagujte na neštandardné telefonáty** ohľadne investičných príležitostí.
- **Buďte opatrní** pri ponukách sľubujúcich bezpečné investovanie, garantovanú návratnosť a veľký zisk.
- **Dajte si pozor na ďalšie podvody.** Ak vás podviedli pri investovaní, podvodníci vás pravdepodobne znovu oslovia alebo predajú informácie o vás ďalším zločincom.
- Svoje podozrenie **nahláste polícii.**

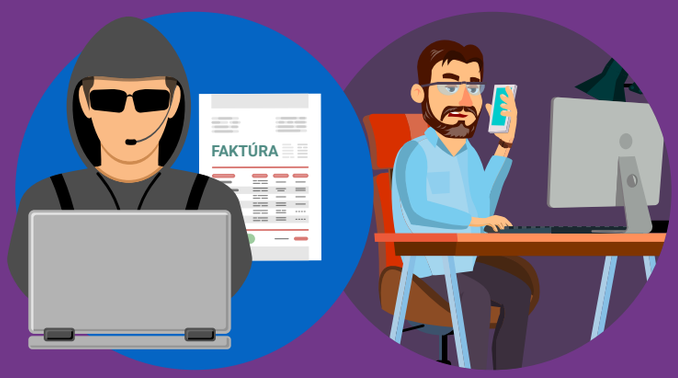
EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams

FAKTURAČNÝ PODVOD



AKO TO PREBIEHA?

- Firmu osloví niekto, kto predstiera, že je dodávateľ/poskytovateľ služby/veriteľ.
- Môžu byť použité rôzne spôsoby oslovenia - telefonát, list, e-mail a pod.
- Podvodník žiada zmeniť údaje o banke (napr. údaje o bankovom účte príjemcu platby) na platbách za budúce faktúry. Podvodník má nad novým účtom kontrolu.

ČO MÔŽETE UROBIŤ?

FIRMA

Informujte zamestnancov o takomto type podvodu a poučte ich, ako mu zabrániť.

Poučte zamestnancov zodpovedných za platbu faktúr, aby **preverili každú nezrovnalosť.**

Prehodnoďte informácie uvedené na firemnej webovej stránke, najmä zmluvy a dodávateľov. Zabezpečte, aby zamestnanci obmedzili množstvo informácií o firme na sociálnych sietiach.

Implementuje postup ako overiť oprávnenosť žiadosti o platbu.

ZAMESTNANEC

Overte všetky žiadosti vašich veriteľov, obzvlášť ak vás žiadajú o zmenu údajov o banke na budúcich faktúrach.

Vytvorte postup na potvrdenie správneho bankového účtu a príjemcu pri platbách nad určitú hranicu (napr. stretnutie s predstaviteľom firmy).

Nepoužívajte kontaktné údaje z listu/faxu/e-mailu, v ktorom žiadajú zmenu. Použite údaje z **predchádzajúcej komunikácie.**

Keď platíte faktúru, **informujte príjemcu e-mailom**. Kvôli bezpečnosti uveďte názov banky príjemcu a posledné štyri číslice účtu.

Zriaďte jednotné kontaktné miesta s firmami, ktorým pravidelne platíte.

Obmedzte informácie, ktoré zverejňujete o zamestnávateľovi na sociálnych sieťach.

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

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams

PODVODY PRI INTERNETOVOM NAKUPOVANÍ

Aj keď sú internetové ponuky často výhodné, dajte si pozor na podvody.

ČO MÔŽETE UROBIŤ?

- Pokiaľ je to možné, **nakupujte na tuzemských internetových obchodoch -** ľahšie vyriešite možné problémy.
- **Urobte si prieskum -** pred nákupom si prečítajte recenzie.
- **Používajte kreditné karty -** ľahšie dostanete späť vaše peniaze.

- **Používajte iba zabezpečené platby -** žiadajú od vás zaslať peniaze alebo vykonať bankový prevod? Dobre si to premyslite!
- Plaťte len na **zabezpečenom internetovom pripojení** - nepoužívajte verejné Wi-Fi.
- **Plaťte len na bezpečnom zariadení -** aktualizujte si operačný systém a bezpečnostný softvér.
- Dajte si pozor na mimoriadne ponuky alebo zázračné výrobky **- je to príliš dobré na to, aby to bola pravda!**
- Vyskakovacie okno s výhrou? **Buďte obozretní,** možno ste vyhrali škodlivý softvér.
- Ak vám nedodajú tovar, kontaktujte predajcu. Ak vám neodpovie, **kontaktujte Vašu banku.**

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

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams

BANKOVÉ PHISHINGOVÉ E-MAILY

Phishing znamená posielanie podvodných e-mailov, ktoré oklamú príjemcov, aby vyzradili osobné, finančné alebo bezpečnostné údaje.

AKO TO PREBIEHA?

Phishingové e-maily

môžu vyzerať ako komunikácia s vašou bankou.

žiadajú vás stiahnuť prílohu alebo kliknúť na odkaz.

kopírujú logá, grafiku a štýl pravých e-mailov.

používajú formuláciu navodzujúcu neodkladnosť.

ČO MÔŽETE UROBIŤ?

- **Aktualizujte si softvér** vrátane prehliadača, antivírového programu a operačného systému.
- Buďte obzvlášť **obozretní**, ak e-mail z „banky" žiada od vás citlivé údaje (napr. heslo do vášho internetového bankového účtu).
- **Podrobne si prezrite e-mail** - porovnajte adresu s predchádzajúcimi správami z banky. Skontrolujte pravopis a gramatiku.
- **Neodpovedajte na podozrivý e-mail,** ale prepošlite ho vašej banke, pričom adresu napíšte manuálne.
- **Neklikajte na odkazy ani nesťahujte prílohy,** ale adresu do prehliadača napíšte manuálne.
- Ak máte o niečom pochybnosť, **preverte** si to na webovej stránke alebo zavolajte do banky.

Podvodníci sa spoliehajú, že ľudia sú zaneprázdnení; podvodné e-maily na prvý pohľad vyzerajú ako pravé.

#CyberScams

Dajte si pozor, keď používate mobilné zariadenie. Rozpoznať phishing môže byť ťažšie na mobile alebo tablete.

EUROPOL EC3 European Cybercrime Centre

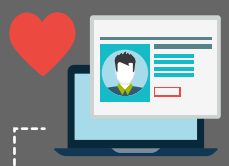
EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

ZOZNAMOVACÍ PODVOD

Podvodníci hľadajú obete na internetových zoznamkách, ale využívajú aj sociálne siete a e-maily.

AKÉ SÚ TYPICKÉ ZNAKY?



Niekto, koho ste nedávno spoznali na internete, vám prejavuje náklonnosť a chce chatovať.

Ich správy často obsahujú chyby a sú všeobecné.

Ich internetový profil nezodpovedá tomu, čo vám tvrdia.

Môžu vás žiadať o zaslanie intímnych fotografií alebo videí.

Najprv si získajú vašu dôveru. Potom chcú od vás peniaze, darčeky alebo údaje o bankovom účte/kreditnej karte.

Ak im nepošlete peniaze, tak vás môžu vydierať. Ak im peniaze pošlete, budú žiadať ešte viac.

STE OBEŤ?

Nemusíte sa hanbiť!
Okamžite prerušte všetky kontakty.
Ak je to možné, uchovajte si všetku komunikáciu, napr. chat.
Podajte trestné oznámenie na polícii.
Nahláste to na stránke, kde vás podvodník prvýkrát oslovil.
Ak ste niekomu poskytli údaje o vašom účte, oznámte to banke.

ČO MÔŽETE UROBIŤ?

- **Zvážte,** aké osobné údaje zdieľate na sociálnych sieťach a zoznamkách.
- **Vždy zvážte možné riziká.** Podvodníci sú aj na serióznych stránkach.
- **Neunáhlite sa** a pýtajte sa.
- **Preverte,** či fotka alebo profil osoby nebol použitý na iných stránkach.
- **Všímajte si** pravopisné a gramatické chyby, nezrovnalosti v príbehoch a výhovorky, napr. že nefunguje kamera.
- **Nezdieľajte** žiadny kompromitujúci materiál, ktorým by vás mohli vydierať.
- Ak súhlasíte s osobným stretnutím, **povedzte rodine a priateľom**, kam idete.
- **Dajte si pozor na žiadosti o peniaze.** Nikdy neposielajte peniaze, údaje o kreditnej karte alebo internetovom účte, ani kópie osobných dokladov.
- **Neposielajte vopred peniaze.**
- **Nerobte peňažné prevody** miesto niekoho iného - pranie špinavých peňazí je trestný čin.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams

BANKOVÉ PHISHINGOVÉ SMS-KY

Smishing (slovo vzniklo kombináciou slov "SMS" a "Phishing") je pokus podvodníkov získať osobné, finančné alebo bezpečnostné údaje SMS-kou.

AKO TO PREBIEHA?

SMS-ka vás vyzve, aby ste klikli na odkaz alebo zavolali na telefónne číslo, aby „overili“, „aktualizovali“ alebo „obnovili“ váš účet. Avšak... odkaz smeruje na falošnú stránku a telefónne číslo má pod kontrolou podvodník, ktorý sa tvári ako predstaviteľ firmy.

ČO MÔŽETE UROBIŤ?

- **Neklikajte na odkazy, prílohy alebo obrázky** v nevyžiadaných SMS-kách pred tým, ako si overíte odosielateľa.
- **Neponáhľajte sa.** Pred tým, ako odpíšete, si všetko overte.
- **Nikdy nereagujte na SMS-ku,** ktorá žiada od vás PIN kód, heslo do internetového bankovníctva alebo prihlasovacie údaje.
- Ak si myslíte, že ste odpovedali na smishingovú SMS-ku a poskytli údaje o vašej banke, **ihneď kontaktujte banku.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams

FALOŠNÉ WEBOVÉ STRÁNKY BÁNK

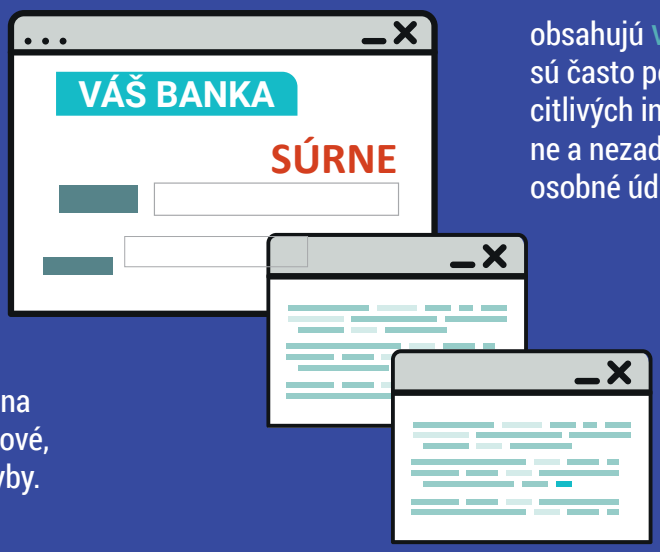
Bankové phishingové e-maily obvykle obsahujú odkaz na falošnú webovú stránku banky, na ktorej vás žiadajú o poskytnutie finančných alebo osobných údajov.

AKÉ SÚ TYPICKÉ ZNAKY?

Falošné webové stránky bánk vyzerajú skoro ako pravé. Často však obsahujú vyskakovacie okná, ktoré od vás vyžadujú prihlasovacie údaje. Banky takéto vyskakovacie okná nepoužívajú.

Falošné webové stránky obvykle

zobrazujú kritické správy - pravé webové stránky takéto správy neobsahujú.



obsahujú vyskakovacie okná - sú často používané na získavanie citlivých informácií. Neklikajte na ne a nezadávajte do nich žiadne osobné údaje.

majú zlý dizajn - dajte si pozor na stránkach, ktoré obsahujú dizajnové, pravopisné alebo gramatické chyby.

ČO MÔŽETE UROBIŤ?

Nikdy neklikajte na odkazy v e-mailoch, ktoré odkazujú na webovú stránku banky.

Internetovú adresu vždy píšte manuálne alebo používajte odkazy z obľúbených položiek.

Používajte prehliadač, ktorý dokáže **blokovať vyskakovacie okná.**

Na dôležité skutočnosti vás banka upozorní **v internet bankingu.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams

BANKOVÝ VISHING

Vishing (slovo vzniklo kombináciou slov „Voice“ a „Phishing“) je podvod prostredníctvom telefonátu, kedy sa podvodníci snažia oklamať obeť, aby vyzradila osobné, finančné alebo bezpečnostné údaje alebo previedla peniaze.

ČO MÔŽETE UROBIŤ?

- **Dajte si pozor** na neštandardné telefonáty.
- **Poznačte si telefónne číslo volajúceho** a povedzte, že mu zavoláte naspäť.
- Aby ste si overili totožnosť volajúceho, **vyhľadajte si telefónne číslo spoločnosti** a priamo ju kontaktujte.
- **Neoverujte si volajúceho na telefónnom čísle, ktoré vám uviedol** (môže ísť o falošné číslo).
- Podvodníci môžu nájsť údaje o vás na internete (napr. na sociálnych sieťach). **Nemusia vás poznať,** aj keď majú o vás informácie.
- Nikomu **neposkytujte** PIN kód k vašej platobnej karte alebo heslo do internet bankingu. Banka nikdy nežiada tieto údaje.
- **Neposielajte peniaze** na cudzí účet na základe žiadosti inej osoby. Banka vás o toto nikdy nežiada.
- Ak si myslíte, že ide o podvodný telefonát, **nahláste to banke**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

#CyberScams