

UPOZORNENIE NA ODCUDZENIE KORPORÁTNEJ IDENTITY

Odcudzenie korporátnej identity je jedným z „prekvitajúcich obchodov“ vo svete biznisu. Jeho široký záber a vyvíjajúca sa tendencia znamenajú, že treba proaktívne konať, aby ste ochránili svoje aktíva a identitu.

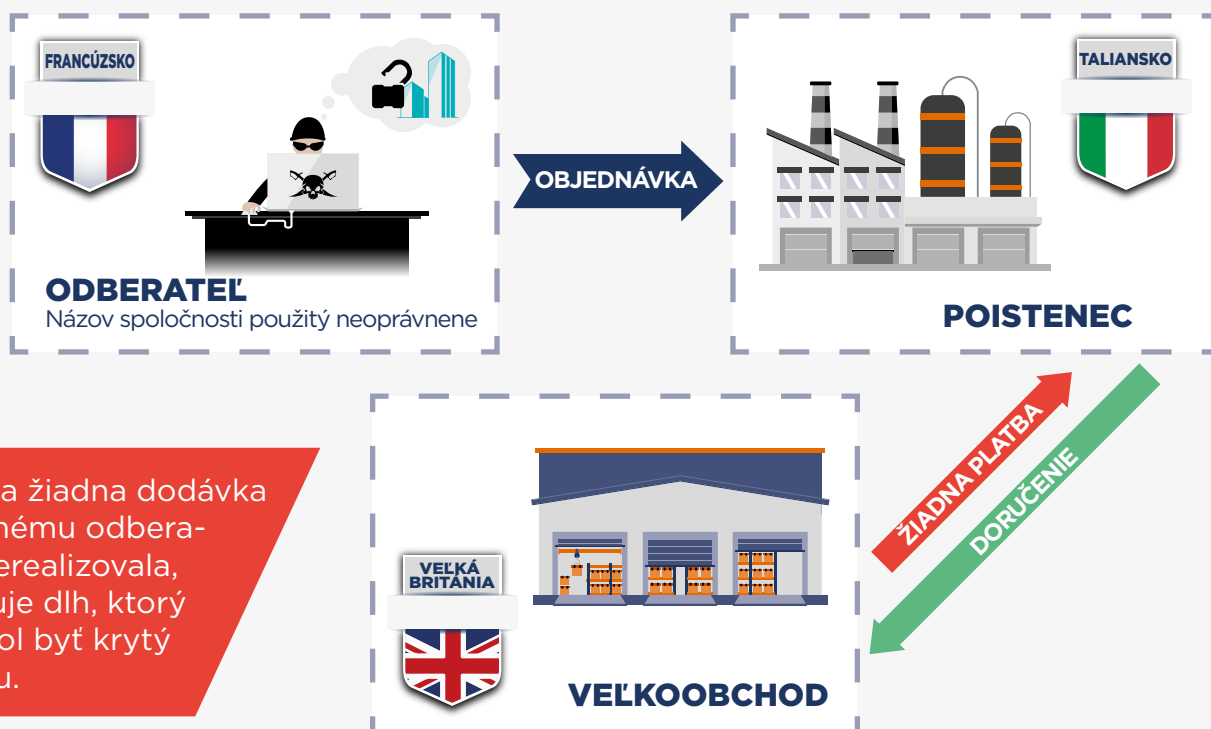
Ak falošná korporátna identita alebo identifikačné údaje inej spoločnosti sú použité na podporu protiprávnej aktivity, predstavuje to vážne prevádzkové riziko.

V ostatných pár týždňoch bola spoločnosť Coface informovaná o niekoľkých podvodoch súvisiacich s krádežou identity a odporúča zvýšenú opatrnosť.

V praxi to prebieha tak, že podvodníci používajú firemnú identitu reálnej spoločnosti, najčastejšie s dobrým platobným záznamom a morálkou, aby si zaobstarali tovar a služby od ich zákazníkov / poistencov.

Nedávna schéma podvodu, s ktorou sme boli konfrontovaní, by mohla byť popísaná nasledovne:

Odcudzenie korporátnej identity: príklad



Keďže sa žiadna dodávka solventnému odberateľovi nerealizovala, neexistuje dlh, ktorý by mohol byť krytý poisťkou.

Podvodníci sú dosť dobre organizovaní, dostanú sa do telefónnych liniek, vytvárajú emailové adresy, falšujú objednávkové formuláre, kupujú informácie z obchodného registra a podiely v obchodnom registri s cieľom otvorenia účtu kupujúceho v spoločnosti.

Toto je dôvodom, prečo by ste mali podniknúť niektoré preventívne opatrenia, keď dostanete objednávkový formulár, obzvlášť, ak prichádza z cudziny a od nového odberateľa.



V skutočnosti však falošné objednávkové formuláre nikdy nebudú dokonalé. Zastavenie podvodnej objednávky sa poriadne oplatí za tých pár minút času, ktoré venujete jej overeniu.

Keď vaše oddelenie pre verejné obstarávanie / obchodné oddelenie dostane objednávku, tento základný kontrolný zoznam môže poukázať na akékoľvek oblasti, ktorých sa to týka.

Takže sa uistite, že:

- Porovnávate logo spoločnosti na webstránke s tým na objednávke, niekedy sa môžu líšiť.
- Porovnávate formát emailovej adresy (meno osoby a spoločnosti) vášho obchodného partnera s tými, ktoré môžete nájsť na webe (často v záložke „Kontakty“), keďže zvyčajne existuje len jeden formát pre celú spoločnosť. Akýkoľvek rozdiel by ste mali považovať za podozrivý (napríklad: jozko_mrkvicka@spolocnost.sk, je použitý ako j.mrkvicka@spolocnost-sluzby.com alebo mrkvicka_jozko@spolocnost-skupina.eu ...)

Budte obzvlášť opatrní ku generickým emailovým adresám, príklad: uctovneoddelenie_spolocnost.com

Podvodníci zvyčajne používajú mená osôb, ktoré v spoločnosti naozaj pracujú.

- Porovnajte formát telefónneho čísla (hlavne prvé 2 číslice)
- Skontrolujte, či spoločnosť pôsobí, má dcérske spoločnosti alebo projekt v krajine, kam má byť doručený tovar.

Tiež je niekedy možné nájsť chyby vo vetnej skladbe alebo preklepy v objednávkovom formulári, hlavne v špecifických podmienkach. Teda treba dávať pozor na takýto dokument a nastaviť interné meradlá na kontrolu pravosti dokumentu.

- Spýtajte sa sami seba, či je odberateľova aktivita kompatibilná s vašou. Dôveruj, ale preveruj: ak máte pochybnosti (objedávka, zmena bankových údajov...), vždy zavolajte svojmu odberateľovi, aby ste si to potvrdili, a uistite sa, že zamestnanci vášho účtovného oddelenia pochopili dôležitosť týchto vecí.

Radi by sme vám pripomenuli, že prípady phishingu a platby na falošný bankový účet sú stále bežné. Preto je vždy dôležité potvrdiť všetky typy zmien požiadaviek (adresa, bankový účet) s vašim dodávateľom.

 **FAXY A EMAILY
NIE SÚ BEZPEČNÉ**