

## UPOZORNĚNÍ NA VRŮSTAJÍCÍ NEBEZPEČÍ ZNEUŽITÍ IDENTITY FIRMY

Zneužití totožnosti firem je nyní globálně na vzestupu. Díky širokému rozsahu a charakteru to znamená, že společnosti musí přijímat opatření na ochranu svého majetku a firemní identity proti takovýmto útokům.

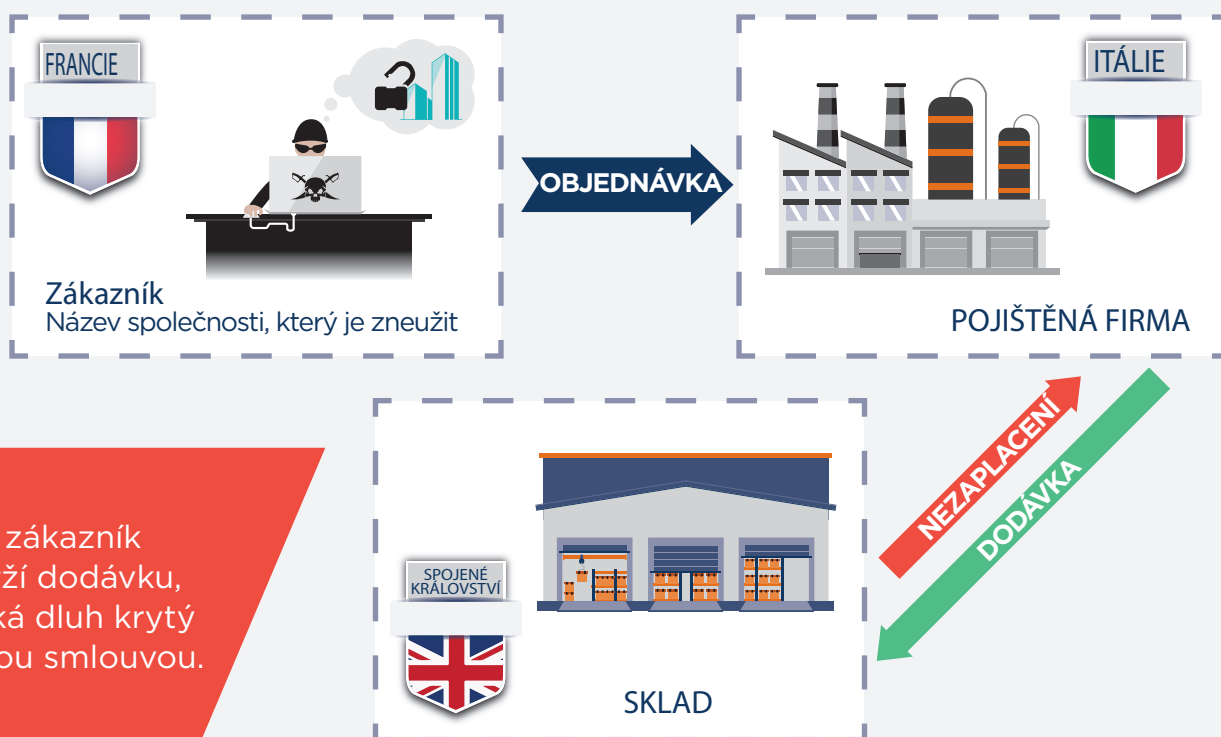
Vážnou hrozbu představuje skutečnost, kdy je falešná identita firmy nebo údaje společnosti zneužívány jinou společností k protiprávní činnosti.

Vzhledem k tomu, že v posledních týdnech byl Coface informován o několika případech podvodu spojených s krádeží firemní identity, doporučujeme Vám zvýšenou opatrnost.

V praxi to znamená, že podvodníci zneužijí totožnost skutečné firmy, nejlépe s dobrou platební morálkou a pověstí za účelem nákupu zboží od společností, které jsou našimi pojistníky.

Schéma podvodu, se kterým jsme se v poslední době setkali, lze popsat následovně:

### Příklad zneužití identity firmy



Jelikož zákazník neobdrží dodávku, nevzniká dluh krytý pojistnou smlouvou.

Skupiny podvodníků jsou dobře organizované, dokáží nabourat telefonní linky, vytvořit e-mailové adresy, falšovat objednávky, pořídit si výpis z rejstříku trestů nebo zanést údaje do obchodního rejstříku, a to vše s cílem otevřít si bankovní účet na danou společnost.

Proto je třeba zvýšené opatrnosti při přijetí objednávky, zejména pokud přichází ze zahraničí nebo od nového zákazníka.

Na druhé straně falešná objednávka není nikdy dokonalá. Stojí zato věnovat o něco více pozornosti k ověření objednávky, pokud tím můžete odhalit právě takovou podvodnou objednávku.

Při přijímání objednávky Vaším obchodním oddělením si ověřte několik skutečností:

- Logo společnosti na webových stránkách je shodné s logem na objednávce. Mohou se lišit.
- U stávajících zákazníků došlo ke změně obvyklého místa dodání.
- Obvyklá velikost objednávky se významným způsobem zvýšila.
- Formát e-mailové adresy (jméno osoby a název společnosti) Vaší kontaktní osoby je shodný s adresami uvedenými na webových stránkách. Zpravidla existuje jen jeden formát adresy pro celou společnost. Jakýkoli rozdíl by měl být považován za podezřelý (př: jan\_novak@firma.cz uveden také jako j.novak@firma-servis.com nebo novak\_jan@firma-group.eu).

Buďte obzvláště opatrní při

obecných e-mailových adresách, př.: uctarna@firma.com

Podvodníci zpravidla zneužívají jména osob, které v dané společnosti skutečně pracují.

- Porovnejte formát telefonního čísla (zvláště první 2 číslice).
- Zkontrolujte, zda společnost funguje, má dceřiné společnosti nebo působí v zemi, do které má být zboží dodáno.
- Může se objevit syntaktická chyba nebo chyba v pravopisu v objednávce a to zejména ve zvláštních podmínkách. Z tohoto důvodu je třeba věnovat pozornost takovému dokumentu a nastavit interní opatření na kontrolu platnosti dokumentu.

- Pokud jste na pochybách (u objednávky, změně bankovního spojení), vždy raději kontaktujte Vašeho zákazníka a potvrďte si správnost informací. Ujistěte se, že i Vaši zaměstnanci chápou důležitost těchto opatření.

Bohužel případy phishingu a plateb na falešný bankovní účet jsou stále běžnější. Proto je vždy důležité ověřit si všechny požadované změny (adresy, bankovního účtu, místa dodání) s Vaším dodavatelem.

 **FAX A E-MAIL  
NEJSOU BEZPEČNÉ**

