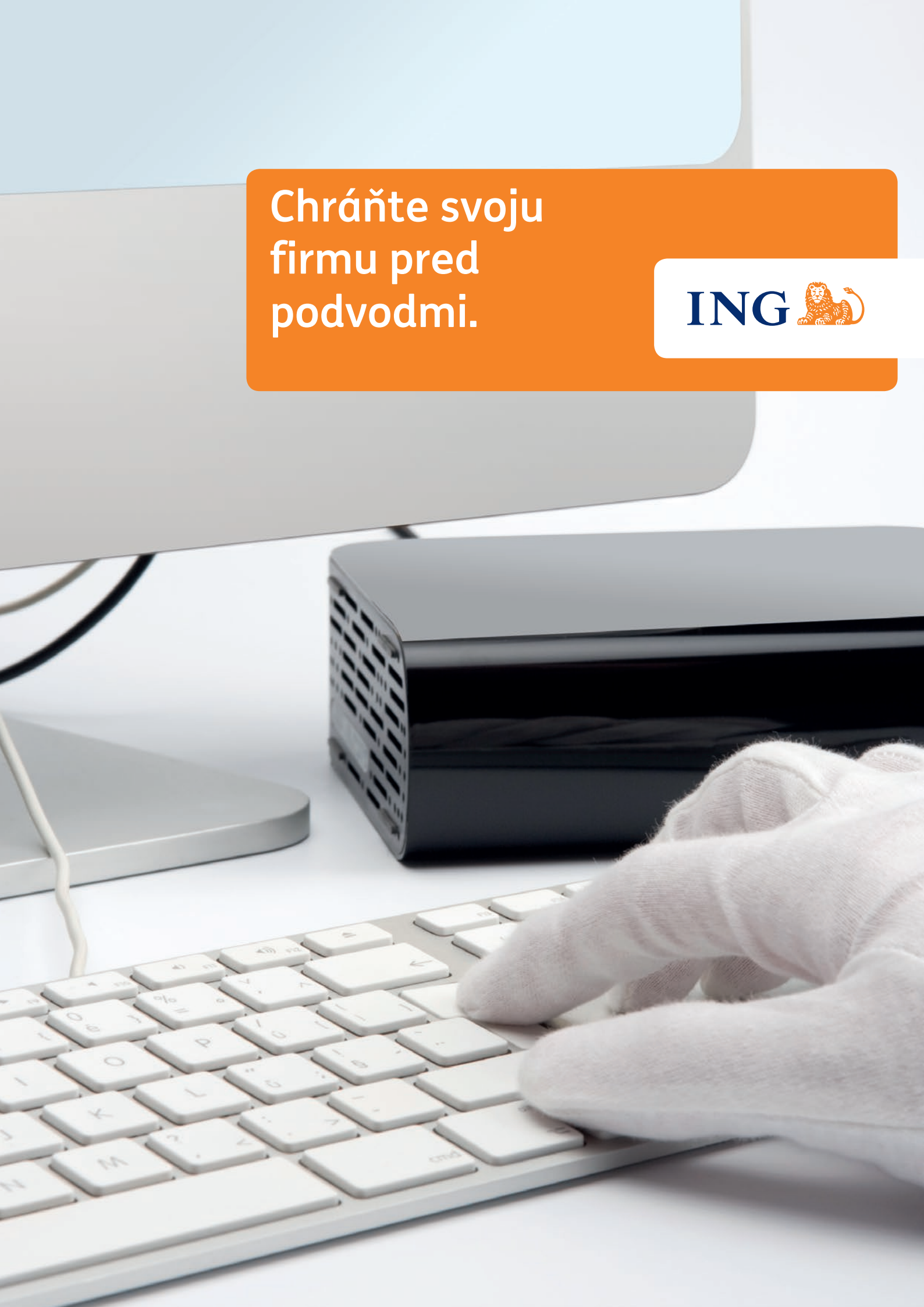
Chráňte svoju firmu pred podvodmi.



1 Podnikové podvody

Čo je v tomto dokumente?

Tento leták skúma najčastejšie prípady podvodov, ktoré môžu mať dopad na vaše podnikanie, ako aj rady, ktorých cieľom je ochrániť vás pred týmito podvodmi. Ako uvidíte, podvodníci sú šikovní a veľmi dobre organizovaní. Prípady podvodov nie sú triviálne, stávajú sa každodenne na celom svete. Majte sa na pozore.

Dôležité informácie!
Ak bol podvod odhalený, aj keď už bol prevod zrealizovaný, ihneď oznámte svojmu vzťahovému manažérovi z ING, aby sa pokúsil zablokovať finančné prostriedky predtým, než zmiznú. Majte na pamäti, že po 24 hodinách je prakticky nemožné získať späť ukradnuté prostriedky.

Ako použiť tento dokument?

Odporúčame distribuovať tento dokument vo vašej spoločnosti. Informujte všetkých riaditeľov, aby si ho prečítali, ako aj ktokoľvek s plnou mocou k účtom spoločnosti. Podvodníci sa často zameriavajú na túto druhú skupinu.

Bohužiaľ úplná ochrana neexistuje, pretože podvod je často spojený s ľudským faktorom. Napriek tomu, ak komunikujete a použijete odporúčania uvedené v tomto letáku vo svojej firme, môžete značne obmedziť riziká. Tento leták je ponúkaný spoločnosťou ING výlučne na informačné účely a nepredstavuje záväzok ING. V dôsledku toho nesmie za žiadnych okolností slúžiť ako základ na to, aby spoločnosť ING bola braná na zodpovednosť najmä v prípade, že vaša spoločnosť je napriek týmto odporúčaniam obeťou podvodov uvedených na týchto stránkach.

2 Sociálne inžinierstvo alebo CEO podvody

Čo je to?
Aké sú následky?

Sociálnym inžinierstvom je zhromažďovanie informácií o cieľovej spoločnosti s cieľom manipulovať internú osobu takejto spoločnosti, aby podnikla kroky (často na vykonanie platby) alebo sprístupnila dôverné informácie.

Čo sa stane?

1 Podvodníci sa obrátia na vašu spoločnosť e-mailom alebo telefonicky, predstierajú, že sú audítori, účtovníci alebo dokonca štátni orgán, ktorý vedie vyšetrovanie. Týmto spôsobom zhromažďujú informácie o interných platobných postupoch vašej spoločnosti, ako aj o jednotlivcoch, ktorí ich vykonávajú.

2 Potom kontaktujú zamestnancov vašej spoločnosti s oprávnením na realizáciu veľkých platieb a vystupujú ako generálny riaditeľ alebo finančný riaditeľ (často služobne v inom subjekte skupiny). Odvolávajú sa na možnosť prevziať zahraničného konkurenta, čo si bude vyžadovať veľkú transakciu. Tiež sa odvolajú na fiškálnu kontrolu v inom subjekte skupiny, ktorý vyžaduje, aby boli finančné prostriedky prevedené na tento subjekt. Možné sú aj ďalšie scenáre. V každom z nich je výslovne stanovené, že transakcia musí byť vykonaná urgentne a s maximálnym utajením.

3 Podvodníci dokonca použijú externú poradenskú firmu (ktorej identitu ukradli), aby operáciu urobili dôveryhodnejšiu. Táto poradenská firma následne kontaktuje zamestnanca vašej spoločnosti s cieľom potvrdiť transakciu a zdôrazniť utajenie a naliehavosť platby, ktorú je potrebné vykonať. Ak zamestnanec zaváha, podvodníci použijú niekoľko trikov, ako napríklad použitie mien vrcholových manažérov spoločnosti, lichôtky, dokonca aj hrozby.

Aké bezpečnostné opatrenia prijať?

- Vždy buďte opatrní, keď sa požaduje, aby boli finančné prostriedky prevedené naliehavo a tajne.
- V prípade naliehavej žiadosti vždy zavolajte späť osobu, ktorá podala žiadosť na známe telefónne číslo.
- Nikdy nedovoľte, aby tá istá osoba mala duálne podpisové právomoci (karty a čísla PIN)
- **Ďalšia ochrana:** menovať referenčného pracovníka (ktorý nie je ani generálnym riaditeľom, ani CFO), ktorý musí byť kontaktovaný pri žiadosti o dôvernú alebo naliehavú transakciu. Takáto osoba môže kontaktovať riaditeľa spoločnosti osobne, aby skontrolovala pravosť žiadosti. Pozor, takéto právomoci nesmú byť známe mimo spoločnosti.

3 E-podvody

Čo je e-podvod?
Aké sú následky?

E-podvody zahŕňajú podvody typu phishing a malware. Môžu mať dopad na vašu spoločnosť alebo osobne na váš súkromný život.

V každom prípade sa kyber zločinci pokúsia ukradnúť peniaze tým, že získajú identifikačné kódy a elektronický podpis svojej obete. S týmito kódmi prevedú peniaze na svoje účty vyprázdnením vašich bankových účtov.

Čo sa stane?

1 Dostanete e-mail, údajne od vašej banky, ktorý tvrdí, že je bezpečnostnou kontrolou, že účet bude zablokovaný, alebo že sa vykonajú zmeny v službách ponúkaných bankou. Ďalšie motívy sú možné. Zakaždým je cieľom dosiahnuť, aby ste klikli na odkaz v e-maile a presmerovať vás na falošnú identifikačnú stránku pre váš Online banking.

2 Na tejto stránke zadáte svoje inicializačné kódy, ktoré zločinci získajú, keďže sa nachádzate na ich stránke, a nie na stránke vašej banky. Pomocou kódov môžu títo zločinci vstúpiť do vášho Online bankingu a pripraviť transakcie. Za týmto účelom teraz potrebujú podpisový kód, aby previedli peniaze z vašich účtov.

3 Aby získali váš podpisový kód, budú vás telefonicky kontaktovať a požiadajú vás o vloženie karty do čítačky kariet (toto sa nazýva vishing), alebo uvidíte obrazovku, ktorá vás požiada o niekoľko minút čakania. Po uplynutí času sa objaví nová obrazovka, ktorá vás požiada o podpisový kód (dynamický phishing).

Aké bezpečnostné opatrenia prijať?

- Nikdy nedávajte nikomu svoje kódy k Online bankovníctvu. Ak vás niekto požiada o vloženie karty do čítačky a poskytnútie kódu zobrazeného na obrazovke, je to podozrivé.
- Nikdy nepodpisujte transakciu, ktorú ste sami nezadali (budete požiadaný o vytvorenie kódu s čítačkou kariet pomocou tlačidla podpisu, ktoré sa líši od identifikačného tlačidla, keď nevykonávate platbu.

Správna kontrola nad online platobnými prostriedkami

Niektoré formy firemného správania môžu uľahčiť život podvodníkom a zvýšiť riziko podvodu:

- **Nepostačujúce riadenie duálneho podpisovania:** dvojité podpisovanie je prostriedkom na odhaľovanie podvodov. Osoba, ktorá musí pridať druhý podpis, má externý pohľad na transakciu a dokáže ľahšie odhaliť podvod. Nikdy nenechávajte obidva podpisy v rukách tej istej osoby a skontrolujte, čo podpisujete.
- **Zdieľaný prístup k účtom spoločnosti:** niekedy môže byť jednoduchšie zdieľať prístup k firemnému Online bankovníctvu. Jedna osoba má prístup a zdieľa svoje kódy s kolegami. To však zvyšuje riziko podvodu a zabraňuje vám vedieť, kto bol obeťou podvodu.
- **Nesprávne použitie poverenia k účtu:** zdieľaním elektronického prístupu k účtom spoločnosti sa mandáty tiež zdieľajú. Týmto spôsobom dáte prístup aj k svojim osobným účtom. Každá osoba musí mať vlastný individuálny prístup k účtom spoločnosti. To predstavuje bezpečnosť pre spoločnosť a tiež pre danú osobu, ktorá bude mať môcť vplyv len na účty vašej firmy.

4 Fakturačné podvody

Čo je to?
Aké sú následky?
Fakturačné podvody majú mnoho podôb. Vo všetkých prípadoch zmenia podvodníci bankové údaje spoločnosti, ktorá vystavila faktúru, tým že uvedú svoje vlastné a v dôsledku toho príjmu fakturované sumy.

Čo sa stane?

1 Zločinci zachytia faktúru medzi okamihom odoslania faktúry a jej prijatím alebo hackovaním polí na odosielanie e-mailov.

2 Podvodníci zmenia faktúru tým, že na ňu uvedú svoje vlastné bankové údaje. Môžu to robiť rôznymi spôsobmi: nová faktúra je zostavená s novými údajmi, nálepkou (často fluoreskujúcou) s bankovými údajmi podvodníkov a zmienkou o zmene banky, ktoré sú uvedené namiesto skutočných bankových údajov, atď. Potom je faktúra opätovne zaslaná.

3 Faktúra je prijatá a uhradená na nové číslo bankového účtu. Je veľmi pravdepodobné, že na nesprávny účet budú uhradené aj nasledujúce faktúry, až kým skutočný vystavovateľ faktúry si neuvedomí, že ich faktúry neboli zaplatené, a obráti sa na debetnú spoločnosť.

Obmeny tohto typu podvodu

Fakturačné podvody majú niekoľkých obmien. Napríklad debetná spoločnosť dostane e-mail, zdanlivo jej dodávateľa, v ktorom je oznamovaná zmena banky a následne číslo účtu. Táto správa bude na hlavičkovom papieri dodávateľa a bude sa javiť ako legitímna. V takýchto prípadoch nie sú zachytené žiadne faktúry, ale posiela sa obyčajná správa s novými bankovými údajmi. Všetky čakajúce faktúry, ako aj následná faktúra, musia byť uhradené na nové číslo účtu.

Bez ohľadu na scenár je cieľom zločincov urobiť zmenu v tom, čo my nazývame údaje dodávateľa (telefónne číslo, bankové údaje, e-mailová adresa), aby ukradli peniaze.

Ako sa chrániť ako vystavovateľ faktúr?

Ak chcete obmedziť riziko zachytenia faktúr, zabráňte ich odosielaniu v obálke s vašim logom alebo akýmkoľvek názvom, ktorý identifikuje vašu spoločnosť.

Odporúča sa odoslať každú faktúru dvomi rôznymi kanálmi. Napríklad e-mailom a poštou. Týmto spôsobom musí byť dlžník informovaný, že musí uhradiť len v tých prípadoch, ak sú obidve faktúry rovnaké. Uvedením bankových údajov červenou farbou na faktúru môžete pred platbou uľahčiť kontrolu.

Ako sa chrániť ako príjemca faktúr?

Je veľmi jednoduché chrániť pred týmto typom podvodov prostredníctvom spätného telefonátu na potvrdenie. Každá zmena v údajoch dodávateľa (adresa, telefónne číslo, e-mailová adresa, číslo účtu atď.) musí viesť k telefónnemu hovoru na známe číslo (a nie na tel. číslo uvedené na faktúre). Takto možno rýchlo odhaliť možné podvody.

5 Na koho sa obrátiť v prípade pochybností alebo podvodu?

ING Anti-fraud officer
anti-fraud@ing.sk

Ak spozorujete pokus o podvod alebo ak došlo k podvodu vo vašom podniku, ihneď informujte vašu kontaktnú osobu v ING. Rýchlym kontaktom vašej banky zvýšite pravdepodobnosť získania odcudzených finančných prostriedkov naspäť.

Môžu byť požadované aj ďalšie kroky vo vzťahu k štátnym orgánom (podanie oznámenia na políciu atď.). Naši odborníci vám tiež môžu poradiť ktoré kroky je potrebné podniknúť.

Tento leták je ponúkaný spoločnosťou ING výlučne na informačné účely a nepredstavuje záväzok ING. V dôsledku toho nesmie za žiadnych okolností slúžiť ako základ na to, aby spoločnosť ING bola braná na zodpovednosť najmä v prípade, že vaša spoločnosť je napriek týmto odporúčaniam obeťou akéhokoľvek z podvodov uvedených v tejto brožúre.

ING Bank N.V. Bijlmerplein 888, 1102 MG Amsterdam, Holandsko, akciová spoločnosť, register Obchodnej a priemyselnej komory pre Amsterdam, spisová značka: 33031431 prostredníctvom ING Bank N.V., pobočka zahraničnej banky, Pribinova 10, 811 09 Bratislava, IČO: 30 844 754, Obchodný register Okresného súdu Bratislava I, oddiel: Po, vložka č. 130/B