Policie České republiky - podvody na internetu

Online prostředí je jako dělané pro podvodníky, kteří s obětí nemusí jednat tváří v tvář, a mají tak nekonečné možnosti, za koho se mohou vydávat. Využívají různých prostředků, aby docílili důvěryhodnosti a své postupy stále „modernizují“. Kdo by totiž nevěřil bankovnímu úředníkovi nebo policistovi, když od nich elektronicky obdrží oficiálně vyhlížející dokument? Jak by je mohl okrást někdo. Kdo si chce zboží zakoupit? Pro svoji vlastní ochranu je třeba znát, jak tito pachatelé operují a co lze od nich očekávat.

Nechcete-li se nechat okrást, měli byste vědět, že telefonní hovory od bankéřů a policistů o napadení účtu bývají zpravidla PODVOD.

Pachatelé se v rámci vishing podvodů nejčastěji vydávají za bankéře nebo jiné úřední osoby s tím, že užívají reálná jména, která lze běžně dohledat na oficiálních stránkách různých institucí. Před hovorem si často zjistí o dotyčném základní informace, aby nabyli vyšší důvěryhodnosti. Oběti kontaktují s legendou napadení jejich bankovního účtu a naléhají, že je potřeba co nejdříve převést prostředky na zabezpečený účet, aby o své peníze nepřišly. Bankéř tak vyzve svého „klienta“, aby nejprve v hotovosti vybral veškeré své finanční prostředky z běžného, případně i spořícího účtu, poté, aby si online vyžádal před schválený úvěr a hotovost, pak vložil do vkladomatu na virtuální měny dle poslaných instrukcí. Peníze mohou vylákat i v rámci chatovacích mobilních aplikací, kdy zasílají obětem velké množství QR kódů, které slouží, jako příkaz k transakci.

Aby pachatelé vypadali věrohodněji, používají tzv. spoofing, při kterém dokáží napodobit jakékoliv telefonní číslo, třeba právě i infolinku banky. Celou legendu následně doplní falešný policista, který doporučí s bankéřem spolupracovat a s nikým jiným o hovorech nemluvit. Na každý útok mají předem vytvořené velké množství dokumentů, kterými jsou tiskopisy, tvářící se, jako oficiální dokumenty vytvořené bankou či policií. Pachatelé jsou velmi přesvědčiví a manipulativní, sofistikovaně ovládají češtinu a bankovní terminologii. Také v těchto případech se způsoby páchání posouvají stále kupředu. Policie se setkává i s případy, kdy pachatel poté, co okrade svoji oběť, shodí masku bankéře a vyžaduje po ní intimní fotografie výměnou za vrácení peněz.

Dalším způsobem, jak se podvodníci snaží podvést důvěřivé lidi:

- Lákají na investice do kryptoměn s nadprůměrným zhodnocením vložených finančních prostředků
- Investování do známých společností
- Využití inzerátu k prodeji zboží – podvodník projeví o zboží zájem, domluví se s prodávajícím, kterému zašle email s odkazem na přepravní společnost – například PPL, DHL atd. V emailu je umístěný internetový odkaz, který po vyplnění platební karty a přístupových údajů k bankovnictví je podvodníkem zneužit a poškozený je okraden.

Jak se bránit:

- neumožňujte nikomu převod finančních prostředků přes Váš bankovní účet.
- i když se veškeré okolnosti tváří, že jednáte s oficiální institucí, zbystřete. Banky po Vás nikdy nebudou žádat provedení převodu, výběr z Vašeho účtu v rámci zabezpečení či vkládání finančních prostředků do vkladomatů na kryptoměny.

- nikomu neposkytujte vzdálený přístup do Vašeho zařízení, a to i když se jedná o osobu, kterou znáte nebo o bankovní instituci.
- pokud podvodný hovor již přijmete, neváhejte si ho poznamenat a následně se s těmito podklady obraťte na svoji banku nebo na policii.
- dávejte si pozor při prodeji Vašeho zboží, pokud Vám chce někdo zaplatit, stačí mu číslo Vašeho bankovního účtu, nepotřebují další údaje k číslu platební karty a kódu platební karty.
- nenechte se do ničeho tlačit, raději obchod s dotyčným neuskutečněte.

Buďte opatrní, chraňte si své peníze!

npor. Mgr. Milan Horníček
vedoucí obvodního oddělení Lanškroun