Podvodníkům na telefonu se daří i dál. Jak nenaletět na metody zvané vishing či spoofing?

11.10.2023 - Petr Lesenský | Dýcháme

Přestože policie i finanční instituce opakovaně varují před telefonáty podvodníků vydávajících se za zástupce bank a dalších organizací, zločinů daného typu kontinuálně přibývá. Průměrná výše odcizených částek zároveň podle dat kriminalistů sahá zhruba k 400 tisícům korun, výjimkou však nejsou ani milionové krádeže. Nechat se napálit je stále snadnější, neboť podvodníci pravidelně zdokonalují své postupy.

Jen v roce 2022 řešili policisté v České republice v souvislosti s kyberkriminalitou přes osmnáct a půl tisíce případů. Oproti předchozímu roku jde o prakticky stoprocentní nárůst. Řadu případů přitom lidé vůbec nenahlásí. Vedle internetových podvodů ve velké míře bují i ty telefonické. Mezi relativně nové metody zlodějů se řadí například takzvaný vishing či spoofing.

„Vishing je typ podvodného volání, které se z člověka snaží vylákat citlivé údaje či jej rovnou přimět k převodu peněz. Útočníci se často vydávají za bankéře, makléře či policisty a využívají různé formy psychologického nátlaku, aby oběti dostali tam, kam potřebují,“ přibližuje **Jan Nedělník**, ředitel společnosti Konecta Czech a Hungary, která se specializuje na outsourcing zákaznických služeb.

Falešný bankéř či investiční poradce

Typickým příkladem, před nímž v letošním roce již řada bank své klienty varovala, je scénář, v rámci kterého se podvodníci snaží u lidí navodit dojem, že jsou jejich finance v ohrožení. Útočník se obvykle představí jako pracovník banky a informuje volaného, že jeho účet byl napaden. Jediným východiskem z dané situace má být odeslání financí na bezpečný účet či jejich vložení do bezpečného bankomatu.

Kromě falešného bankéře oběti často kontaktuje i další komplic vydávající se typicky za policistu. Realističnost celého podvodu mnohdy zloději ještě zdokonalují použitím metody známé jako spoofing, kdy dokážou napodobit jakékoli jiné telefonní číslo. Člověku se tak na mobilním telefonu skuteční zobrazí, že mu volá policie či jeho banka.

„Triky a vyjednávací techniky podvodníků jsou velmi propracované. Zdařile napodobují chování zaměstnanců klientského centra a umí si klienta pod záminkou falešného bankéře, zástupce vybrané instituce či bezpečnostního experta získat na svoji stranu,“ doplňuje **Petr Zíma**, manažer České spořitelny pro klientskou bezpečnost a bankovní identitu.

Neustále se zvyšující úroveň dovedností útočníků potvrzuje i **Marek Macháček**, expert na prevenci platebních podvodů v Komerční bance. *„Řešil jsem případ, kdy útočník napsal e-mail s pomocí umělé inteligence, která okopírovala styl nadřízeného z korespondence dostupné na internetu. I on sám následně říkal, že by podle použitých slovních obratů uvěřil, že to sám napsal,“* uvádí.

Na hesla se banka nikdy neptá

Základem toho, jak podvodníkům neskočit na jejich finty, je být ostražitý. *„Bankovní společnosti za žádných okolností nežádají po klientech citlivé údaje, jako jsou hesla, CVV kódy a podobně. Pokud k takové situaci během hovoru dojde, jedná se s vysokou pravděpodobností o podvod,“* varuje Jan

Nedělník.

V momentě, kdy se člověk cítí pod tlakem či si zkrátka v dané situaci není jistý, měl by telefonát raději ukončit a vzít si čas na rozmyšlenou. Veškeré obdržené informace si může následně nechat ověřit u své bankovní společnosti či jiné instituce. *„Pokud má náš klient během hovoru s kolegy z kontaktního centra jenom stín pochybnosti o tom, jestli mu skutečně volá někdo z banky, vždy klientovi doporučujeme hovor ihned ukončit a neprodleně nám zavolat na naši blokační linku,“* doporučuje **Jana Pokorná**, tisková mluvčí pro Air Bank.

V momentě, kdy dotyčný zjistí, že podvodníkovi naletěl, je nezbytné co nejrychleji kontaktovat svoji banku. V některých případech lze ještě transakci včas zastavit a finance klienta ochránit.

https://www.dychame.cz/podvodnikum-na-telefonu-se-dari-i-dal-jak-nenaletet-na-metody-zvane-vishing-ci-spoofing