Podvodníci se vydávají za zaměstnance bank či dokonce i policisty

KRAJ - Policisté v Libereckém kraji zaznamenali již desítky těchto případů.

Podvodníci využívají metodu tzv. vishingu, při níž se volající člověk vydává za pracovníka banky a přesvědčí jejího klienta, aby své peníze převedl z vlastního účtu na jiný. Pachatelé při hovorech užívají tv. spoofing, to znamená, že dokážou napodobit jakékoliv telefonní číslo včetně infolinek bank a nyní dokonce i Policie ČR.

Podvodníci osloveným klientům bank tvrdí, že zjistili napadení jejich účtu. Tito domnělí pracovníci banky svými tvrzeními vystraší osobu, které volají, přičemž jejich hlavním cílem je získat její peníze. Sdělí, že je nutné, aby finanční prostředky byly z vlastního účtu okamžitě převedeny na jiný účet, který jim sdělí, s tím, že budou po vyřešení celé věci následně vráceny, což se samozřejmě nestane.

Pachatelé také mohou tímto způsobem vylákat z oběti podvodu i další citlivé údaje, které následně zneužijí.

Aby to vše vypadalo ještě důvěryhodněji, přišli na další trik, kdy klientům sdělí, že jejich případem napadení účtu se již zabývá kriminální policie a že je bude v následujícím telefonátu policista kontaktovat. Skutečně jim vzápětí zavolá "podvodný policista", aby dokázal tu svou legendu. Působí to vše velmi věrohodně. Jednou z metod těchto podvodů je, aby člověk jednal rychle, okamžitě a mnohdy ve stresu. Umí využít manipulativní techniky, kdy člověka zastihnou někde v obchodě, v zaměstnání, kde není v klidu a dostanou ho do stresu. Vše působí profesionálně. Zavolá člověk, který se tváří, že je z nějakého coll centra, za ním je skutečně slyšet nějaký ruch a další hlasy a navíc se odvolává na policistu, který skutečně zavolá. Většinou při tom podvodníci využívají reálná jména i reálné útvary. A také reální čísla coll centra bank nebo Policie ČR, která skutečně existují.

Česká bankovní asociace zaznamenává i další případy, které se týkají dalších scénářů. Opět kontaktuje zaměstnanec banky klienta s tím, že jsou jeho peníze na účtu v ohrožení. Přinutí člověka veškeré peníze vybrat, pošlou mu QR kód, a prostřednictvím tohoto kódu dále vložit do tzv. bitcoinového bankomatu. I zde jsou peníze nenávratně pryč.

Nechybí ani další scénář, kdy pracovník banky nabídne klientovi, že vše společně vyřeší na dálku. Klient dá útočníkovi vzdálený přístup do jejich PC, kdy podvodníci požadují instalaci programů AnyDesk a TeamViewer pro získání vzdáleného přístupu k počítači, čímž jim lidé nadiktují i přístupové údaje nejen k jejich počítači, ale nakonec i do internetového bankovnictví.

Pokud člověk informuje banku ihned poté, co se mu něco takového stalo, je ještě reálná šance, že banka muže transakci zastavit.

Kde berou podvodníci telefonní čísla? Dochází k úniku například ze sociálních sítí nebo i z různých e-shopů, kde lidé například v minulosti platili za objednané zboží.
Žádná banka se svými klienty nikdy nejedná tímto způsobem. Nikdy po klientovi nemůže chtít přístupové údaje k bankovním účtům, hesla, PIN kódy. To vše jsou údaje, která se nikomu nesdělují, a to ani v této době, kdy se kvůli pandemii omezují osobní kontakty a komunikace probíhá telefonicky či psanou formou.

Preventivní rady, jak se zachovat:

- Nereagujte na podobné hovory a v žádném případě nesdělujte k Vaší osobě žádné citlivé údaje ani bezpečností údaje z vaší platební karty, nebo přístupové údaje k online bankovnictví.
- Nikdy nikomu nesdělujte a ani nepřeposílejte bezpečnostní / autorizační kód, který Vám přišel formou SMS zprávy.
- Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu.
- Nikdy nikomu podezřelému neumožňujte vzdálený přístup do Vašeho počítače.
- Sledujte a pečlivě čtěte informace od Vaší banky v internetovém bankovnictví.
- Při každém vstupu do internetového bankovnictví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje.
- Aktualizovat software, antivirový program, firewall.
- Buďte neustále ostražití, protože i vy se můžete stát cílem podobného podvodného jednání.
- Během, nebo po takovémto podezřelém hovoru, si zaznamenejte údaje, které Vám útočník sdělil (jména, e-mailové adresy, čísla účtů, odkazy na webové stránky, apod.)

Apelujeme na veřejnost, aby lidé nereagovali na obdobné telefonní hovory, SMS zprávy, e-maily, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další kroky pro jejich záchranu. Kdyby byly vaše peníze v ohrožení, tak banka sama zareaguje a učiní další opatření. Pokud se vám již skutečně něco podobného stalo nebo stane, věc bezprostředně oznamte na Policie ČR prostřednictvím bezplatné tísňové linky 158 nebo na kterékoliv policejní služebně a informujete svůj bankovní ústav.

4. 6. 2021

kpt. Bc. Vladimíra Šrýtrová

koordinátorka prevence KŘP Libereckého kraj