Desatero kyberbezpečnosti #4

Vishing aneb podvodníci telefonují

Ve čtvrtém článku z tohoto cyklu kyberbezpečnosti se dozvíte, co to je „Vishing“, jak útočníci využívají sociálního inženýrství s cílem vylákat z oběti citlivé osobní nebo platební údaje, a jak se účinně bránit proti těmto sofistikovaným útokům.

Jak takový útok probíha?

- Zazvoní telefon. Číslo nemáte uložené, ale je vám povědomé. Zvednete to a představíte se.
- Ozve se neznámý hlas. Představí jako pracovník bezpečnostního oddělení vaší banky a sdělí vám, že právě zachytili pokus o převod velké částky z vašeho účtu do zahraničí a chce si ověřit, jestli jste ho opravdu provedli vy coby majitel účtu. Popřete to a docela se vylekáte.
- Volající řekne, že se to tedy pokusí zablokovat (snad se to ještě stihne, proč jste nevzal telefon dřív) a požaduje pár údajů, aby si ověřil, že mluví skutečně s vámi.

V šoku odpovídáte a sdělujete své jméno, datum narození, číslo bankovního účtu a přihlašovací jméno. Chvíli slyšíte jen klapání klávesnice a pak "Tak se to podařilo". S úlevou pokračujete v rozhovoru, který se stočil na téma "A tušíte, jak se vám mohli dostat do účtu, nemáte moc slabé heslo? To by pak totiž byla vaše vina". S úlevou se rozpovídáte o kvalitě svého hesla a vyhláskujete ho. Druhá strana uzná, že chyba nemůže být na vaší straně. Požádá ještě o vaši autorizaci storna nadiktováním autorizačního kódu. Za chvíli opravdu přijde SMS, kterou přečtete a volající zavěsí. Za chvíli dostanete z banky SMS s informací o změně zůstatku na účtu – aktuální zůstatek 0,- Kč. Naletěli jste.

Co bylo na tom rozhovoru špatně?

Byl v pořádku až do chvíle, kdy po vás volající začal požadovat řadu citlivých osobních informací. Vše to byly údaje, které skutečná banka zná a nemusí je po klientovi chtít. Skutečný pracovník banky by v tu chvíli řekl jen "děkuji, transakci jsme stornovali a váš účet jsme zablokovali, aby se do něj útočníci nedostali. Zajděte si prosím s občanským průkazem do nejbližší pobočky, kde vám nastaví nové přihlašovací údaje".

Vaší největší chybou bylo samozřejmě své citlivé informace prozradit. Ale také jste si neověřili, že volající je skutečně tím, za koho se vydává.

Volajícímu se podařilo vás zmanipulovat. Jaké techniky použil?

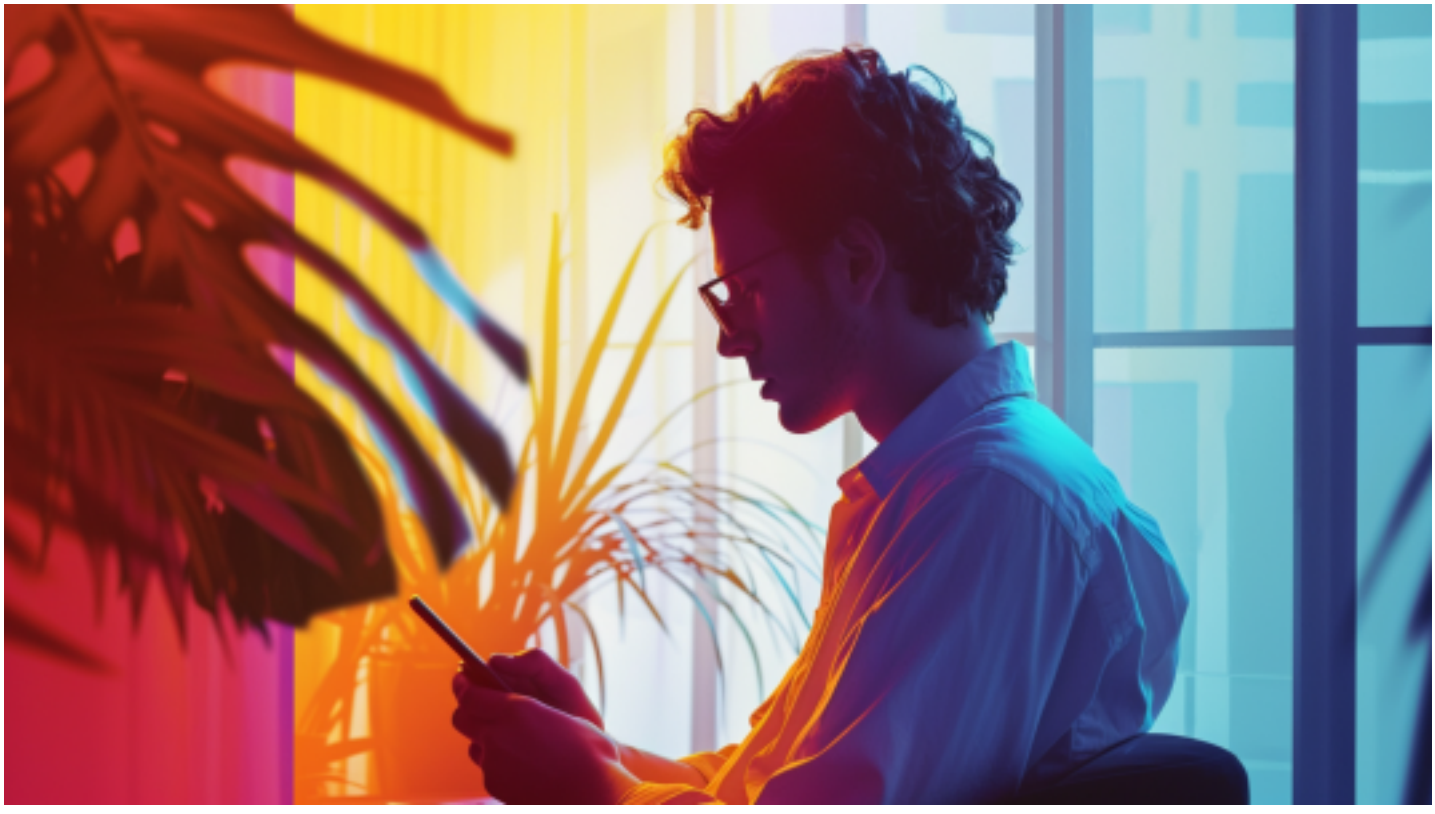
1. Zfalšoval číslo volajícího – na displeji telefonu bylo skutečné telefonní číslo banky, za kterého vám nedávno volali. Ano, je to tak. Telefonní číslo volajícího jde podvrhnout – stejně jako jméno odesílatele v e-mailu.

2. Představil se jako autorita – v tomto případě jako pracovník bezpečnostního oddělení, ale také podvodník může tvrdit, že je policista, asistent vašeho nadřízeného apod.

3. Dostal vás do stresu hrozbou velké finanční ztráty.

4. Vyvolal pocit časové tísně (snad se to ještě stihne, proč jste nebral telefon...).

Jak se takovému útoku bránit?



1. Nenechte se vystresovat údajnou časovou tísní nebo hrozící škodou. Následky chybného jednání mohou být větší, než údajná "hrozba".

2. Zamyslete se, jestli volající opravdu potřebuje citlivé informace, které požaduje nebo proč by si akci, kterou po vás chce, nemohl udělat sám. Hlavně správce počítačové sítě rektorátu NIKDY nebude potřebovat, abyste mu řekli své heslo. A když dostanete služební notebook, program TeamViewer pro vzdálenou správu už na něm je.

3. Pokuste se ověřit, že je volající skutečně tím, za koho se vydává. Ideální samozřejmě je, pokud ho znáte osobně a poznáte ho s jistotou po hlase. Nesmíte se spolehnout na to, že jde o známé telefonní číslo, může být podvržené.

Pokud vám volá **"pracovník podpory počítačové sítě rektorátu"**, můžete zavěsit, ověřit si číslo volajícího (a jméno a funkci) v adresáři univerzity https://whois.cuni.cz a zavolat mu zpátky. Nebo si celou věc ověřit na telefonním čísle podpory (224 491) 555.

Pokud vám volá **"banka"** a chce pro ověření vaše datum narození nebo rodné číslo, požádejte o ověření přes bankovní aplikaci. To proběhne podobně jako potvrzení platby kartou – v aplikaci se objeví výzva pro potvrzení hovoru z banky s uvedením tel. čísla, jména volajícího a PINem, který vám na požádaní do telefonu přečte.

Pár příkladů možných podvodných telefonátů

Všimněte si manipulace – zaštítění autoritou a nátlaku vyvolaném časovou tísní a hrozbou něčeho nepříjemného.

? Tady pracoviště Podpory. Někdo se vám dostal do mailu a teď si stahuje vaše e-maily. Musíte si okamžitě změnit heslo. Nadiktujte mi své stávající heslo a potom dvakrát nové.
? Tady pracoviště Podpory. Máte plnou schránku a ztrácí se vám e-maily. Mám vám ji zvětšit? Aby nedošlo k omylu, řekněte mi prosím ještě své číslo osoby. Děkuji. Potvrďte mi to prosím ještě svým heslem.
? Tady XY, nový asistent pana rektora. Přeje si, abych mu zpracoval stav řešení projektů a potřebuji vaše heslo, abych se k úložišti vašeho odboru dostal... Ne, nemůžete s ním mluvit, má jednání a nechce být rušen. A musí to být hotové, než skončí jednání. Mám mu říct, že jste to sabotoval? Děkuji. Hezký den.
? Nadporučík Bouda, Krajského ředitelství Policie v Ruzyni. Dostali jsme z Interpolu informaci, že z vašeho počítače, u kterého zrovna sedíte se distribuuje dětská pornografie a právě teď je to aktivní. Podle §83 vás vyzývám ke spolupráci. Nainstalujte si okamžitě na počítač program, přes který naši specialisté zkontrolují váš počítač. Nebudete-li spolupracovat, budete obviněn z šíření dětské pornografie a informujeme o tom vašeho zaměstnavatele.

Chcete-li se o tématu kyberbezpečnosti dozvědět více, navštivte web Kyberbezpečnost na Univerzitě Karlově .

Autor článku:
Ing. Vladimír Horák, vedoucí CSIRT (Computer Security Incident Response Team)

Pokud máte k článku připomínky, korektury, nebo dotazy, kontaktujte nás prosím na e-mailu: internikomunikace@ruk.cuni.cz .