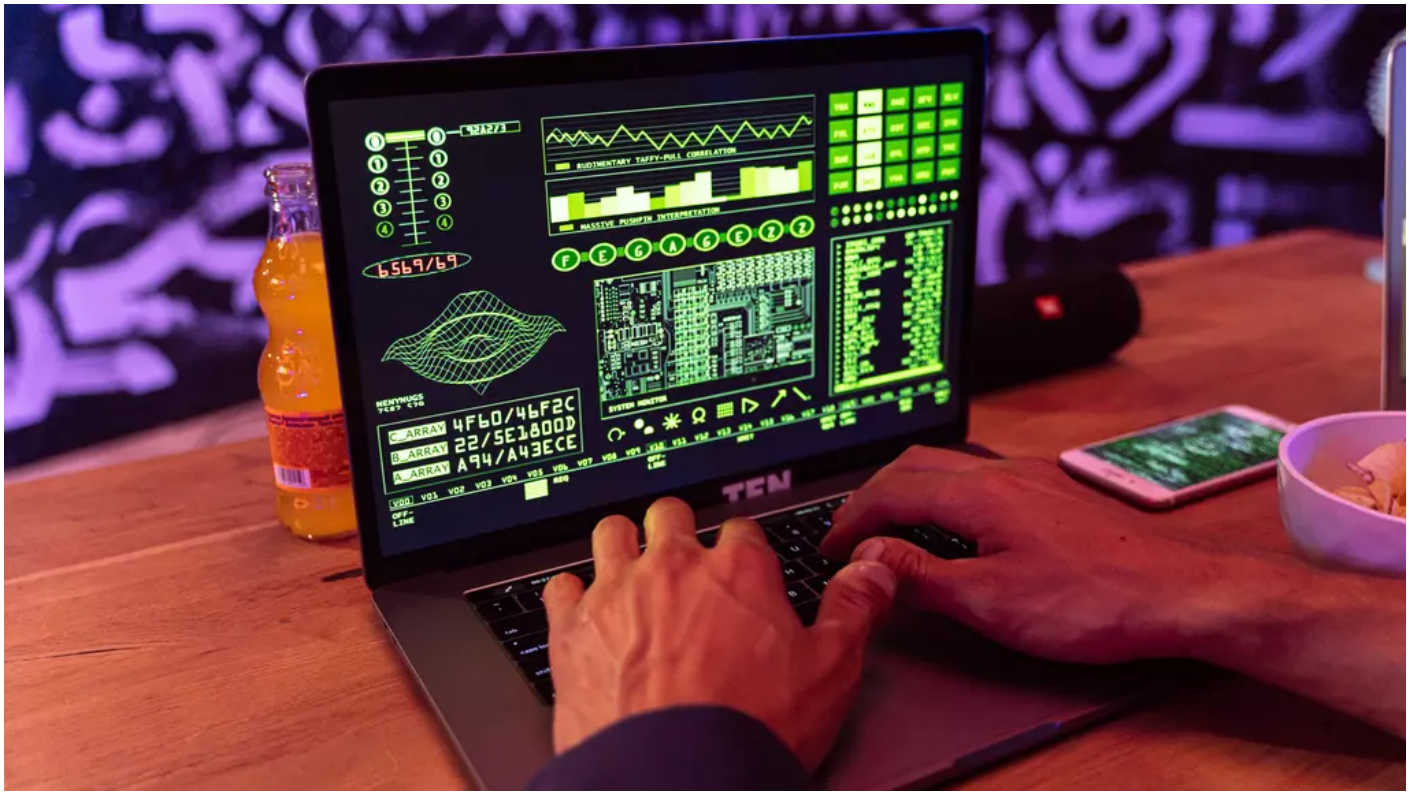
Nový typ kybernetického podvodu vám vyprázdní celý účet

By Lenka Peterková ⋮⋮ 5. 4. 2023



Zločinů v kyberprostoru přibývá. K vykradení peněz z banky nepotřebují dnešní zločinci zbraně, masky a ani odvahu. Stačí znalost a drzost. Nový způsob internetového podvodu dokonale vykresluje tři hlavní slabiny na straně poškozeného. Následující řádky tedy nechť nejsou pouhým varováním před novým typem útoku, ale také univerzálním popisem celého procesu. Ten vždy využívá technické neznalosti, psychologii a bohužel, jak si ukážeme, i slabých míst u samotných bank. Nový způsob útoku je skvělou ilustrací všech tří slabin a popíši ho na reálném příkladě z blízkého okolí.

Kamarád chtěl prodat atypickou vanu, které se mu nějakou dobu válela zabalená v garáži a neměl pro ni využití. Dal si inzerát. Brzy mu přišla poptávka. S „kupcem“ komunikoval přes messenger. Kupec se zeptal, jestli je vana volná a když obdržel kladnou odpověď ihned řekl, že má zájem. Peníze že pošle hned na účet, jehož číslo si od kamaráda vyžádal. Následně se kamaráda zeptal, zdali mu nemůže poslat vanu

přes Balíkovnu. Kamarád reagoval, že netuší, jak se taková věc realizuje. Obdržel screenshot ze stránek Balíkovny s vysvětlením, že si stačí zřídit u Balíkovny účet, že oni si vanu vyzvednou, zabalí, odešlou. Ať jen pošle telefon a e-mail. Kamarád souhlasil. (Screenshot byl montáží skutečné stránky se smyšlenou nabídkou služeb vyzvednutí u zákazníka a zabalení.)

Zde první zastávka – psychologická. V tomto způsobu podvodu je poměrně „geniálně“ nastavená komunikační situace ve prospěch zločince a obroušená ostražitost oběti. Vy totiž prodáváte zboží, nikdo po vás nechce žádné tajné údaje – jen číslo účtu, e-mail a telefon – a ještě vám řekne, že zaplatí předem a vy zboží odešlete až uvidíte peníze na vašem účtu.

Zpět k událostem. Následně zájemce kamarádovi napsal, že je třeba účet u Balíkovny potvrdit a instrukce z Balíkovny, že má v e-mailu. Krátká technická odbočka. Technologicky průměrně znalý uživatel by už zde dále nešel, a to z několika důvodů. Z hlavičky e-mailu je totiž jasné, že neodešel z domény balikovna.cz, následující stránky jsou samozřejmě také podvržené, což lze odhalit z url adresy. Bohužel, běžný uživatel nemá o těchto věcech tušení a hlavně – opět psychologie – není to o penězích. Chcete přece jen poslat balík, nikdo po vás nechce žádné platební údaje. Co stránka skrytá za odkazem v e-mailu udělá ve skutečnosti – a tady bohužel neznám přesnou funkcionalitu, tyto stránky přestanou po úspěšném útoky fungovat – je, že se pokusí získat další důležitý střípek (nebo spíše střep) k ovládnutí vašeho účtu. Na podvržených stránkách se nachází informace, že zřízení účtu je třeba potvrdit kódem, který vám právě přišel z technické podpory aplikace Balíkovna.

Tento kód vám přijde ve skutečnosti z vaší banky a je to PIN pro instalaci Smart klíče, nebo analogického produktu vaší banky, na nové zařízení. Žádost o něj vygeneroval útočník na svém zařízení pomocí vašeho e-mailu a čísla telefonu. Co máte za banku ví z čísla vašeho účtu také. Mezi tím vaši pozornost upoutává konverzace s nakupujícím, který vás ochotně informuje a odvádí pozornost. Následující krok, vložení potvrzujícího kódu, už opravdu žádá velkou míru nepozornosti a opět je tu ve hře kombinace neznalosti uživatele a psychologie. A také, poprvé, nedostatečná komunikace ze strany banky.

Banka z hlediska technologické části zabezpečení udělá přesně to, co má. Pošle vám kód na váš mobilní telefon. Ale bezpečnost není pouze technologická část, ale i ta komunikačně psychologická a zde banky zaostávají naprosto kruciálně. A přitom by stačilo opravdu velmi málo. Usuďte sami. SMS z banky kamaráda zní: „CSOB SMS

klic: Pro první prihlaseni a vstup k nastaveni prihlasovacích udaju pro uzivatele xxx pouzijte kod xxxxx. Vase CSOB.“ Ano, v sms jsou všechny potřebné informace, jasně je tam psáno, že je to od ČSOB, ale znovu se vraťme k celé komunikační situaci. Prodáváte vanu, chcete jen poslat balík, vše časově sedí, stránka si prostě vyžádá ověřovací kód, do toho vám píše zájemce, jestli je vše v pořádku, že už by poslal peníze…. Kopírujete kód a vkládáte ho do aplikace „Balíkovny“

A teď si představte, kdyby zpráva zněla nějak takto. „Posíláme kód k aktivaci autentizační aplikace pro přihlášení do vašeho elektronického bankovnictví, která umožní úplný přístup k vašemu bankovnímu účtu! Nikdy ho nezadávejte jinam než do aplikace elektronického bankovnictví na vašem mobilním telefonu. Máte-li sebemenší pochybnosti, volejte na číslo ….. Váš kod je ….“ Takto málo by stačilo, aby i neznalý uživatel i v této komunikační situaci zpozorněl.

Jděme dál. Banka samozřejmě následně zasílá na e-mail ještě aktivační link. Zde už fungují staré triky. Kupec vám napíše, že aktivace účtu z neznámého důvodu neprošla a že vám přišel e-mail od technické podpory s potvrzujícím odkazem. Ten samozřejmě přijde znovu z banky. Funguje zde úplně stejný trik, jako v předchozím kroku. E-mail sice přijde z banky, a opět máte další příležitost se zamyslet, co se to vlastně děje, ale – jste ve vleku procesu, nikdo po vás nechce žádná hesla, čísla karet, tzn. nerozsvítí se bazální varovná kontrolka na pozadí. Klikáte na odkaz..

Pochybení banky č. 2 je úplně stejné jako v prvním případě. E-mail zní: „Dobrý den, pro dokončení aktivace ČSOB Smart klíče klikněte na odkaz níže.“ Pro člověka analogového věku, staršího ročníku, živícího se řemeslem je to totální technologické ptydepe. Kde je nějaké upozornění na to, co vlastně děláte? Varování?

V tuto chvíli má lupič, skrze smart klíč nainstalovaný na svém zařízení plný přístup do vašeho elektronického bankovnictví. Ke cti banky nutno říci, že následně dorazila další zpráva. Tentokráte již poměrně srozumitelná, i když také by mohla být napsána lépe: „Upozorneni: Prave jste uspesne aktivovali novou aplikaci Smart klic. Pokud jste to nebyli vy, neprodlene nas kontaktujte na tel…“ Kamarád nezareagoval ani na takto explicitní varování. Proč? Opět psychologie – právě jste úspěšně aktivovali známou službu na odesílání balíků Balíkovna (mozek vám to nějak okecá – ČSOB – Balíkovna, nemusím rozumět všemu, nebudu trapnej, že něčemu nerozumím…), kupec vám do toho píše, že je vše ok a ať nic neposíláte dříve, než od něj neuvidíte na vašem účtu peníze, že během tří hodin dorazí.

Chvíli po tomto však přišla kamarádovi notifikace z banky, která mu oznamovala, že mu byl navýšen finanční limit pro odeslání transakce. To už kamarád pochopil, že je něco špatně a volal okamžitě do banky. A zde pochybení banky č. 3 a to zásadní.

Volali jste někdy poslední dobou do nějaké bankovní instituce? Pokud ano, tak asi víte, že proklikat a prokřičet se hlasovým automatem a donutit chatbota, aby vás přepojil na živého člověka je někdy prakticky nemožné. Kamarádovi to trvalo skoro 30 minut. Stres, strach atd. v této situaci určitě nejsou urychlujícím faktorem. Z výpisu hovoru a odchozích transakcí jasně vyplývá, že pokud by se kamarád dovolal ihned, žádné peníze by mu z účtu neodešly. Takto měl štěstí v neštěstí. Navýšení limitu už lupiči nestihli, a tak přišel sice o dost peněz, ale mohlo to být násobně více. U výslechu u policie se dozvěděl, že je jediný, kdo vůbec u úspěšného útoku tohoto typu zareagoval aspoň takto „včas“. Od úplné katastrofy ho zachránil nastavený menší limit na odchozí transakce.

Rada(y) na závěr

1. Moderní technologie jsou zrádné v tom, že je může používat každý a při tom často vůbec netušíme, jak fungují. Vyplatí se proto princip předběžné opatrnosti. Pokud si nejsem jist tím, co dělám, je lepší to nedělat vůbec.

2. Než na něco kliknu nebo někam vložím jakýkoliv kód, dvakrát si pozorně přečtu, na co klikám, kdo mi to posílá. Mám-li sebemenší pochybnost, že něco nesedí, končím. Dva tři nádechy navíc před každým úkonem nám mohou ušetřit hodně trápení.

3. Rada pokročilejší. Pokud mi někdo pošle e-mail za nějakou známou službu, ověřím, jestli je to opravdu ona. Tzn. podívám se na adresu odesílatele, jestli je e-mail z domény služby, za kterou se vydává. Viz dále. (Někdy to může být těžší, protože v případě sofistovanějších útoků to zjistím až z hlavičky e-mailu, která je skrytá – samotná adresa, kterou vidím v řádku od, může vypadat v pořádku). Kde je to už jednodušší, je na samotných stránkách – zde třeba podvržené stránky balíkovny. V tomto případě stačí do vyhledávače zadat Balíkovna a nechat si načíst oficiální stránky. V adresním řádku si nechám zobrazit celou adresu. Uvidím: https://balikovna.cz nebo https://www.balikovna.cz Důležitá je ta část před poslední tečkou značící národní doménu. Před ní musí být vždy balikovna. (to co je za případným následným lomítkem již není důležité) Tzn. pokud je na stránce kam jsem odkázán adresa třeba www.balikovna.cz.servis-baliku.cz – tak skutečná doména, kam jsem byl přesměrován je servis-baliku.cz – nikoliv balikovna.cz. V takovém okamžiku vím, že nejsem na

oficiálních stránkách. Triků s adresou je více. Jako třeba: balikovna.cc (jiný identifikátor národní domény) nebo třeba ballikovna.cz. To je zákeřné, zdvojeného l si už nemusíme všimnout. Řádná kontrola je ale potřebná.

4. Jakékoliv údaje, které nám přijdou z naší banky, nejsou nikdy určeny ke vkládání a posílání do žádných dalších služeb!

5. Nenechat se zahnat do pocitu, že jsem moula, že něčemu nerozumím atd. Prostě mám pochybnost, končím.

PS:

Popis podvodu sem dávám se svolením kamaráda. Přál si, aby jeho případ pomohl ostatním.