Digitálna bezpečnosť

Keď sa ohliadneme za uplynulým rokom so zreteľom upriameným na rozvoj technológii, tak aj výrok, že napredujú míľovými krokmi je už zastaraný. Vývin, aktualizácia, nástup nových technológii vykazujú exponenciálny rast. Spolu s nástupom nových technológii aj v oblasti elektronického bankovníctva, platobných nástrojov prichádzajú tiež nové bezpečnostné riziká, ktoré sa týkajú hlavne odcudzenia dôverných informácii (záujem je o informácie akéhokoľvek druhu, ale najčastejšie prístupové heslá, kódy k platobným nástrojom, databázam s osobnými údajmi, dôverným komunikáciám, informáciám o našom prehliadaní webu, online návykoch a iné.) Tieto informácie dokážu útočníci potom zneužiť buď priamo na prístup k našim financiám, alebo sa nás prostredníctvom nich potom pokúšajú vydierať a obohatiť sa výmenou za nezverejnenie informácii, ktoré nám odcudzili, alebo sa o nás dozvedeli. Nepríjemný a znepokojivý, ale hlavne rastúci je aj trend, ktorý zaznamenáva presun záujmu kyberútočníkov od veľkých nadnárodných spoločností, štátnych/vládnych organizácii k úplne obyčajným, bežným používateľom internetu.

V nasledujúcom texte sa budeme venovať najčastejším typom kyberútokov, ktoré sú veľmi bežné aj u nás, popíšeme si taktiku útočníkov ale tiež návod, ako sa takýmto online útokom čo najefektívnejšie vyhnúť, ako ich rozpoznať.

Phishing

Je typ útoku cez e-mail, kedy dostanete e-mail, zdanlivo od vašej banky, prípadne z rozhrania PayPal, prípadne Apple, či Amazon účtu. Táto správa vás vyzýva na prihlásenie do vášho účtu, obyčajne je podporená tvrdením, že ste boli odhlásení, prípadne, že na váš účet prichádza väčšia transakcia, ktorú treba autentifikovať. V skutočnosti vaše prihlasovacie údaje po takomto prihlásení putujú do databáz falošných stránok, ktorých úlohou je takéto údaje zhromaždiť a poskytnúť útočníkovi. Existujú tiež varianty phishingu, kde riziko nie je priamo v e-maili, ale v jeho prílohe – súbore, ktorý sa môže tváriť ako zľavový kupón, alebo dotazník, ktorý treba vyplniť. Takáto príloha však obsahuje vírus, ktorý dokáže identifikovať vaše prihlasovacie údaje a odcudziť ich.

Ako takýto útok odhaliť?
Majte na pamäti:

Banka si nikdy či už prostredníctvom e-mailu, sms alebo telefonicky nepýta citlivé údaje o internetbankingu (prihlasovacie meno, heslo, údaje na potvrdenie transakcie), platobnom účte alebo platobnej karte (číslo karty, platnosť karty alebo CVV kód), ani nevynucuje inštaláciu žiadnej mobilnej aplikácie alebo programu do počítača a mobilného zariadenia. Zlatým pravidlom je, že na takúto požiadavku by klient nikdy nemal reagovať, ale okamžite na to upozorniť banku cez zákaznícku linku.

Sú dva možné spôsoby, ako tento útok odhaliť:

1. Pozrite sa, ako je e-mail adresovaný, ako Vás odosielateľ oslovuje. Phisheri väčšinou používajú všeobecné oslovenie, ako “Milý pane, pani”, "Vážený zákazník". Pravý e-mail by mal obsahovať vaše meno, napr. “Milý pán Vážny…”.
2. Skontrolujte adresu, z ktorej bol e-mail odoslaný. Útočníci nedokážu odoslať e-mail z domény vašej banky (napríklad: noreply@tvojbank.sk), podozrivá adresa odoslania obsahuje reťazce čísel a znakov (napríklad: noreply@12sa34Tvojbank.sk), nezriedka obsahuje aj gramatické chyby.

Čo robiť/nerobiť?

Nikdy neklikajte na takéto podozrivé odkazy v e-mailoch. Ak máte pocit, že by naozaj mohol na vašom bankovom účte nejaký problém, na ktorý vás takáto pošta upozorňuje, skontrolujte svoje bankovníctvo cez zaužívaný prístup - oficiálny internetbanking, prípadne mobilnú aplikáciu.

Pharming

Je útok podobný phishingu, len namiesto e-mailovej komunikácie cieli priamo na stránku, na ktorej sa prihlasujete prostredníctvom citlivých údajov. Napíšete správnu webovú adresu, ale v okamihu ste, bez toho aby ste si to uvedomili, presmerovaní na falošnú verziu danej stránky, na ktorej sa identifikujete svojimi prihlasovacími údajmi. A to je všetko, čo od vás útočník potrebuje.

Ako takýto útok odhaliť?

Musíte byť opatrní pozorovatelia. Podvodníci sú často majstri v napodobovaní vzhľadu pôvodnej stránky, takže často je na nerozoznanie od tej skutočnej. Sústreďte sa hlavne na riadok webovej adresy. Ak sa nezobrazuje ako obyčajne (napr. https://banka.sk), ale ako reťazec čísel a znakov, prípadne je podobná, len s poprehadzovanými znakmi, prípadne s chybami, jedná sa o pascu na vaše peniaze.

Čo robiť/nerobiť?

Pri prihlasovaní do vašich účtov (elektronické bankovníctvo, PayPal) vždy sledovať riadok s webovou adresou stránky, aktualizovať si operačný systém a hlavne internetové prehliadače, odborníci tiež radia zadovážiť si a pravidelne aktualizovať anti-vírusový software.

Vishing

Je telefonický útok, pri ktorom útočník predstiera, že vás telefonicky kontaktuje v zastúpení vašej banky, sociálnej/zdravotnej poisťovne. Počas telefonického rozhovoru vás požiada o dôverné/osobné/prihlasovacie údaje, ktoré následne zneužije.

Ako takýto útok odhaliť?

Tu platí základná rada:

Banka si nikdy či už prostredníctvom e-mailu, sms alebo telefonicky nepýta citlivé údaje o internetbankingu (prihlasovacie meno, heslo, údaje na potvrdenie transakcie), platobnom účte alebo platobnej karte (číslo karty, platnosť karty alebo CVV kód), ani nevynucuje inštaláciu žiadnej mobilnej aplikácie alebo programu do počítača a mobilného zariadenia. Zlatým pravidlom je, že na takúto požiadavku by klient nikdy nemal reagovať, ale okamžite na to upozorniť banku cez zákaznícku linku.

Banky však klienta môžu kontaktovať telefonicky napríklad v prípade bezpečnostnej hrozby. Preto aj klientom odporúčajú, aby pravidelne aktualizovali telefonický kontakt, ktorý im poskytli. Môže ísť o overovanie reálnosti transakcie, ak je platobná karta použitá v nezvyčajných destináciách. Banka vtedy vyhodnocuje, či sa klient náhodou nestal obeťou skimmingu a niekto sa nesnaží použiť klon jeho platobnej karty. Telefonát pritom možno kedykoľvek prerušiť a spotrebiteľ môže iniciatívne kontaktovať svoju banku, aby si hrozbu overil.

Sprievodným znakom telefonátu je podozrivo úporná snaha získať vaše údaje, aj po prvotnom odmietnutí.

Čo robiť/nerobiť?

Ak máte podozrenie, že sa jedná o Vishing, jednoducho ukončite hovor. Ak máte obavy, pochybnosti, zavolajte do banky vy a informujte sa na problém, o ktorom sa vás snažil podozrivý telefonista presvedčiť.

Podvod s prísľubmi odmeny, podielu

Toto je pravdepodobne najčastejší druh útoku prostredníctvom elektronickej pošty. Prišiel vám už e-mail s oznámením o vysokej výhre, dedičstve od vášho neznámeho predka, alebo zúfalá prosba občana niektorého afrického štátu, ktorý príde o celý svoj majetok, ak sa mu nepodarí previesť svoje celoživotné úspory na účet občana EÚ? Jediné, čo potrebuje sú vaše prihlasovacie údaje k bankovému účtu. Hneď ako svoje úspory zachráni, prevedie vám z nich štedrý podiel…
Princípom tohoto podvodu je vyvolanie pocitu núdze a apelovanie na okamžitú akciu. Takáto dobročinnosť väčšinou končí vybieleným bankovým účtom.

Ako takýto útok odhaliť?

Ak vám táto ponuka znie príliš dobre na to, aby to bola pravda, je to preto, lebo ide o podvod. Dobrými identifikátormi sú tiež gramatické chyby.

Čo robiť/nerobiť?

Takýto e-mail treba vymazať a nereagovať naň.

Podvod s bezpečnými účtami

Väčšinou spočíva v tom, že vás kontaktuje osoba tvrdiaca o sebe, že je z vašej banky. Oznámi vám, že váš účet bol skompromitovaný/unikli vaše prihlasovacie údaje a vyzve vás k urýchlenému presunu financií na takzvaný "bezpečný/zabezpečený bankový účet", ktorý je samozrejme bankovým účtom podvodníka.

Ako takýto útok odhaliť?

Tu platí základná rada:

Banka si nikdy či už prostredníctvom e-mailu, sms alebo telefonicky nepýta citlivé údaje o internetbankingu (prihlasovacie meno, heslo, údaje na potvrdenie transakcie), platobnom účte alebo platobnej karte (číslo karty, platnosť karty alebo CVV kód), ani nevynucuje inštaláciu žiadnej mobilnej aplikácie alebo programu do počítača a mobilného zariadenia. Zlatým pravidlom je, že na takúto požiadavku by klient nikdy nemal reagovať, ale okamžite na to upozorniť banku cez zákaznícku linku.

Útočník v tomto prípade obvykle apeluje na urýchlené jednanie v atmosfére strachu, ktorú vyvolal, na druhej strane vám poskytuje "riešenie a pomoc".

Čo robiť/nerobiť?

Pokiaľ máte podozrenie, že telefonát vykazuje znaky takéhoto útoku, ukončite hovor, kontaktujte svoju banku vy a vyžiadajte si informácie.

Podvody s pôžičkami

Ak hľadáte online pôžičku, môže sa ľahko stať, že natrafíte na podvodníkov, ktorí vám ponúkajú pôžičku priamo a hlavne, za podozrivo výhodných podmienok. Vyzvú vás na zaplatenie poplatku za vybavenie pôžičky, ktorý v momente odoslania vidíte naposledy.

Čo robiť/nerobiť?

O úver žiadajte vždy v banke, napriek tomu, že zázračná ponuka na sociálnej sieti vyzerá dôveryhodne a samozrejme výhodnejšie, rýchlejšie, bez dokladovania príjmu.

Podvody s lístkami na kultúrne podujatia

Kúpite si lístky na koncert, športové podujatie, tešíte sa naň, no žiadne lístky neprídu, alebo vás pri vstupe na podujatie otočia s tým, že vaše lístky sú falošné. Aj takýto scenár môže nastať, ak si pri nákupe lístkov nedáme pozor na podvodníkov.

Mnohé stránky, ktoré obchodujú s lístkami, nie sú vyslovene podvodné, používajú resellingovú stratégiu - teda skúpia veľký počet oficiálnych vstupeniek a potom ich so ziskom predávajú. No často sa vám stane, že oficiálny predajca sa bráni tým, že vydáva lístky na meno kupujúcej osoby, ktorou v tomto prípade nie ste vy, ale resellingová podvodná spoločnosť, takže cesta na koncert v Londýne môže skončiť pri vstupnej bráne podujatia.

Ako takýto útok odhaliť?

Často až do dňa, kedy vás nevpustia na podujatie žijete v domnienke, že vaše lístky sú pravé. Podozrivá môže byť hlavne stránka, ktorá obsahuje len podozrivé medzinárodne vyzerajúce telefónne číslo, adresu na P.O. Box. Často tiež pri nákupe na vás vyvíja nátlak časovým údajom, za ktorý musí byť transakcia ukončená (obvykle 2 minúty) a údajom o tom, že niekto práve v tejto chvíli zakúpil vstupenky na podujatie, o ktoré máte záujem. Takto vás donútia jednať v strese a bez dôkladného zváženia krokov, ktoré robíte. Straty môžu byť nemalé, často rádovo v stovkách Eur.

Čo robiť/nerobiť?

Vyhnite sa nákupu lístkov cez sociálne médiá, online aukciám, sekundárnym trhom. Kupujte lístky od oficiálnych predajcov. V adrese predajcu hľadajte dôležité “s” symbol zabezpečenia - teda https:// namiesto nedôveryhodného http://.

Treba tiež dodať, že útočník nemá vždy zálusk len na ukradnutie prístupu do internetbankingu, PayPal, či Amazon, ale aj do obyčajného e-mailového účtu. Rovnako ako v predchádzajúcich popísaných prípadoch, príde správa, že e-mailová schránka je plná, a ak ju chceme naďalej používať, treba poslať meno a heslo administrátorovi...a princíp už je rovnaký. Často útočník nepotrebuje vyvinúť ani snahu na prelomenie našich bezpečnostných kódov. Stačí, že sa zabudneme odhlásiť z prehliadača na školskom, pracovnom, verejnom počítači a všetky údaje o našom prehliadaní doslova ponúkame ľuďom, ktorí ich dokážu zneužiť. Potom je to už len krôčik k e-mailu, v ktorom sa nám niekto vyhráža, že vie, “na akej zoznamke” fungujeme a s kým a o čom si tam píšeme a tiež aj, koľko nás to bude stáť, aby sa o tom nedozvedela celá naša rodina, alebo všetky kontakty na Instagrame.

Podvodné telefonáty

V posledných dňoch a týždňoch obyvatelia Slovenska zaznamenali nevyžiadané prichádzajúce hovory zo zahraničných čísiel, prevažne z Afriky či z iných „exotických“ vzdialenejších krajín.
Tieto hovory môžu byť pre ľudí potencionálne nebezpečné. Užívateľov mobilných telefónov môže prekvapiť vysoká faktúra alebo dodatočné poplatky za spätné hovory na takéto neznáme čísla.

Ako možný nebezpečný hovor odhaliť a ako pri podozrení konať?

Nevyžiadané prichádzajúce hovory viete identifikovať už na prvý pohľad. Na displeji mobilného telefónu sa objaví číslo s netradičnou predvoľbou, ktoré nemáte uložené v adresári. Niektoré mobilné telefóny zobrazia aj názov krajiny, z ktorej hovor prichádza.

Medzi predvoľbami si môžete všimnúť čísla ako +236 (Stredoafrická republika), +252 (Somálsko), +717 (Čína) +224 (Guinea) a im podobné. Prichádzajúci hovor sa môže opakovať s cieľom, aby podvodníci donútili užívateľov zavolal späť. V žiadnom prípade to nerobte.

Čo robiť/nerobiť?

Pokiaľ v niektorej zo vzdialených krajín žije váš príbuzný, známy alebo napr. kolega a domnievate sa, že hovor môže prichádzať od neho, aj napriek tomu hovor neopätujte. Jeho číslo máte pravdepodobne uložené v zariadení.

Pokúste sa ho kontaktovať prostredníctvom iných kanálov, napríklad sociálnych sietí alebo komunikačných aplikácií, čím si overíte, či vám náhodou netelefonoval. Je zvykom, že ak človek opakovaný prichádzajúci hovor nezdvihne, volajúci napr. zašle SMS-ku.

Zhrnutie, alebo ako sa bezpečne chrániť pred rôznymi druhmi útokov:

1. **Svoje osobné údaje zverejňujte len keď je to nevyhnutné, robte to profesionálne a čo najmenej!** Vaši potenciálni zamestnávatelia alebo zákazníci nepotrebujú vedieť o vašom vzťahu, stránkach z ktorých nakupujete, a nepotrebujú poznať vašu domácu (fyzickú) adresu. Platí, že kto je ľahko čitateľný a nestráži si súkromie, je pre útočníkov ľahšou korisťou, ako človek, ktorý si svoje súkromie stráži.
2. **Zapnite si ochranu súkromia v aplikáciách prehliadačoch a hlavne na sociálnych sieťach.** Ušetrí vám to kopec peňazí. Ak sa aj nestanete obeťou útočníkov, stanete sa obeťou marketérov. Čudovali ste sa, aký je to zázrak, že Vám odrazu príde do mailu neodolateľná ponuka na topánky, o ktorých len tajne snívate, a zrazu sa reklama na ne zobrazuje aj vo videách na youtube? Ste sledovaní, a čitateľní, či sa vám to páči, alebo nie. Napriek tomu, že vývojári ako Mozilla sa snažia o najviac chrániť vaše súkromie, nezmôžu nič, ak to nezačnete robiť aj vy. Používajte "private" browsing v prehliadači.
3. **Trénujte bezpečné prehliadanie.**
   V realite by ste sa nevydali do nebezpečnej štvrte. Prečo to ale robíte online? Neklikajte na neodolateľné ponuky, ktoré na prvý pohľad vyzerajú až priveľmi dobre, aby boli pravdivé. Nenavštevujte stránky s podozrivým, nelegálnym obsahom (najnovšie hry, filmy, seriály, hudba, značkový tovar za "rozprávkové" ceny, pornografia…) Takéto vyhľadávanie vás môže stáť veľmi veľa peňazí.
4. **Používajte zabezpečené internetové pripojenie, nie verejné siete, keď sa prihlasujete a stránku pomocou vašich osobných identifikátorov a hesiel.**
5. **Buďte opatrní, aké súbory sťahujete**
   Cieľom kyberútočníkov je presvedčiť vás, aby ste si pod akoukoľvek zámienkou stiahli malware - program, aplikáciu, ktorá vás na pozadí sleduje, sprístupňuje útočníkovi vaše zvyky, prístupy, heslá, komunikácie. Najlepšie je inštalovať si oficiálne distribuované aplikácie, hry, filmy, hudbu kupovať, prípadne kúpiť si prístup k streamingovým službám, namiesto nelegálneho sťahovania cez pokútne stránky a fóra, či nedôveryhodné PTP siete.
6. **Používajte silné heslá**
   Poznáte to, jedno heslo na všetko? Väčšina z nás áno. Silné heslo by malo mať aspoň 15 znakov , a malo by byť kombináciou číslic, znakov, veľkých a malých písmen. Ku každému prístupu by sme mali mať silné originálne a unikátne heslo, ak máte obavy, že heslá zabudnete, existujú aplikácie, ktoré si vaše heslá zapamätajú a sú chránené jediným heslom, odtlačkom vášho prsta, alebo skenom vašej tváre. Neodporúča sa tiež umožňovať prehliadačom zapamätať si vaše prístupové heslá, kódy a údaje platobných kariet, či iných nástrojov.
7. **Platby realizujte zo zabezpečených stránok,**
   tie rozpoznáte podľa symbolu zámku v riadku s webovou adresou a webovej adresy začínajúcej https:// namiesto http://.
8. **Dajte pozor, čo o sebe publikujete online**
   Internet má dobrú pamäť. To čo nemá, je tlačidlo "detete". Publikujte o sebe len také informácie, o ktorých ste si istí, že by vám nevadilo, ak by si ich prečítal váš nastávajúci partner, či zamestnávateľ.

9. **Dajte pozor na to, s kým sa online stretávate**
   Buďte pri nadväzovaní vzťahov na sociálnych sieťach takí opatrní, ako ste pri nadväzovaní skutočných vzťahov v realite. Za falošnými profilmi na sieťach sa často skrývajú podvodníci a útočníci s veľmi rozličnými, ale málokedy dobrými, pohnútkami.
10. **Aktualizujte, čo sa dá**
    Operačný systém, prehliadač, software, s ktorým pracujete, mobilné aplikácie bánk a platobných nástrojov anti-vírusové programy, ale aj technické zariadenia ako wifi routre. Poskytovatelia sa vždy snažia "zaplátať " bezpečnostné diery v produktoch, ktoré vám poskytujú. Tým, že aktualizujete, mali by ste mať vždy zabezpečený aj najaktuálnejší a najvyšší možný stupeň ochrany.
11. **Nainštalujte si bezpečnostné rozšírenie webového prehliadača, ktoré kryptuje (kóduje a tak zvyšuje bezpečnosť) vašu komunikáciu cez konkrétny prehliadač. https://www.eff.org/https-everywhere**

Ostatné je na vás.

Zdroje:
https://www.sbaonline.sk/sk/novinky/17/ako-to-je-naozaj-opatrenia-proti-phishingu
https://www.sbaonline.sk/sk/novinky/19/bezpecnost-nadovsetko
https://www.moneyadviceservice.org.uk
https://usa.kaspersky.com/