NEJČASTĚJŠÍ HACKERSKÉ TRIKY

Kybernetičtí zločinci se při pokusech vás okrást neustále zdokonalují. K vašim penězům se již dávno nesnaží dostat jen s pomocí e-mailů slibujících snové dědictví či falešných stránek plných gramatických chyb a překlepů. Jejich metody jsou dnes daleko sofistikovanější a kombinují nedostatečné zabezpečení vašich chytrých telefonů a PC, znalosti vašich osobních dat, umění manipulace a momentu překvapení.

JAKÉ JSOU NEJČASTĚJŠÍ TYPY ÚTOKŮ NA KLIENTY BANK?

1.Telefonáty podvodných bankéřů či policistů (vishing)

Útočník vás chce vystrašit a zároveň vzbudit důvěru, že je tím, kdo vám pomůže ochránit peníze na účtu. Pod záminkou napadení vašeho účtu či podezřelé transakce vám zavolá v nezvyklý čas a představí se jako pracovník banky, či policista. Na hovor se dobře připraví – zná vaše jméno, adresu nebo číslo bankovního účtu. Může volat z čísla podobného či stejného, jako má vaše banka, dokonce vás vyzve k identifikaci, jako to dělají banky. S vaší získanou důvěrou vás pak bude tlačit k okamžitému převedení zůstatku na bezpečný účet, který je ale ve skutečnosti jeho.

Scénáře se mohou lišit – útočník po vás bude chtít vaše přihlašovací údaje, údaje z vaší platební karty či potvrzovacích SMS, případně umožnit vzdálený přístup k vašemu PC. Závěr je ale stejný – své peníze již pravděpodobně nikdy neuvidíte.

2.Podvodné mobilní aplikace

Jedním z velmi aktuálních triků útočníků jsou i malwarem infikované mobilní aplikace či jejich aktualizace, které si nejčastěji stáhnete z neoficiálních obchodů s aplikacemi a webových stránek. Výjimkou ale nejsou ani podvodné aplikace nainstalované přímo z oficiálního obchodu. Pokud v telefonu nemáte nainstalovaný bezpečnostní software, který by vás varoval, a při instalaci aplikaci udělíte vysoká oprávnění – například aplikaci pro nahrávání hovorů i přístup k fotoaparátu či SMS – dokáže odcizit vaše přihlašovací údaje do bankovnictví, obejít dvoufázové ověření či získat potvrzovací SMS zprávy. Aplikace proto nakupujte nejlépe jen na Google Play či App Store, čtěte jejich recenze a nedávejte jim více oprávnění, než potřebují.

3.Falešné stránky internetového bankovnictví

Jedná se již o známou útočnou metodu, přesto se může stát, že se díky své nepozornosti nachytáte. Útočník chce získat vaše přihlašovací údaje s pomocí falešné webové stránky banky. Ta může na první pohled vypadat úplně stejně jako skutečný web vaší banky, včetně loga a barev. Na druhý pohled ji ale odhalit lze – URL adresa webu se bude odchylovat od oficiálního názvu či zkratky banky, na stránce jsou překlepy, v řádku s adresou nebude visací zámeček označující bezpečnostní certifikát webu, nýbrž upozornění apod. Pokud se přes takové stránky přesto přihlásíte, získá útočník vaše přihlašovací údaje do internetového bankovnictví. Pomocí dalších podvodných technik mu pak stačí získat váš potvrzovací kód či autorizační SMS a cestu k vašim penězům na účtu má volnou.

4.E-maily plné virů a podvodných odkazů

V tomto případě jdou útočníci cestou kvantity nad kvalitou – rozešlou podvodné e-maily na mnoho adres včetně té vaší, kterou získali například z vašeho profilu na sociálních sítích, a čekají, kdo se chytne. Dávno už se nejedná jen o výzvy k převzetí dědictví po vaší zapomenuté tetičce či nabídky k sňatku od nigerijských princů, plné překlepů a gramatických chyb. E-maily se tváří jako oficiální zprávy banky, pošty nebo třeba obchodního řetězce. Obsahují odkazy na falešné stránky, kde máte zadat platbu či se přihlásit do internetového bankovnictví, případně vyzývají ke stažení přílohy, která je ale samozřejmě infikovaná virem či malwarem. Pokud trik včas neodhalíte, útočníci získají vaše přihlašovací údaje či údaje z platební karty.

5.Falešné profily na sociálních sítích

Útočníci typicky vytvoří falešný profil osoby, kterou znáte. Z tohoto profilu vás pak žádají o vyplnění formuláře či zaslání finanční částky na pomoc, případně pod záminkou výhry v soutěži posílají odkazy směřující na falešné stránky, kde již jen čekají, až zadáte vaše údaje z platební karty či jiné důvěrné údaje. Pokud podobnou výzvu obdržíte, raději si ji s danou osobou telefonicky ověřte. Podvodníci mohou ale falšovat i profilové stránky bank, přes ně se můžete dostat na falešné internetové bankovnictví či podvodnou platební bránu.

6.Získání nadvlády nad vaší platební kartou v mobilu

Získá-li útočník vaše údaje o platební kartě, pokusí se ji pravděpodobně tzv. digitalizovat, tedy ji nahrát do svého telefonu, resp. do Google Pay či Apple Pay. Pokud se mu následně podaří registraci potvrdit aktivačním kódem (zasílaným do internetového bankovnictví či SMS), ke kterému se dostane pomocí nějaké podvodné techniky, bude již moci „vesele“ platit svým telefonem a odčerpávat vám peníze z účtu, dokud si toho nevšimnete.

PĚT ZÁSAD, DÍKY KTERÝM BUDOU VAŠE ÚDAJE I PENÍZE V BEZPEČÍ

1. Nikdy nikomu nesdělujte své přihlašovací údaje do internetového bankovnictví ani čísla ze své platební karty. Banky se na ně opravdu NIKDY neptají, a to ani telefonicky, ani e-mailem, ani SMS či jinými zprávami. Zároveň nikdy neposílají odkazy na weby, kde jsou údaje vyžadovány!

2. Nereagujte na telefonní hovory, e-maily ani zprávy, 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 skutečně v ohrožení, banka by již zareagovala dávno a bez vaší pomoci.

3. Nezadávejte ani v aplikaci nepotvrzujte platby, které vám někdo bude diktovat po telefonu. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.

4. Mějte aktualizovaný software a antivirus v PC i telefonu. Aplikace stahujte jen z oficiálních zdrojů a nedávejte jim více oprávnění, než potřebují.

5. Buďte vždy v pozoru, nenechte se zviklat ani nalákat. V případě pochybností vždy kontaktujte svou banku či volejte Policii (158).