JAK NA INTERNET

Jak nenaletět internetovým podvodníkům

Podvodníci na Internetu vymýšlejí stále nové triky, jak se uživatelům dostat na kobylku. Proto je potřeba být při práci na počítači stále ve střehu. To však neznamená, že bychom se měli bát počítač používat. V reálném světě na nás také číhá řada filutů, kteří by se rádi obohatili na náš úkor. Stejně, jako dbáme určité opatrnosti v běžném životě, je potřeba dodržovat určitá základní pravidla i při práci s počítačem. Následující krátký přehled by vám měl pomoci s rozpoznáním aspoň těch nejčastějších fíglů.

Phishing

Oblíbenou strategií útočníků je vylákat z oběti nějaké přihlašovací údaje, nejlépe k jejich bankovnímu účtu, ale může se jednat i o jiné služby, například e-mailové účty, které mohou mít pro podvodníky také svou hodnotu. Pokud vás zajímá jakou, přečtěte si níže o falešných přátelích. Phishing obvykle snadno poznáte podle některých typických prvků. Tím hlavním, který je ostatně společný většině podvodů, a to nejen těch internetových, je vytváření tlaku a zastrašování, díky kterému není uživatel schopen se racionálně rozhodnout. Typickým příkladem může být e-mail, ve kterém jste vyzváni k odeslání odpovědi obsahující například číslo vaší platební karty, dobu její platnosti a CCV/CVC kód. Důležité je, že v takové zprávě bude například napsáno, že došlo k nějakému bezpečnostnímu problému v bance a že pokud neposkytnete požadované údaje do určitého časového limitu, bude váš účet z bezpečnostních důvodů zablokován a vy se budete nuceni pro jeho odblokování osobně dostavit na pobočku. Představa času stráveného čekáním někde na pobočce je pak pro určité procento uživatelů dostatečně silnou motivací k poskytnutí požadovaných údajů.

V případě phishingových útoků, které odkazují na napodobeninu stránek nějaké služby na Internetu by pak mělo být dostatečným varováním změněné URL, i když útočníci se často snaží aspoň nějakým způsobem v URL název služby zakomponovat. V praxi se tak setkáváme s názvy jako je například *www.podvodna-domena.com/nazev_vasi_banky*. Dále by nás měla varovat neexistence zabezpečeného připojení HTTPS, případně použití falešných certifikátů. Obecně ale platí, že banky ani žádné další společnosti po vás nebudou vyžadovat zasílání jakýchkoliv přihlašovacích údajů! Pokud máte pochybnosti, zda se přece jen nejedná o nějakou důležitou zprávu, vždy je třeba si zdroj ověřit telefonicky na čísle, které najdete na oficiálních webových stránkách dané služby. Podezření často budí také špatně použitá čeština či oslovení. Ale toto již dnes nemusí být pravidlem a s legendárními phishingovými e-maily začínajícími oslovením „Drahoušek zákazník“ se dnes již nesetkáme.

Malware

Jedním z dalších cílů útočníků je nahrát do počítače oběti nějaký škodlivý kód. V poslední době jsme se mohli setkat například s rozesíláním e-mailů, které se tvářily jako informace o balíku uloženém u *České pošty*, či jako informace o neuhrazené pohledávce, či přímo jako exekuční příkaz. Všechny tyto spamy obsahovali přiložený .zip soubor, který ve skutečnosti obsahoval spustitelný soubor a vedl k zavirování počítače. Následně došlo k finančním ztrátám pro majitele daného účtu.

Malware však můžete chytit i pokud žádný soubor nespustíte. V každém software se čas od času objevují různé chyby. Některé z nich, kterým se říká zranitelnosti, mohou vést například ke spuštění nebezpečného programu bez vědomí uživatele. Existují specializované nástroje, které umožňují útočníkům napadnout váš počítač například pouhým navštívením speciálně upravené stránky. Na tu se však můžete dostat i při návštěvě běžné webové stránky, která však předtím byla útočníky napadena. Toto je důvod, proč byste měli vždy instalovat nejnovější aktualizace jak pro váš operační systém, tak také pro ostatní používaný software. Při pravidelné aktualizaci značným způsobem minimalizujete riziko úspěšného útoku na váš počítač, neboť většina kriminálních útoků používá při útocích již záplatované díry a spoléhají se na pohodlnost, či neznalost uživatelů.

Pozor na falešné přátele

Oblíbeným trikem útočníků je také zneužití e-mailového, či facebookového účtu k získání peněz od kontaktů z napadeného účtu. Jedná se o nejrůznější triky a příběhy. Dnes již klasikou je zpráva, že majitel dané e-mailové schránky zůstal okradený v zahraničí a nyní žádá své přátele o zaslání finanční částky, která by mu pomohla. Asi není třeba dodávat, že pokud svému „kamarádovi“ pomůžete, on ani vy už peníze nikdy neuvidíte. Dalším podobným trikem zaznamenaným nedávno v ČR je žádost o přeposlání kódu z mobilního telefonu. Obvykle pod záminkou, že dotyčný je mimo signál a potřebuje vaši pomoc. Kódy obvykle slouží k zaplacení nějakého zboží, či kupónů a dotyčný, který pomohl svému „kamarádovi“ to často pocítí až s příchodem vyúčtování od mobilního operátora.

Zneužívání „populárních“ událostí

Útočníci se často neštítí využít různých sportovních událostí jako je olympiáda, ale také tragédií, jako byl teroristický útok v americkém Bostonu. Tak se můžete setkat s vějičkou v podobě videa, které má ukazovat domácí popravu islámské ženy, videa z pádu letadla nad Ukrajinou, či v posledních dnech rozšířeného videa, které má být dopisem na rozloučenou populárního herce Robina Williamse, parazitujících na lidské zvědavosti a touze po senzacích. Kliknutí na podobná videa obvykle vede k různým akcím, od žádosti o vyplnění dotazníku, za který podvodník inkasuje peníze, až k nabídce instalace aktualizace pro přehrávač, který však ve skutečnosti obsahuje virus. Netřeba snad dodávat, že slibovaného videa se oběť nedočká, neboť takové video ani neexistuje.

Existují i aplikace, které například slibují změnu barvy *Facebooku* z modré na jinou, či další podobné vychytávky. Obvykle na ně narazíte na samotné sociální síti, buď jako na status vašich přátel, nebo vám přijde odkaz přes osobní komunikaci. Většina virů pocházejících ze sociálních sítí je totiž nebezpečná také tím, že v případě úspěšného útoku dokáží přidat reklamu na sebe sama na zeď napadeného uživatele, či se přes soukromé zprávy infiltrovat k dalším uživatelům v jeho kontaktech.

Nigerijské dopisy

Poslední podvod, u kterého se krátce zastavíme, patří mezi letité podvody a ještě před masivním rozšířením Internetu byl provozován pomocí klasických dopisů či faxů. Zde se vlastně vracíme k úvodu, kde jsme si řekli, že i v reálném světě na nás číhá řada podvodníků. Nigerijské dopisy jsou klasickým podvodem, který existoval už dříve a po příchodu Internetu se jen transformoval do podoby méně nákladné pro podvodníky. Principem těchto podvodů je, že vás kontaktuje cizí

člověk a pod záminkou, že zdědil obrovský majetek, nebo jej dokonce spravuje pro někoho jiného, případně že jako zaměstnanec nějakého fondu našel peníze po zemřelém klientovi, o kterých nikdo neví, vás vtáhne do své hry, jejímž výsledkem bude, že přijdete o své peníze. Obvykle je vám za pomoc s převodem peněz slíben určitý podíl z celé částky, nicméně podvodník postupně z oběti tahá peníze pod různými záminkami.

Podvodníci stále vymýšlejí nové triky k ošálení svých obětí a činí tak jak v reálném, tak ve virtuálním světě. Když obdržíme e-mail či jinou zprávu s podezřele výhodnou nabídkou, s žádostí o pomoc, s přiloženým souborem, či s požadavkem na poskytnutí našich údajů je potřeba vzít rozum do hrsti a vše si v klidu promyslet.