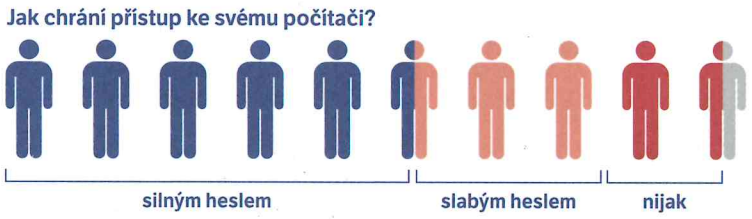
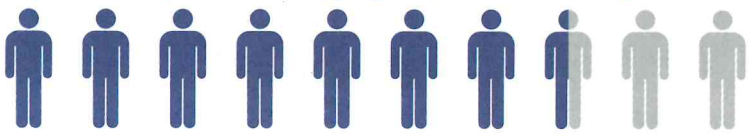
V kyberprostoru je největším nebezpečím člověk sám sobě

Když jde člověk z bytu a zamkne za sebou, přijde mu to přirozené. Podobně by se měl chovat i při práci na internetu, ale ani za léta užívání nových technologií se to pořád nevžilo. Ukazuje to mimo jiné čerstvý výzkum mezi studenty Masarykovy univerzity. Velké množství z nich se vystavuje nebezpečí zneužití svých osobních údajů.

JAK SI STUDENTI MUNI (NE)HLÍDAJÍ SVÉ BEZPEČÍ?



66 %
studentů si nikdy nezměnilo primární nebo sekundární univerzitní heslo



33 %
studentů někdy sdělilo své primární heslo další osobě

36 %
studentů si pravidelně neaktualizuje operační systém nebo aplikace

40 %
studentů si nezamyká počítač v učebně při krátkodobé nepřítomnosti

Napadení počítače virem, kráděž osobních údajů nebo jejich nežádoucí využívání. To všechno se uživatelům může stát. Odborných doporučení, jak se chovat, aby k tomu nedošlo, existuje řada. Jenže mezi jejich existencí a reálným využíváním je podle výzkumníků z Masarykovy univerzity velká propast.

Hlavní problém? Sdílení a neměnění hesel

Mezioborový tým provedl v průběhu podzimního semestru dotazníkové šetření, kde se studentů Masarykovy univerzity ptal na jejich chování v oblasti IT. Díky umístění ve vybraných počítačových učebnách se podařilo sesbírat data od 1149 studentů, ale výsledky výzkumu odborníky nepotěšily.

„Asi nejzásadnějším zjištěním je informace o chování studentů k heslům. 55 procent z nich si nikdy nezměnilo primární heslo v ISu a 66 procent si nikdy nezměnilo sekundární heslo. Vzhledem k tomu, že pomocí těchto hesel jsou přístupné podstatné univerzitní agendy, nejedná se především u primárního hesla o dobrou zprávu," stojí ve zprávě z výzkumu.

Takový výsledek jde přesně proti doporučení expertů. Chránit svoji virtuální identitu lze mnoha sofistikovanými způsoby, jimž nemusí laik rozumět. Velkou službu udělají ale už jen základy, jako je občasné měnění hesel u klíčových účtů.

Uživatelé ovšem selhávají už v tomto počátečním bodu. „Výsledky do jisté míry odpovídají očekávání. Na to, že se problém často nachází mezi židlí a počítačem, se snažíme dlouhodobě upozorňovat. Přesto jsou závěry zneklidňující," podotknul Václav Matyáš, expert fakulty informatiky na bezpečnostní technologie.

Problematický je podle výzkumníků také způsob zacházení s hesly. Ačkoliv naprostá většina respondentů ve výzkumu správně vyhodnotila sdílení hesel jako rizikové, přesto více než třetina z nich své primární heslo někdy někomu sdělila, z toho pětina v rozmezí posledních tří měsíců.

Důvody pro sdílení hesel zahrnují například pomoc při registraci do seminární skupiny nebo přihlašování na zkoušky. Což je typickým příkladem chování, které je pro uživatele univerzitních systémů zapovězené.

Od října loňského roku totiž platí směrnice o používání univerzitních informačních technologií, která specificky tento příklad zmiňuje jako to, jak se člověk nemá chovat. Ačkoliv směrnice je záměrně psaná způsobem, aby jí porozuměl kdokoliv, ne každý o ní má povědomí.

„Přitom je nutné akceptovat, že také používání různých IT nástrojů se řídí svými pravidly a je třeba se podle nich orientovat podobně jako podle studijního a zkušebního řádu," podotknul David Šmahel, psycholog zabývající se kyberprostorem.

Lehkomyslnost se podle výsledků výzkumu lidem vrací jako bumerang. Přes 13 procent respondentů uvedlo, že někdo použil osobní informace, které o sobě sdíleli na internetu, způsobem, jaký se jim nelíbil. Více než 24 procent účastníků výzkumu mělo účet na stránce, která se někdy potýkala s únikem uživatelských dat. A přes 30 procent respondentů mělo zkušenost s tím, že se někdo někam přihlásil pod jejich přihlašovacími údaji bez jejich vědomí.

Pomůžou správci hesel

Což problém vrací zpátky k heslům a k tomu, že právě ona jsou základem bezpečnosti. Hlavně pro služby, na kterých uživateli velice záleží, by se měla používat unikátní a nelehko odhadnutelná hesla. Na argument, že zapamatovat si více takových písemných nebo číselných řad je nemožné, odborníci reagují výzvou k využívání správců hesel. Apel se týká i studentů Masarykovy univerzity. Z výzkumu vyplynulo, že zhruba třetina z nich používá svoje primární nebo sekundární heslo ještě pro další služby a účty.

Silná hesla jsou základ, uživatelé s nimi ale ještě pořád neumí pracovat.

„Že se hesla nepoužívají pro více služeb, by mělo platit hlavně pro ty kriticky důležité, jako jsou internetové bankovnictví nebo třeba právě univerzitní informační systém. Oboje je samo o sobě zabezpečené velice dobře, ale pokud někdo totéž heslo využije například v méně chráněných malých e-shopech, vystavuje se nebezpečí, že právě kvůli tomu se mu někdo dostane i do důležitějšího systému," zdůraznila Vlasta Šťavová, doktorandka fakulty informatiky, která se uživatelskou přívětivostí bezpečnostních systémů zabývá.

Obecnou radu na to, které weby nebo účty by si člověk měl hlídat nejvíc, odborníci nemají. „Citlivé jsou samozřejmě informace o zdravotním stavu nebo finanční služby. Někdo to ale může brát tak, že je pro něj nejcennější jeho přístup do herního účtu na World of Warcraft," podotkla Šťavová s tím, že priority jsou různé.

Pomoct by podle ní mohlo zeptat se u každého účtu nebo služby sám sebe, jestli by uživateli vadilo, kdyby se dovnitř někdo nepovolaný dostal. Pokud ano, je na místě zvolit si patřičně silné heslo nebo pokročileji chráněnou službu.

Šťavová chválí ty služby, které v sobě mají takzvanou dvoufaktorovou autentizaci. To znamená, že je zapotřebí použít dva různé způsoby, jak se do služby přihlásit (k heslu například ověřovací kód z mobilu). Navíc, pokud se člověk do těchto služeb hlásí z jiného počítače než obvykle (typicky toho domácího nebo pracovního), přijde mu upozornění, které funguje jako otazník, jestli je takové chování v pořádku. V drtivé většině případů to uživatel vnímá možná jako zbytečnost, ale nikdy neví, kdy se taková přidaná služba může hodit.

Také odborníci, kteří dělali univerzitní výzkum, uznávají, že nejvíc si lidé dávají na svoji virtuální identitu pozor až po tom, co ji někdo zneužije. Poselstvím jejich práce by ale mělo být, že se má každý uživatel starat co nejvíc o to, aby na to nedošlo.

Martina Fojtů

5 rad, jak se nespálit v kyberprostoru

1. Vaše heslo je podobně důležité jako klíče od bytu. Proto ho nikdy nikomu nesdělujte, nemějte ho všude stejné a svá hesla občas změňte. Ideální heslo je nesnadno uhodnutelné, ale dobře zapamatovatelné (př. Osel1984kytkA%humoristKabaToh). Začněte tím, že zkontrolujete a případně změníte hesla u služeb, které jsou pro vás nejvíce významné.

2. Neopakujte stejná hesla, můžete využít správce hesel, které najdete na internetu.

3. Při čtení e-mailů vždy kriticky zpochybňujte požadavky, které jsou na vás kladeny. Zejména pokud jde o žádost o zaslání jakýchkoli informací, otevírání příloh či odkazů. Zvláště opatrní buďte v situacích, kdy se vás zpráva snaží dostat pod tlak.

4. Zamykejte svůj počítač i při krátké nepřítomnosti. Přestože je třeba ve studovnách Muni nastavený mechanismus automatického uzamčení obrazovky při delší nečinnosti, není dobré na to spoléhat.

5. Pokud máte podezření na bezpečnostní incident či ztrátu přihlašovacích údajů do systémů Masarykovy univerzity, neprodleně uvědomte bezpečnostní tým CSIRT-MU na csirt@muni.cz.

Infografika: Petr Hrnčíř Zdroj: Masarykova univerzita

I používání wi-fi chce obezřetnost

V říjnu loňského roku proběhla technologickým světem nepříjemná zpráva. Stávající ochrana bezdrátového připojení wi-fi pomocí šifrování WPA2 je zranitelná a problémem trpí prakticky všechny bezdrátové sítě současnosti. Přitom na otevřené nebo heslem chráněné wi-fi připojení třeba v kavárnách spoléhá řada lidí.

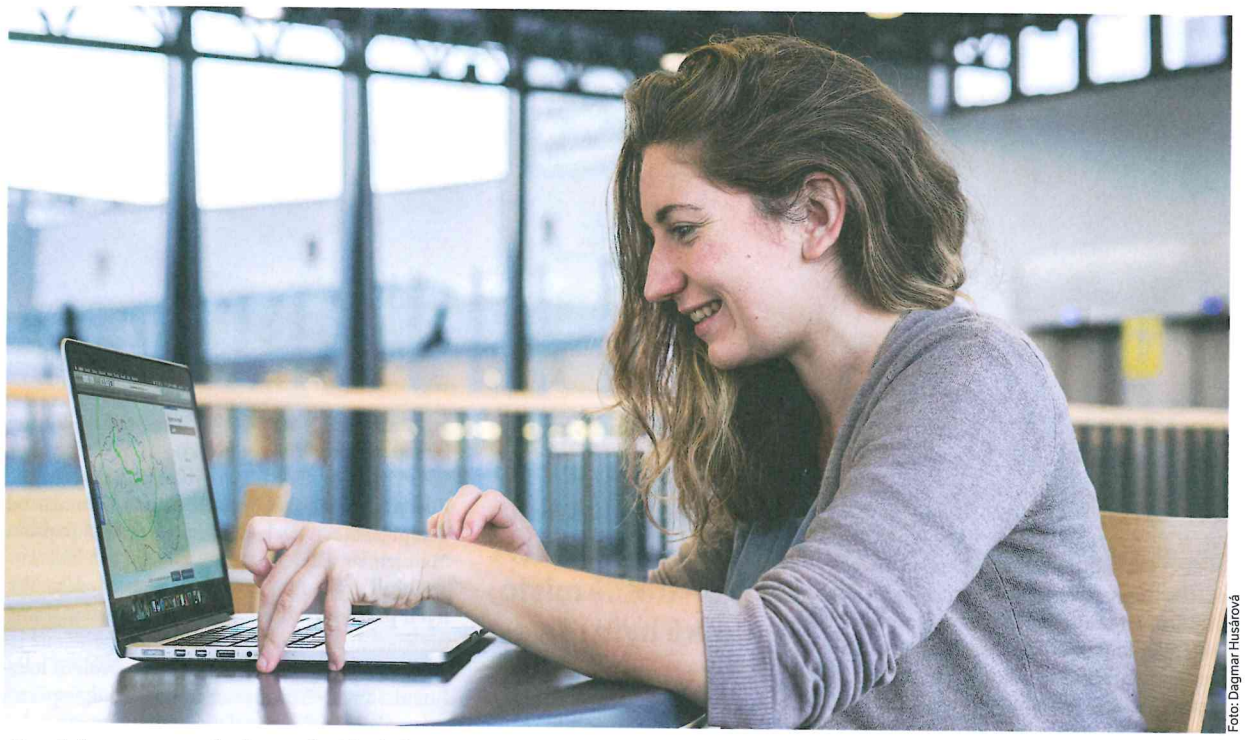


Foto: Dagmar Husárová

„Zranitelnost znamenala, že za určitých okolností bylo možné odhadnout šifrovací klíče, s nimiž útočník mohl číst nebo zasáhnout do komunikace," přiblížil Petr Velan z univerzitního bezpečnostního týmu CSIRT-MU. Jako náhradu za nevyhovující šifrování WPA2 už odborníci oznámili vznik pokročilejšího WPA3. Neznamená to ale, že problémy zmizely.

Běžný uživatel by měl vědět, že pro zařízení, která používala staré šifrování, jejich výrobci většinou vydali aktualizace. „V IT komunitě to funguje tak, že producenti o problému věděli už ve chvíli, kdy se informace o něm dostala do světa, a byli nachystaní jej řešit. Otázka ale samozřejmě je, jestli si koncoví majitelé zařízení aktualizace nainstalovali. A problematická jsou také zařízení s mobilním operačním systémem Android, protože na jeho starší verze se aktualizace často ani nedělají," doplnil Marek Saitl, systémový analytik Ústavu výpočetní techniky MU. Důvodem je podle něj to, že verzí Androidu je dnes už tolik, že je pro výrobce ekonomicky nevýhodné a skoro i nemožné, aby je udržovali v patřičné formě všechny.

Pro uživatele wi-fi připojení, které je v cizích rukou, to znamená to, že by k nim měl přistupovat s rozumnou mírou podezřívavosti a nevstupovat přes internet například v kavárnách do systémů, u nichž by ho mrzelo, kdyby se do nich dostal ještě někdo cizí. Útok je potenciálně možný, i když málo pravděpodobný. „Vyžadovalo by to, aby byl uživatel i útočník napojený na té samé síti a ve fyzické blízkosti a pak samozřejmě docela rozsáhlé technické znalosti," podotknul Velan.

Když už člověk veřejné wi-fi sítě využívá, liší se přístup do nich zpravidla tím, jestli je, nebo není nutné zadávat heslo. Z hlediska bezpečnosti jde o docela důležitý rozdíl. „V otevřené síti se heslo nezadává a komunikace je tím pádem nešifrovaná, kdokoliv v dosahu sítě ji může odposlouchávat," přiblížil Saitl.

Šifrovaná dnes stále ještě většinou znamená zabezpečená systémem WPA2. Pokud je zařízení aktualizované, lze připojení považovat za bezpečné. Pokud tedy člověk věří jeho majiteli a nemá důvod ho podezřívat z nekalých úmyslů.

Pokud se chcete na wi-fi třeba v kavárně cítit bezpečněji, připojte se přes univerzitní VPN, která je šifrovaná.

Pro studenty nebo zaměstnance Masarykovy univerzity je po všech stránkách výhodnější používat síť s označením Eduroam. Pokud člověk obětuje pár minut a nainstaluje si ji podle návodu na it.muni.cz/sluzby/wifi bude mít k dispozici připojení k internetu na všech fakultách a díky tomu, že tutéž síť používají i jiné univerzity, tak i ve velké části Brna a dalších městech, a to také v zahraničí.

„Odborníci z té konkrétní univerzity síť opravdu hlídají, to je její velká výhoda," zdůraznil Saitl. A Velan doplnil ještě další drobnost, která se může hodit při používání méně důvěryhodné sítě: „Univerzita poskytuje uživatelům také virtuální privátní síť, zkráceně VPN, ke které se dá na dálku připojit třeba i z oné kavárny. Je šifrovaná, takže i kdyby se komunikaci snažil někdo číst, dovede ho to jen na univerzitu, ale už ne ke konkrétním informacím."

Oba odborníci se shodují na potřebě být obezřetný, ale také na tom, že kdyby chtěl mít člověk pocit absolutního bezpečí při práci s počítačem, dovedlo by ho to možná až k paranoie. Také oni ale upozorňují na neustále se opakující a zbytečné problémy.

Řada uživatelů pořád podléhá phishingu a svěřuje svoje citlivé údaje na základě nedůvěryhodných zpráv nebo e-mailů, chodí na nedůvěryhodné weby a také stahuje hlavně do mobilních telefonů aplikace, které nadělají víc škody než užitku.

„Hlavně systém Google Play je známý svojí otevřeností, je jednoduché do něj aplikaci jako vývojář dostat. Útočníci toho ale zneužívají a vkládají tam také aplikace, které nejsou důvěryhodné. Proto by lidé neměli skočit na kdejakou hru s pěknou grafikou," zdůraznil Saitl, který radí orientovat se podle kvality a množství hodnocení dané aplikace.

Martina Fojtů

Užitečné pojmy

Bot (Robot)
Programy, které ovládnou počítače v síti a používají je k provádění zločinných aktivit – například distribuovaným útokům (DDoS) a hromadné distribuci nevyžádané komerční pošty. Individuální boty jsou základem velkých skupin robotů známých jako botnety. Počítač zcela nebo částečně ovládaný botem je známý jako „zombie".

Crack
Neoprávněné narušení zabezpečení ochrany programu nebo systému či jeho integrity. Někdy se používá také slovo hack, což je ale i označení podařeného, neobvyklého, nápaditého či rychlého vyřešení programátorského či administrátorského problému.

Červ (Worm)
Autonomní program schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů, kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin.

Firewall
Ucelený soubor bezpečnostních opatření, která mají zabránit neoprávněnému elektronickému přístupu k počítači či konkrétním službám v síti. Také systém zařízení nebo soubor zařízení, který lze nakonfigurovat tak, aby povoloval, zakazoval, šifroval, dešifroval nebo vystupoval v roli prostředníka pro všechny počítačové komunikace mezi různými bezpečnostními doménami, založený na souboru pravidel a dalších kritérií.

Pharming
Podvodná metoda používaná na internetu k získávání citlivých údajů od obětí útoku. Principem je přesměrování klienta na falešné stránky internetbankingu, e-mailu nebo sociální sítě po zadání webové adresy do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek např. banky a ani zkušení uživatelé nemusejí poznat tuto záměnu (na rozdíl od příbuzné techniky phishingu).

Phishing
Podvodná metoda usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet nebo účtu za účelem jejich následného zneužití. Jde o vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu.

Ransomware
Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného.

Spyware
Program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (např. počítačová hra), s jehož funkcí však nesouvisí.

Zdroj: Výkladový slovník Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)