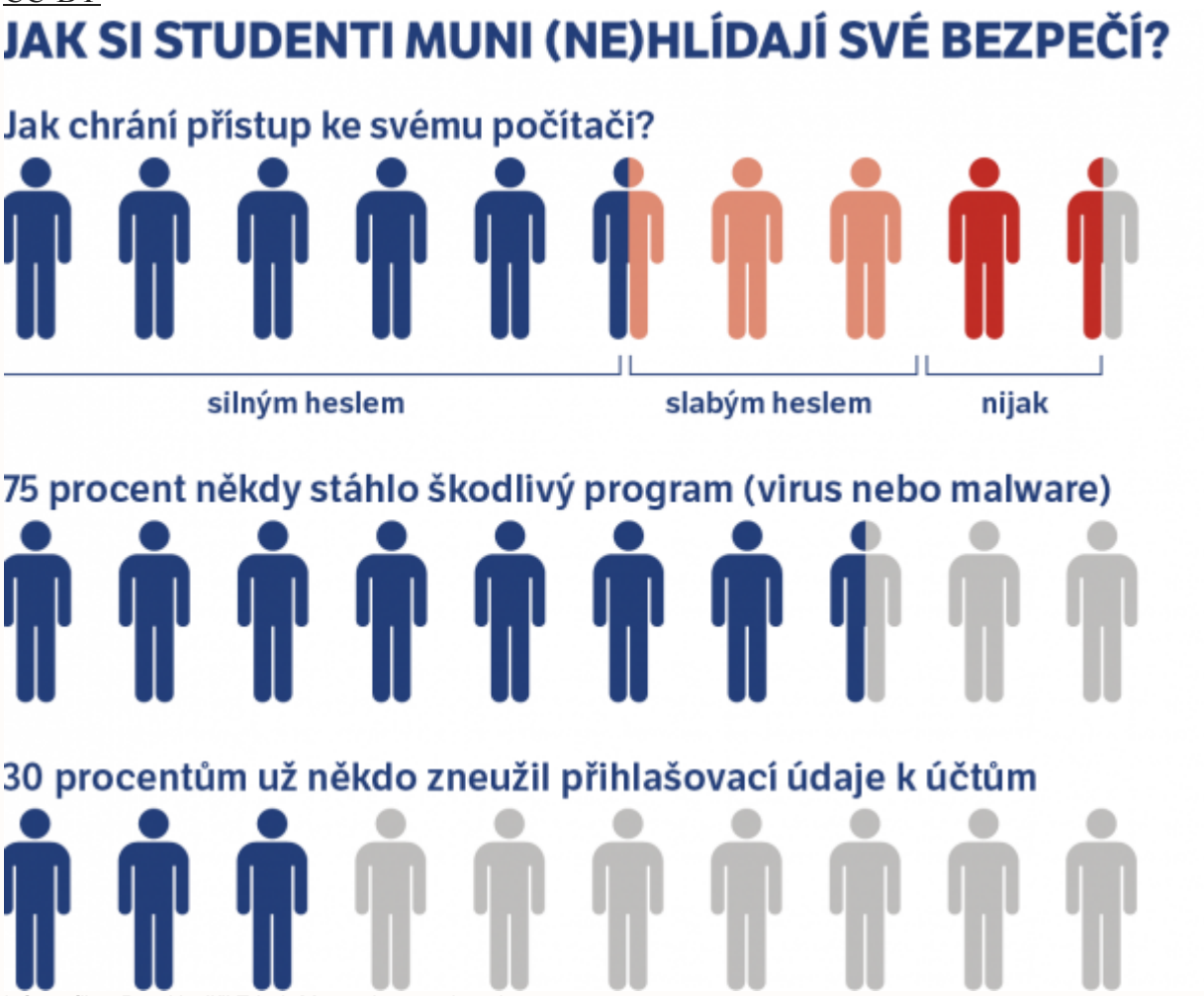
Odkaz: https://www.online.muni.cz/veda-a-vyzkum/10276-v-kyberprostoru-je-nejvetsim-nebezpecim-clovek-sam-sobe

Průzkum: Jak si studenti hlídají své bezpečí v kyberprostoru

věda & výzkum

26. února 2018

Martina Fojtů



Infografika: Petr Hrnčíř Zdroj: Masarykova univerzita

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

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.

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 (například Osel1984kytkA%humorist). 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**.

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 MU 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 (po přihlášení dostupná v IS MU)**, 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 z Fakulty sociálních studií MU 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.

„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 MU, 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.