**Češi na internetu zbytečně riskují aneb čtyři časté chyby v nakládání s osobními daty**

**PRAHA, 15. PROSINCE 2021 – K internetu se denně připojuje přes 80 procent Čechů starších 16 let. Jen málokdo z nich si ale uvědomuje, jaké datové stopy po sobě na internetu zanechává a komu nevědomky poskytuje své osobní údaje. Jakých chyb v ochraně svých dat se lidé nejčastěji dopouštějí?**

**1. MANIPULACE S HESLY**

Odborníci se shodují, že psát si hesla na jedno místo je špatně – notýsky, útržky papíru v peněžence nebo složky s názvem „hesla“ v počítači jdou snadno odcizit. Přesto to podle červnového průzkumu společnosti ESET a Seznam.cz dělá bezmála třetina Čechů. Stejnou chybou je mít jedno heslo pro více účtů. „Silná hesla vyžadují osm až 12 znaků, kromě písmen a čísel je dobré zařadit také symboly jako hvězdičku, pomlčku, plus, podtržítko, tečku a podobně. To však ve světě zahlceném hesly nikdo v hlavě neudrží. K jejich bezpečnému uchování existují zašifrované softwary, které umožňují snadno schraňovat hesla ke všem svým účtům. Některé z nich je možné propojit i s prohlížečem,“ vysvětlil Martin Vodička, ředitel Soukromé střední školy výpočetní techniky (SSŠVT).

Velké riziko úniku dat s sebou nese ukládání hesel do prohlížeče v mobilním zařízení nebo ve veřejně přístupném počítači v zaměstnání. „Pro firmy je obecně ochrana a uchování dat velmi důležité téma, ale už neřeší, že v kanceláři s desítkami pracovníků má každý ve svém prohlížeči uloženo plno hesel a někteří své počítače při odchodu ani nevypínají. Takže tomu, kdo by na tom měl zájem, jednoduše stačí přijít k jakémukoli počítači a tam citlivá data získat, aniž by musel nabourávat server. V takové situaci firmě nepomůže ani nejvíc sofistikovaný systém na ochranu dat,“ dodal Martin Vodička.

**2. DŮVĚRA VE VEŘEJNÉ SÍTĚ**

Velký pozor by si lidé měli dávat u veřejných bezdrátových sítí, které nejsou chráněny heslem. Internetová komunikace na veřejné wifi může být sledována, případně i měněna. A to buď provozovatelem dané wifi, nebo při špatném zabezpečení i třetí stranou. Jedním ze způsobů, jak se proti úniku dat chránit, je využití virtuální soukromé sítě (VPN). „Ta vytvoří mezi uživatelem a vzdáleným serverem šifrované spojení a brání tak odposlechu komunikace ve wifi síti. Na veřejných sítích je uživatel lehce sledovatelný – veškerou svou on-line aktivitou po sobě zanechává stopy, odhaluje své zájmy, polohu, důležité informace. Správně nastavené VPN připojení svého uživatele chrání a je v boji proti kybernetickým útokům velkým pomocníkem. Přesto by ani na to lidé neměli spoléhat a manipulaci s citlivými daty, jako je například internetové bankovnictví, na veřejných sítích neprovádět, vždy by si pro takové úkony měli zapnout mobilní data,“ varoval Martin Vodička.

**3. DATA SVĚŘENÁ E-SHOPŮM**

On-line nákupy bývají spojeny s přijmutím tzv. cookies. Když uživatel internetu navštíví web, vyskočí na něj box s obsáhlým textem a tlačítkem na přijmutí, v lepším případě možností nastavení. „Většina lidí okamžitě přijme vše a nezajímají se, co si díky tomu o nich web uloží za informace. Málokdo věnuje pozornost a čas osobnímu nastavení cookies, na které má ale podle současných pravidel nárok. Když například návštěvník webu nechá zaškrtnuté cookies pro marketingové účely, je pravděpodobné, že se mu budou zobrazovat personalizované nevyžádané reklamy,“ poukázal Martin Vodička.

**4. OTVÍRÁNÍ NEZNÁMÝCH PŘÍLOH**

Tzv. spamy ohrožují data v počítači nejčastěji – někdy jsou snadno rozpoznatelné, jindy se ale tváří jako věrohodná e-mailová zpráva od poskytovatele služeb. „Ke každé zprávě od neznámého odesílatele je třeba přistupovat opatrně, zkontrolovat e-mail, ze kterého byla zpráva odeslána, to bývá první indicií, že nezní jako obvyklé formální adresy. Sdělení bývá naléhavé, nutí adresáta, aby rozklikl přílohu nebo odkaz, to je další indicie. Pokud se navíc jedná o služby, které v posledních dnech adresát nijak nepoptával, nabídku peněz, zázračného produktu nebo naopak výzvu k zaplacení dluhu či zadání osobních údajů, je vhodné zprávu ihned označit jako nevyžádanou a smazat,“ popsal Martin Vodička.

Po otevření špatné přílohy může být počítač napaden a veškerá data z něj „putují do světa“. Proto je třeba preventivně myslet na to, co ve své on-line komunikaci uvádět, a co ne. „Informace o heslech nepatří ani do e-mailu, ani na chat, kde jsou po napadení hackerem snadno dohledatelné. Je-li to nutné, hesla by se měla posílat ve formátu obrázku, ve kterém je robot nerozezná, a následně zprávu smazat. Některé portály, když pošlou uživateli nově vygenerované heslo e-mailem, už jej také upozorní, že si má heslo hned změnit, anebo jde pouze o jednorázový přístupový údaj, případně odkaz ke změně. Tento bezpečnější přístup však zatím není pravidlem u všech, proto je žádoucí zprávu s vepsaným heslem z účtu po přečtení smazat,“ doplnil Martin Vodička.

**MLADÍ NEJSOU LEPŠÍ**

Mladá generace se v internetovém prostředí orientuje o něco lépe než ti dříve narození, obvykle však internet vnímá jako svého kamaráda a nijak pečlivě svá osobní data nechrání. „U studentů prvních ročníků býváme překvapeni, jak neopatrně se svými citlivými údaji zacházejí, byť jsou přesvědčeni, že to tak není. Rizikové je zejména jejich chování na sociálních sítích – profily užívají veřejně, propojují se s neznámými lidmi, mají zapnuté sledování polohy nebo sdílí podezřelé zprávy a videa, které slouží k nabourání jejich účtu. Žijí neustále on-line, ale už si nevšímají, zda jsou připojeni k veřejné síti a že mohou být jejich data pro další osoby viditelná. Naším úkolem je studenty v rámci výuky seznámit s bezpečností na internetu a ochranou dat. Když se naučí, jak informační technologie a virtuální svět funguje od základu, pochopí, jak s daty nakládat a co může být naopak riskantní. To v budoucnu využijí v jakékoli profesi i soukromém životě,“ uzavřel ředitel SSŠVT Martin Vodička.

**KONTAKT PRO MÉDIA:**

**Mgr. Eliška Crkovská\_mediální konzultant**

**pear_media logo_fin rgb_bez okraju.jpg**

**+420 605 218 549,** [**eliska@pearmedia.cz**](mailto:eliska@pearmedia.cz) **,** [**pearmedia.cz**](http://www.pearmedia.cz)

**SOUKROMÁ STŘEDNÍ ŠKOLA VÝPOČETNÍ TECHNIKY,** [**www.sssvt.cz**](http://www.sssvt.cz)

Soukromá střední škola výpočetní techniky (SSŠVT) se od svého založení v roce 1994 specializuje na výuku maturitních oborů zaměřených na informační technologie. Zároveň je také spolutvůrcem těchto oborů. V současné době škola nabízí studentům tři specializace: grafické systémy a tvorbu webových stránek, správu počítačových sítí, programování a databázové systémy. Kvalita pedagogického sboru, důraz na samostatné myšlení studentů a neustále modernizované vybavení školy se každý rok promítají do bezmála stoprocentní úspěšnosti absolventů při přijímacích zkouškách na VŠ. Mimo to se studenti uplatňují v širokém spektru zaměstnání spojených s využitím výpočetní techniky a informačních technologií. Roční školné činí 19 500 Kč. SSŠVT je členem Sdružení soukromých škol ČMS.