Internet (nejen) ve školách = napadená síť, ohrožené děti, šmírovaní uživatelé, úniky osobních údajů?

Odvážím se tvrdit, že riziko odpovědi ANO na v titulku položené otázky, je vysoké. Kde? Na vaší škole. A u vás doma taky.

Tak se vás zkusím zeptat.

Používáte na více místech **stejné heslo**? Tak to je velká, velká chyba. Každou chvíli se z médií dozvídáme, z jaké služby zase unikly osobní údaje, často včetně hesel. Jedna ze služeb, která se shromažďováním těchto incidentů zabývá, je Have I Been Pwned (HIBP). Když sem napíšete svůj e-mail, dozvíte se, jestli byl součástí nějakého úniku. Pokud se vám zdá, že to jsou úniky z nějakých neznámých služeb, je to jen nepřehledností tohoto seznamu. Když trochu zapátráte, najdete tam jména jako Twitter, Facebook, Apple, NVIDIA, LinkedIn, Dropbox a třeba také MALL.CZ. A mimochodem, pokud jste školní IŤáci, určitě nepřehlédněte Domain search.

Ale abych se vrátil... k těm stejným heslům. Když už jednou vaše heslo uniklo nebo když ho někdo uhodne, protože je slabé, určitě ho zlí hoši (od pověstmi opředeného „hackera“ po naštvaného studenta či zvědavého kolegu) začnou zkoušet, kde se dá, a také se stane součástí nejrůznějších databází hesel. A pokud jej máte na více službách stejné, hodně riskujete. Pokud ho máte pouze podobné, riskujete jen o něco málo méně.

Takže, každá služba, jiné heslo. Opravdu nechcete, aby vám někdo sebral e-mailovou schránku a resetoval hesla na účtech, které na ni máte napojeny. Nebo vám ukradl účet na sociální síti a začal vaše přátele zkoušet, jestli by neposlali telefonní číslo, pětistovku... A příjemný není ani průnik do míst, kde máte citlivá data, nebo jste na nich nechali pár hodin/dní/týdnů práce. Ano, dvoufázové ověření je moc dobrý nápad. Banky už to snad ani jinak nedovolí. Jen pozor, ať ten druhý faktor nenávratně nezmizí třeba se ztraceným či utopeným mobilem.

A ano, máme hodně účtů, zapamatovat se to nedá. Zvláště, když (velmi správně) používáte dostatečně silná hesla. Ať už jste o **správci hesel** slyšeli nebo ne, je určitě ten pravý čas začít ho používat. A je vcelku jedno, zda si vyberete Bitwarden, český Sticky Password či staromilský opensourcový KeePass (popř. KeePassXC).

Ukládáte hesla do prohlížeče? Pokud je nechráníte hlavním (primárním) heslem, jsou pro výše definované zlé hochy lehce dosažitelné. A když svá hesla uložíte ve sdíleném zařízení do sdíleného profilu (PC ve sborovně, zapůjčený školní NTB...), bude možná bezpečnější napsat je na monitor ;-)

I když použití hlavního hesla v prohlížeči ochranu vašich uložených hesel podstatně zvýší, je určitě lepší nápad použít na odbornou práci odborníka – zmíněného správce hesel. A kromě hesel může být užitečné poznačit si do něj také číslo občanky, pasu, rodná čísla rodinných příslušníků, PUK sim karty, VIN auta...

Je nejvyšší čas myšlenku opustit. Tak teď třeba něco k vašim kamarádům.

Máte alespoň jednoho opravdu dobrého, který s vámi chodí po ulicích, dívá se vám přes rameno, když píšete maily, čtete noviny a prohlížíte rodinné fotky? Takového, který ví, o co se zajímáte a s kým, kdy a kde se potkáváte, kam chodíte do hospody a jezdíte na dovolenou? Navíc se zajímá o vaše zdraví, o on-line aktivity, kterým se věnujete, o vaše názory na to i ono? A ještě to vše pro vás dělá zadarmo, chce maximálně pár vašich I Agree?

Já myslím, že máte. Třeba strejdu **Google** s bráchou Androidem. Hodně toho zvládne i kámoš Facebook. A pokud máte rádi asijskou exotiku, možná u vás tuto roli přebral mladý dravý asijský synovec TikTok. Ale nejvíc toho zvládne asi ten strejda...

Zkusili jste někdy prohlížeč Firefox (Mozilla)? Vedle Safari (Apple) je to jeden z mála významnějších prohlížečů, které neběží na chromiu (Google...). A i proto je velmi dobrý nápad běžně Firefox používat. Když chybí konkurence, však vy víte co... Určitě jej zkuste alespoň kvůli doplňku Lightbeam. Ten vám ukáže, jak jsou weby propojeny službami třetích stran. Nainstalujte si jej, dva dny používejte internet, jak jste zvyklí, a pak se mrkněte. Asi budete překvapeni, co všechno je propojeno.

Samozřejmě, Google má spoustu skvělých služeb. A většina je, pro nás *normální lidi*, zadarmo (např. Chrome, který se mnohým uživatelům zjevil na PC, aniž by tušili jak). Asi pro tuto svou vášeň ve filantropii má jedna z největších světových společností Alphabet, matka Google, hodnotu okolo bilionu dolarů. A největší část jejích tržeb tvoří reklama. Cílená. *Pokud neplatíte za produkt, produktem jste vy.*

Má to nějaké řešení? Hlavní je si to uvědomit. A třeba nepsat do různých služeb svá osobní data a svůj hlavní e-mail, či dokonce osobní data svěřených osob (ať již školou či přírodou), jen pro to, že si o to řeknou. A třeba nebýt pořád přihlášený na Google, Facebooku, Seznamu... když surfujete úplně někde jinde. Pomůžou anonymní okna prohlížečů (Ctrl-N, Ctrl-Shift-P). A ještě více nejrůznější anonymizační doplňky jako Privacy Badger, uBlock Origin či rovnou prohlížeče na soukromí zaměřené – Brave, Vivaldi nebo těžká váha Tor Browser. Nebo alespoň prohlížeč tak trochu alternativní, jako je právě NEchromiácký Firefox. BTW, pokud by se zalíbil IT správcům, Firefox ESR je do školní sítě ten pravý. Stejně je dobrým zvykem mít na (školním) PC alespoň dva, lépe tři prohlížeče, tak proč nezkusit něco méně mainstreamového.

Ano, **soukromí stojí úsilí**. Některé weby se nemusí zobrazovat v plné kráse, budete si zvykat, testovat. Druhá možnost je spolknout modrou kapsli označenou „I Agree“, vyplnit, zalogovat se a zapomenout... A pak se někdy v budoucnu divit, kam ten svět spěje a proč se na monitoru shora dolů sypou zelená písmenka ;-) Že jsem se nějak moc rozfilozofoval? Ale kdepak, vždyť jsem ještě ani slovem nezavadil o **AI**!

A neměli bychom vynechat děti, na které se i ve školách, po vyřízení nezbytné administrativy, také často dostane.

Co tedy můžeme pro děti udělat, aby byly na internetu bezpečnější?

Zaprvé jim **neškoďte**. Třeba nestrkejte jejich fotky na internet pro oblažení rodiny a těch pár (stovek) opravdu nejbližších přátel na sociálních sítích. Teď jim to nevadí a stejně jako vy neví, že to může být protiprávní. Ale až povyrostou a někdo si je vybere jako cíl kyberšikany, stalkingu atp., asi vám za zveřejnění fotek a různých „cool“ informací o nich, které agresoři zneužijí, nepoděkují. „Mne ani nenapadlo, že by...“ už vám pak moc nepomůže.

Zadruhé, když jsou malé, **zajímejte se**, co dělají, a občas (co nejčastěji) buďte na internetu s nimi. Asi vás nebudou bavit jejich oblíbení Youtubeři a další „pitomosti“, které na mobilu sledují. Ale překonejte se, mluvte o tom s nimi. Jen tak jim můžete pomoci vstřebat sprosťárny, násilnosti či jiné „úlety“, na které dříve či později narazí. Vysvětlete jim, že v diskuzích a komentářích na ně může být někdo dost zlý nebo s nimi může manipulovat. Vysvětlete jim, proč je k různým věcem pouštíte postupně. Řekněte jim, že když budou v komunikaci s kamarády hrubé (děti sprosťárny milují), můžou se dostat někam, kam nechtěly (třeba přijít o kamaráda či někoho vyprovokovat k přitvrzení).

Také jim ty internety můžete zakázat a nedat jim před pubertou mobil do ruky. Jenomže to budou mezi vrstevníky out. A to oni nechtějí a vy byste také neměli. Stejně se k těm internetům dostanou a vy přijdete o možnost je tou džunglí provést. To neznamená, že byste neměli zavést nějaký režim, třeba **rodičovské kontroly**. U Apple je to součástí systému, ve Windows můžete zkusit Microsoft Family Safety,

či Google Family Link na Androidu. Na Androidu či Windows bych se osobně raději podíval na kontrolu v aplikacích 3. stran, třeba v Bitdefenderu, nebo u ESETu.

Předchozí řádky byly cílené hlavně na rodiče, ovšem i učitelé by měli vědět, co jejich svěřenci v on-line prostoru potkávají.

Takže zatřetí – **poraďte jim**, jste přece učitelé. A abyste jim mohli poradit dobře, **vzdělávejte se**.

Požádejte o spolupráci vaše IŤáky, nebo lidi, kteří se prováděním dětí internetovou džunglí profesně zabývají. Popravdě, pokud se rizikům internetu pro běžného uživatele a děti sami intenzivně nevěnujete, nemáte moc šanci, vývoj je opravdu rychlý. A vy přece musíte dopsat ty papíry, výkazy, přehledy... Takže to svěřte odborníkům. Osvícené vedení školy na to má určitě svůj plán, ale klidné to zařiďte „zdola“. Pár tipů: https://skolavbezpeci.cz/, https://www.e-bezpeci.cz/, https://revize.edu.cz/knihovna-inspirace-kyberbezpecnost, https://spajk.cz/deti/

Tento článek se o pár věcí jen otřel, ale je toho mnohem víc. Velkou spoustu informací najdete na internetu. Možná až moc velkou, kdo se v tom má vyznat... I v rámci IKAPu proběhly v poslední době webináře, které byly na kyberbezpečnost zaměřené. Jsou to hodiny zajímavého povídání. Ano, je to hodně času. Ale o věci, které takto bezprecedentně prostupují naše profesní i osobní životy, bychom se zajímat měli. Záznamy IKAP webinářů mají doprovodný minutovník, který vám umožní zhlédnout jen to, co vás aktuálně zajímá nejvíc. A taky se dají spustit rychleji, třeba hodnota 1,5× je docela fajn... U čeho bylo možné, jsou vloženy odkazy, nemusíte tedy skoro nic hledat.

Na stránce IKAP.cz / Centrum multimediálních technologií, hledejte „Záznamy z webinářů“. Tři z nich lektoroval Pavel Matějíček (spajk.cz). Jsou to *Kybernetická bezpečnost pro uživatele*, *Ochrana dětí v kyberprostoru* a *Ochrana soukromí a osobních údajů v kyberprostoru*. Webinář *Zabezpečení školní sítě*, určený spíše správcům, vedl Martin Haller (martinhaller.cz). Kromě kyberbezpečnosti zde najdete také něco z oblasti fyziky, mobilních digitálních učeben, programování... Mrkněte.

A ještě, než to zabalíme, dojte i na umělou inteligenci. A také na hackování, samozřejmě to etické (11. 10. 2023), podrobnosti hledejte na webu ikap.cz/udalosti/.

Za IKAP tým z Centra multimediálních technologií zdraví

Hynek Procházka

Vysoká škola logistiky, hp@vslg.cz

.