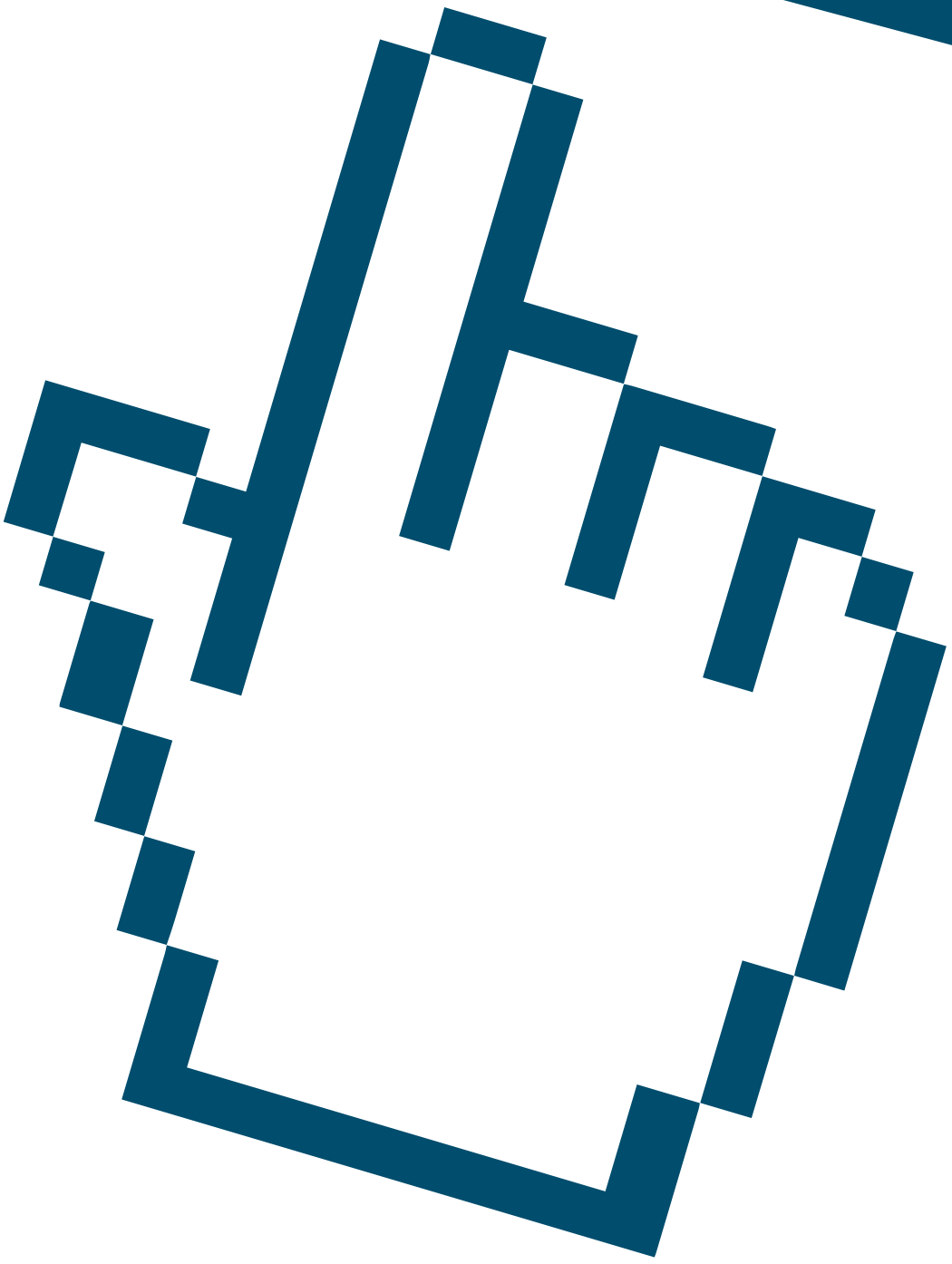
Internet s rozumem



Viktor Janouch

Publikace je spolufinancována za podpory sponzorů:

2. vydání
Responsio Services

O projektu

Naše společnost Responsio Services se zabývá profesionálně online marketingem. Vždy jsme dbali na to, abychom našim firemním zákazníkům poskytli nejlepší služby při dodržení etických pravidel. Lidé ale nevědí, jakým způsobem jsou ovlivňováni a jak s nimi manipulují jiné firmy, které nemají žádné etické zábrany. A vůbec nejhorší je, když svoji manipulaci zaměřují na děti a teenagery. Takové přístupy odmítáme a chceme před nimi varovat. A to je důvod, proč jsme se rozhodli spustit projekt s názvem Internet s rozumem.

Chceme, aby se děti, studenti, učitelé, rodiče i široká veřejnost seznámila se základními pravidly chování na internetu. Aby všichni věděli, jak a proč je někdo sleduje, jak to může ovlivnit jejich názory a postoje, nákupní chování, vztahy, studium, zaměstnání a v podstatě celý život.

Na seminářích/přednáškách ukazujeme mnoho příkladů, co se může stát, pokud člověk není opatrný a jaké to má dopady. To vše se dozvíte také z této publikace.

Úvod

Informace jsou všude. Můžeme se dozvědět, kolik uloví rybář v indické vesnici ryb, jak bydlí lidé uprostřed pouště nebo co měl včera domorodec v pralese k snídani. Ale chceme to vědět? To je první otázka? A ta druhá zní: Je to pravda?

Myslím, že většina z nás určitě nechce vědět všechno. Navíc záplava informací, polopravd a lží se dostala na takovou úroveň, že nesledováním zpráv, například na mnohých televizních stanicích, si vlastně z informačního pohledu polepšíme. Nedozvíme se totiž plno nesmyslů, plků a lží, které by jinak zahltily naši mysl a nutily nás přemýšlet nad věcmi, které nám mohou být ukradené.

Jako dospělí jsme ještě schopni řadu věcí odhalit, ale co naše děti? Zkusme se společně zamyslet, jak se sami zdokonalit ve vnímání informací a zlepšit svoje znalosti o fungování médií. Toto pak musíme vhodnou formou předat našim dětem.

Tato kniha se nezabývá internetovou kriminalitou. Na téma kyberkriminality bylo napsáno mnoho a je realizováno několik přínosných projektů. V této publikaci chceme ukázat, jak se mají lidé (všichni, kdo umí číst a psát) chovat a této kriminalitě tak předcházet.

1 Jak funguje internet

Na Internetu je možné nalézt prakticky cokoliv. Každý může vložit téměř, co chce a zdá se, že v tom začíná být zásadní problém. Přestože jsou na internetu nejrůznější informace, nalézt je může být velmi obtížné. Až 80% obsahu, který se k nám dostane pomocí vyhledávání, zpráv, sociálních médií apod. je cílených. Jak je to možné?

Především je to díky našemu chování. Tím, jak hledáme na internetu (ve vyhledávači) a brouzdáme po stránkách, shromažďuje o nás vyhledávač a všechny weby, které navštívíme, informace. Tyto informace se ukládají pro prohlížeče a říká se jim cookies. Dále si vyhledávač ukládá historii našeho vyhledávání a také informaci na jakou stránku jsem ve výsledcích proklikli.

Weby mohou také analyzovat naše chování na stránkách a na tomto základě pak vytvářet speciální reklamu. Analyzuje se rovněž aktivita na sociálních sítích a dalších sdílených médiích. Tyto služby pak mají o svých uživatelích obrovské množství informací a mohou si s nimi dělat prakticky, co chtějí.

„Shromažďujeme obsah, komunikaci a další informace, které poskytujete při používání našich produktů.“

Toto je část obchodních podmínek služby Facebook. Je zřejmé, že uživatelé nad „svými“ aktivitami nemají žádnou moc.

Díky všem výše uvedeným skutečnostem se tak paradoxně stává, že reklama je často více relevantní než tzv. přirozené výsledky ve vyhledávání.

A ještě jedna poznámka: co je jednou na internet vloženo, to tam taky zůstane. (Téměř) nikdy se nic neztratí, i když je to zdánlivě smazáno.
To je velmi důležitý aspekt.

Na stránce web.archive.org lze například ověřit například, jak vypadaly webové stránky nějaké firmy třeba před 10 lety.

2 Manipulace

Dnešní média jsou zcela jiná než dříve. Lidé jim však stále věří. Říkali to v televizi, tak to musí být pravda. Tímto si lidé zjednodušili život, nemusí totiž nad ničím přemýšlet. Dnes se vše přesouvá na internet, a tak už to neříkali v televizi, ale psali to na fejsu, poslal mě to můj známý / kamarádka nebo kamarádka apod.

Jenže v tom je problém. Nejenže co se píše na různých diskuzích a různých zpravodajských portálech **není v drtivé většině pravda** (to jsou zjištění seriózních výzkumů), ale mnoho lidí se nechá nachytat a šíří dál zjevné nesmysly a účastní se aktivně diskuzí pod falešnou zprávou. Tím se stává z podvodu „skutečnost".

Avšak lidé, kteří šíří nesmysly, vůbec nemusí být skuteční (poslat něco z cizího emailu je to nejjednodušší) nebo vypadají jako skuteční, ale nejsou. Jsou to najatí trollové.

Falešná videa vytvořená za pomoci strojového učení se objevují čím dál častěji. Na jednom z nich vystupuje dokonce sám Mark Zuckerberg, zakladatel Facebooku. Ten zde říká: „Na vteřinu si představte tohle: Jeden muž s totální kontrolou nad ukradenými údaji miliard lidí. Všechna jejich tajemství, jejich životy, jejich budoucnost... ten, kdo ovládá data, ovládá budoucnost." Nic takového ale nikdy neřekl. Video bylo součástí kampaně, která měla ukázat lidem, aby nevěřili nejen všemu, co čtou, ale také tomu, co vidí a slyší.

Jako ukázka, kam je možné dnes zajít díky pokročilým technologiím, může posloužit film Matrix. Hlavní roli v něm ztvárnil Keenu Reeves.
Ale co kdyby ho hrál Will Smith?

Dalším problémem jsou zdánlivě seriózní zprávy na veřejnoprávních médiích (BBC, ČT apod.). I zde musíme být obezřetní a nevěřit všemu, co vidíme a slyšíme.

Redaktor BBC ukazuje, jak se pomocí programu změnila jeho ústa a navíc jeho hlasem jsou prezentovány falešné zprávy v dalších jazycích. Na tomto videu například bulharsky nebo čínsky. Toto je ale čirá manipulaci, kterou můžeme najít třeba na YouTube. Co ale v případě, kdy vidíme a slyšíme něco třeba přímo v televizi.

Když po přehrání tohoto videa necháte načíst další video, uvidíte v něm pokus z anglické školy s falešnými zprávami. Dětem byly předloženy 3 zprávy a všechny falešné. Vypadaly ale věrohodně, a tak jim děti lehce uvěřily. Obě videa jsou sice v angličtině, ale podstatě porozumí každý.

Falešné zprávy také vyvolávají falešné vzpomínky.
To je již delší dobu zcela prokázáno.

Již před mnoha lety chtěla jedna česká agentura dokázat, jak je reklama účinná a vytvořila kampaň na neexistující mléko (probíhala pouze v Praze). Následně se pak v průzkumech ptali lidí, zda ho kupují a jak jsou s ním spokojeni. Nejméně polovina dotázaných potvrdila, že značku zná a mnozí tvrdili, že má skvělou chuť, kupují ho dětem apod.

3 Kdo a proč nás sleduje

Kdo nás sleduje

Sledují nás doslova všichni. Technicky vzato, je to **každý web**, na který se dostanete a **každá aplikace**, kterou máme v mobilu. Začíná to od samotného vyhledávače, kam zadáváte hledaná slova, přes e-shopy, zájmové a zpravodajské portály až po sociální média. Všechny weby si ukládají informace, které později mohou využít. Ukládají se také emaily, chaty, v podstatě úplně všechno.

Největší nebezpečí však představují **sdílené platformy**. Problémem tak není jen největší sociální síť Facebook, ale všechny sítě, kde se cokoliv sdílí, zejména fotky a videa. Dále jsou nebezpečná jakákoliv diskusní fóra, a dokonce i komentáře pod články, které mohou prozradit, co nechceme.

Proč nás sledují

→ Reklama

Firmy chtějí **prodat svoje produkty**. Reklama v online světě je vysoce sofistikovaná. Lze ji velmi přesně zacílit a také vyhodnotit její účinnost. A k cílení se používají právě data získaná z chování zákazníků.

Určitě jste si všimli, že se vám zobrazuje reklama zdánlivě nesouvisející s obsahem, který si právě na webu prohlížíte. Jedná se pravděpodobně o tzv. remarketing. Ten využívá z dat z vašeho předchozího chování a firmy jsou tak schopny vás sledovat kdekoliv.

→ Chování

Určité skupiny, jednotlivci i státy mají zájem na tom, aby se lidé chovali pro ně prospěšným způsobem. Chtějí třeba, aby si lidé něco mysleli, nebo naopak aby vůbec nemysleli. Takto ovlivnění lidé pak zase ovlivňují své okolí a postupně rozšiřují okruh lidí s nějakým názorem.

Hlubší ovlivnění pak již hraničí s vírou v něco nebo někoho. Víra se neopírá o fakta a realitu, ale o pocity. Dost často se tvrdí, že člověk je tvor racionální, vše promýšlí, zvažuje nejlepší možná řešení. Četné výzkumy ukazují, že tomu tak není a nechá se **velmi snadno ovlivnit.**

→ Peníze

Krádeže dat jsou výnosnou kriminální činností. Digitální kriminalita se zaměřuje **na krádeže dat z kreditních karet a přístupů k účtům**, což následně vede ke krádeži peněz. V drtivé většině případů si za to však můžeme sami tím, že necháme svá data nezabezpečená. Samotný přenos dat je totiž bezpečný. Používá se k tomu například šifrování pomocí prvočísel a mnoho jiných metod. Při platbách v e-shopech se dnes již běžně používá 3D zabezpečení, kdy musíte zadat nejen údaje z platební karty, ale také kód, který vám přijde přes SMS.

Při vybírání peněz z bankomatů hrozí také značné nebezpečí. Donedávna se zdálo, že se problém skimmingu (kopírování údajů z karet) dá překonat bezdotykovými systémy, ale to již neplatí. Existují zařízení, které zkopírují data z karty i do vzdálenosti 10 cm (zatím).

Problém je tedy především u nás: náš vlastní počítač, tablet nebo mobil a hlavně naše lehkomyslnost. O způsobech, jak se chránit, budeme mluvit dále.

→ Informace

Říká se, že dnešní informace mají cenu zlata. Domnívám se, že to je ještě hrubě podceněno. Svými aktivitami poskytujeme v online světě, a dnes i mimo něj, obrovské množství cenných informací o tom, jací jsme, co děláme, co nakupujeme, o co se zajímáme, jaký máme politický názor a mnoho dalšího. Nemusíme se ani k ničemu vyjadřovat, stačí jen navštěvovat určité stránky a zadávat slova do vyhledávačů. Vše ostatní si už přeberou jiní a jinde.

4 Kritické myšlení

Internet přinesl do života radikální změny. Najednou má každý, kdo se připojí, k dispozici neuvěřitelné množství informací (otázka je, co je to informace). Jenže jaká je jejich hodnota? Jsou pravdivé, ověřitelné, důvěryhodné, můžeme se na ně spolehnout nebo naopak máme mít a priori pochybnosti? Na tyto otázky nelze odpovědět jednou větou. Zabývejme se proto jakým způsobem informace přijímat, třídit a hodnotit. V tom nám pomůže tzv. kritické myšlení.

Pro výuku kritického myšlení ve školách podává určitý návod Homerová. Jde sice o text již staršího data (2009), ale v principu je stále aktuální.

Kritické myšlení znamená, že člověk nepodlehne prvnímu dojmu, nepřidá se k davu a nenechá se zviklat naléhavostí sdělení. Asi všichni známe ty emaily, že musíme teď hned rychle něco udělat, přeposlat zprávu nebo dokonce zaplatit, jinak se stane něco strašného. Podobně je tomu ve všech oblastech života, kdy je například vyžadována okamžitá reakce na něco, co se třeba vůbec nestalo. Nejlepší je na takové informace vůbec nereagovat. Pokud ale chceme zaujmout nějaký postoj, pak raději až po určité době a hlavně teprve po ověření zprávy z jiných zdrojů. Není na škodu zaujmout zcela opačný pohled a zamyslet se nad vlastními zkušenostmi. Tento mix činností a postojů je většinou tím správným pro udržení si zdravého rozumu a nepodlehnutí prvnímu dojmu.

Jak by mělo fungovat kritické myšlení, si můžeme ukázat na několika příkladech.

Například vědci pracují s různými hypotézami a snaží se je potvrdit nebo vyvrátit. Potvrzení nebo vyvrácení nějaké hypotézy však ještě nestačí k tomu, abychom vyslovili verdikt o pravdivosti či nepravdivosti. Slavný příklad uvádí Taleb ve své knize Černá labuť. Ještě v 60. letech 20. století si lidé mysleli, že existují jen bílé labutě. Pak se však náhle objevila v Austrálii labuť černá. Na tomto problému můžeme demonstrovat, jak přijímat určitá tvrzení. Pokud byla vyslovena hypotéza, že existují jen bílé labutě, pak je tato hypotéza z principu nepravdivá. Nikdo ji totiž nemůže dokázat. Musel by prozkoumat celý vesmír bod po bodu, aby zcela vyloučil, že někde neexistuje labuť jiné než bílé barvy. Naopak, kdyby byla hypotéza opačná, tj. neexistují jen bílé labutě, bylo by ji možné dokázat nalezením labutě jiné barvy. Když by se taková labuť nenašla, tak by závěr byl, že hypotézu se nepodařilo ověřit.

Možná to byl trochu složitější příklad, ale pokud si osvojíme tento způsob myšlení, neměli bychom se nechat jen tak nachytat na různá tvrzení. Ale podívejme se na to ještě jinak. Pokud můžeme nějaké tvrzení opřít o důkazy jeho platnosti, měli bychom také říct, za jakých podmínek by tvrzení neplatilo. Jestliže nemůžeme žádný takový předpoklad najít, pak je tvrzení chybné. Jakékoliv tvrzení tedy může být vyvráceno nebo zpochybněno. Bylo by však velkou chybou připustit naprosto demagogický výrok, že každý má kus pravdy.

Tímto se dostáváme k funkci oponentury. Jde o kritické posouzení určité argumentace. V žádném případě to ale neznamená opačný postoj. Je potřeba zjistit, zda je problém správně definován a vyslovené závěry jsou oprávněné. Oponent zkoumá oprávněnost použitých zdrojů a uváděných fakt a způsob jejich užití. Dále má zjistit, zda nedošlo k opomenutí nebo vyloučení některých zdrojů a zda je cesta k řešení problému konzistentní.

V této části hodí připomenout tzv. Hitchensovu břitvu: „To, co může být přijato bez důkazů, může být i bez důkazů odmítnuto.“

5 Problematika zpráv

Tomu, že nějaký text ještě nemusí být pravdivý, se dá uvěřit. Ale uvěřit, že není pravda to, co vidím na obrázku nebo dokonce na videu je mnohem obtížnější. Obrázek, o videu ani nemluvě, vytváří dojem objektivity, což v mnoha případech není vůbec pravda. Navíc to může být záměrně zmanipulované, sestříhané, upravené. Lidé si tak myslí, že se stávají očitými svědky, ale neznají místo, čas, pozadí ani co tomu předcházelo, případně jak se to vyvíjelo dál.

Jenže toto většinu lidí vůbec nezajímá. Chceme stále pouze aktuální zprávy. Ale co to znamená? Co když se aktualita ukáže jako nepravda a bude nutné ji aktualizovat? Ne jednou, ale mnohokrát. Většinou je už na změnu názoru pozdě. Co bylo včera nebo dokonce před hodinou je zabetonováno ve stavu v jakém jsme to slyšeli nebo viděli. Lidé nejsou ochotni měnit názor. Pouze v určitých případech, kdy se něčemu věnuje v médiích masivní pozornost, jsme ochotni přestoupit na druhou názorovou stranu nebo alespoň svůj názor poupravit.

V médiích téměř nejsou autentické zprávy ve formě přímého svědectví. Na první pohled to však vypadá, že jsou. Vždy se objeví někdo, kdo v 1-2 větách řekne, že něco viděl nebo zažil. Problém je, že jde právě jen o pár vět a nevíme nic dalšího. Přímé ale svědectví znamená, že nám zprávu řekne nejen někdo, kdo byl očitým svědkem, ale někdo, koho známe a můžeme mu věřit. Forma sdělení je přitom důležitá. Sdělení musí být osobní (tváří v tvář, telefon), protože i přátelé na sociální síti vůbec nemusí být těmi, za koho je považujeme. Také systém (sociální síť) sám může vytvářet zprávy za uživatele a také to dělá. Jde o udržení uživatelů na stránkách co nejdéle, aby se jim mohlo zobrazit co největší množství reklam. Různé pseudozprávy se šíří také prostřednictvím emailů. Pro tyto emaily se užívá pojem hoax, což je šíření různých falešných a poplašných zpráv, mystifikací, výmyslů a podvodů.

Na internetu jsou některé weby vytvářeny čistě za účelem matení lidí a sloužící často zájmům cizích států. Tyto weby jsou označovány jako dezinformační a je lépe se jim zdaleka vyhnout. Jejich seznam najdete na webu Konšpirátory.sk. K tomuto seznamu bychom mohli přidat také řadu webů, které produkují směs pravdy a dezinformace, a o to jsou nebezpečnější. Typickým představitelem jsou například Parlamentní listy,

K vyvolávání pocitu zmatení a nejistoty slouží i způsob řazení zpráv. V televizních zprávách se skáče z jednoho tématu na druhé, z ciziny domů a naopak, z války na pláž, z politiky na nedostatek nebo přebytek srážek apod. Pak následuje nějaký ten emoční problém (obvykle ztracené nebo veselé zvířátko) a nakonec přichází rozuzlení ve formě zábavy, což je zpravidla sportovní výkon. Hlavně žádné složitosti, nejasnosti, cokoliv, o čem by se dalo přemýšlet nebo nebylo úplně jednoznačné.

Skutečné problémy jsou naopak často ignorovány, zpochybňovány a vytěsňovány ze zpravodajství. Bulvární zprávy naprosto převažují a lidé už ztrácejí schopnost vidět to podstatné a zajímat se o důležité věci. Pak se může snadno stát, že někdo ovládne jejich životy a dostane je do téměř neřešitelné situace. Od nezvladatelných dluhů přes omezení práv a vytváření nových a nových povinností až po nastolení částečné nebo úplné diktatury. A když toto nastane a naše děti, až budou dospělí, se zeptají, co jsme proti tomu udělali, tak budeme muset říct, že nic? Tohle snad nechceme.

Přes všechny problémy jsou již, hlavně v zahraničí, média, která nezveřejní neověřenou zprávu, neukazují násilí a oběti v detailech.

6 Kdo nás ochrání

Česká republika má zákony na ochranu osobních údajů, zákony proti posílání obchodních sdělení (spam), EU přijala řadu hodně přísných opatření na ochranu uživatelů (mj. GDPR). V praxi se však nedá vše uhlídat a některé firmy zákony stejně nedodržují, neuznávají žádná pravidla a nemají zábrany.

Amazon předával data z kamer na zvoncích policii bez vědomí lidí a soudního příkazu.

V Číně chtějí postupně sledovat všechny lidi (už to skoro mají) a podle jejich chování je budou odměňovat nebo trestat. Naopak EU připravuje omezení používání technologií k rozpoznávání obličejů.

V některých státech nebo městech jsou zaváděna opatření proti dronům sledujícím soukromí. Údaje z pouličních kamer nesmí být ukládány déle, než je přesně stanoveno apod.

Musíme se tedy chránit hlavně sami. Jednak svým zdrženlivým chováním a také nastavením některých technických překážek proti našemu sledování a zneužívání dat.

Jak se chránit technicky

Přestože ani dospělí často netuší, že se mohou bránit využitím některých technických nástrojů, je třeba seznámit děti se základy této problematiky. Co bychom měli dělat pro ochranu zařízení, které používáme (počítač, mobil, tablet, televize)?

a) používat antivirus, antispyware, firewall

Antivirový program (antivir) je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého softwaru (zdroj: Wikipedia).

Antispyware je program, jehož úkolem je odstraňovat či blokovat spyware, jež se bez vědomí uživatele natáhl do jeho počítače (zdroj: Wikipedia). Spyware je špionážní (špehovací) program, která posílá data ze zařízení uživatele bez jeho vědomí. Některé velmi nebezpečné spywary posílají hesla, čísla kreditních karet a jiná citlivá data.

Firewall slouží k zabezpečení provozu mezi sítěmi podle určitých pravidel. Tato pravidla zahrnují identifikaci zdroje a cíle dat, a také informace o stavu spojení, protokolech nebo systémech pro odhalení průniku. Jednoduše řečeno jde o zeď, která vás ochrání před útoky a řídí tok dat směrem dovnitř i ven.

b vypnout určování polohy v mobilním zařízení

Tento bod asi nepůjde tak snadno dodržet. Jsme zvyklí se dívat na počasí v místě, kde se právě nacházíme, používáme navigaci, necháváme si doporučit restaurace atd. Sledování polohy je ale hodně nebezpečné a může o nás velmi mnoho prozradit. Polohu také využívají firmy pro cílenou reklamu.

c vypnout automatické připojování k wi-fi

Přes nezabezpečené wi-fi sítě se dostane do našeho zařízení každý průměrný hacker. Cokoliv pak děláme, je sledováno, a pokud se jedná třeba o vkládání citlivých informací, ocitáme se ve velkých problémech.

d práce s aplikacemi

Při instalaci aplikací do vašeho mobilu si pečlivě přečtěte, k jakým datům chce mít aplikace přístup. Pokud například aplikace o počasí žádá přístup k vašim kontaktům, v žádném případě ji nestahujte.

Také dobře zvažte, zda aplikace, které máte nainstalované v mobilu opravdu používáte. Pokud ne, můžete je vymazat a již neobnovovat. Navíc i u těch aplikací, které jsou pro vás užitečné není třeba mít nastavené automatické aktualizace. Nikdy totiž nevíte, jaká další data nad rámec již schválených, po vás bude někdo žádat. Na druhou stranu může aktualizovaná aplikace odstraňovat chyby v zabezpečení.

Ve Španělsku se objevil případ, kdy manžel sledoval manželku pomocí aplikace v mobilu, o které vůbec nevěděla. Tato aplikace sledovala všechno: pohyb, telefony, sms, kontakty, jiné aplikace. Navíc nešlo vůbec zjistit, že má v mobilu tuto aplikaci nainstalovanou. Cena je přitom cca 7€.

e používat hesla

Heslo jako prostředek k ověření totožnosti zdá asi každý. Měli bychom vědět, že pro vyšší bezpečnost je nutné nejen používat tzv. silná hesla, ale také různá hesla pro různé služby nebo weby.

Silné heslo má být dostatečně dlouhé (doporučuje se alespoň 8 znaků), mělo by obsahovat velká i malá písmena, číslice a ještě lépe také různé znaky. Zcela nevhodná jsou pak hesla typu „1234“ nebo „heslo“. Zároveň by mělo být dobře zapamatovatelné. Jako příklad velmi silného hesla pro osobu jménem Jan Novák, narozeného v roce 1962, můžeme uvést třeba toto: Jan62Novak*.

f nastavit chráněný přístup do mobilu

Dnešní mobily a tablety již často umožňují silné zabezpečení přístupu. Kromě běžných hesel tak máme možnost využít zabezpečený přístup například gestem, otiskem palce nebo rozpoznáním tváře. Jestli to váš mobil umí, hned si to nastavte a ukažte dětem, jak na to (ony to možná vědí lépe, ale nepoužívají).

Nastavení chráněného přístupu do mobilu také vede k podstatnému snížení jeho používání.

g jiná zabezpečení

Zde uvádíme ještě několik málo příkladů, jak je možné technicky zabezpečit počítače a mobily.

Poměrně stoupajícím trendem je spuštění webové kamery cizí osobou. Dochází tak ke šmírování a jistě si dovedete představit, že je to zaměřeno i na děti. Zabezpečení je možné buď pomocí software (některé firmy to mají již v rámci antiviru) nebo rovnou kameru přelepit a vypnout mikrofon.

Jestliže se vám „podaří“ ztratit mobil nebo vám jej někdo ukradl, pak přes vyhledávač Google jej lze najít. Zkuste zadat do vyhledávače „kde je můj telefon“a dále postupovat podle pokynů.

K technickým zabezpečením patří i nastavení mazání historie ve vyhledávači, používání anonymních oken prohlížeče, nastavení ochrany počítače v rámci Windows (Nastavení – Soukromí), případně používání speciálních programů jako Destroy Windows 10 Spying.

7 Jak se chovat v online světě

Tento projekt se sice zaměřuje na děti cca ve věku 12–15 let, ale stojí za to připomenout i rodičům mladších dětí, že výchova začíná již zhruba od 2 let. Děti používají média doslova od rána do večera, přesněji pokud nespí. Naštěstí ve školách je již používání mobilů víceméně zakázáno po celou dobu pobytu dětí ve škole, jinak jsou s nimi pořád. Charakteristické je také používání více medií (a zařízení) najednou. Děti si častou čtou časopis a zároveň píšou zprávy na mobilu, případně k tomu ještě sledují televizi. Toto je vede k pocitu, že lze zvládnout více věcí najednou. Důsledky se již dostavují například ve velkém nárůstu mladých řidičů, kteří používají za volantem mobil stejně, jako jsou zvyklí to dělat, i když neřídí.

Mladá generace preferuje mobil, ale nevíme, co přijde po něm, takže jde stále o princip, nikoliv zařízení.

Rodiče neměly na děti v podstatě nikdy čas. Ale zatímco generace dětí, která neměla k dispozici televizi, a později počítače, byla zvyklá se bavit spolu (prostě jsme šli s klukama ven a dělali samozřejmě taky různé blbosti), tak dnešní děti jsou v podstatě sami se svým mobilem nebo tabletem. Pak se nelze divit, že se najde nějaký ten „přítel“, kterému je možné se svěřit, který vždycky ochotně poradí a chápe jejich problémy. Jak to může skončit, víme.

Režisér Klusák natočil dokument o zneužívání dětí na sociálních sítích. Mladistvě vypadající herečky hrály 12leté dívky, které hledají nové přátele. Během hodiny se přihlásilo desítky pedofilů.

Mnozí dnešní rodiče se často věnují dětem mnohem více než předchozí generace. Je to dáno jednak nabídkou aktivit (kultura, sport, cestování) a také uvědomováním si, že když se nebudu dítěti věnovat já, udělá to někdo jiný. A nakonec i prostou nutností dopravit dítě v dopravním chaosu na místo určení (sport, kroužek), což je samozřejmě problém zejména velkých měst.

Často slyšíme, že vyrůstá nová generace, která je jiná než předchozí díky novým technologiím. Jistě, každá generace je jiná než předchozí, ale mozek člověka se vyvíjí jen velmi pomalu a postupně. Na hodnocení současných vlivů je tedy ještě příliš brzy. Spíše se zdá, že jde pouze o technické dovednosti a změnu psychiky, nikoliv změnu mozku. Někteří vědci tvrdí, že evoluce zamrzla, jiní mají opačný názor. Dokonce nejsou ojedinělé názory, že lidstvo dosáhlo vrcholu před 40.000 lety a od té doby degeneruje. U značné části populace to vypadá, že by to mohla být pravda.

Pro děti je internet prostorem, kde se nemusí zodpovídat za své chování a jednají jen podle sebe a svých kamarádů, nikoliv jako v reálném světě, kde je řada zábran. Děti (a často i dospělí) si navíc někdy mění část své identity (věk, pohlaví), čímž si například zvyšují sebevědomí nebo odstraňují zábrany v komunikaci. Děti se stávají závislými na internetu velmi snadno a tato závislost se stává hrozbou. Sem pak přesouvají svoje aktivity a považují to zásadní věc, kterou je třeba dělat. Pokud nemají přístup k internetu, zhoršuje se jim nálada a toužebně očekávají čas, kdy zase budou online. Logicky tak dochází ke konfliktům v rodině a vede to k zanedbávání všeho ostatního, tj. především učení. V oblasti závislostí různé výzkumy ukazují různé výsledky. Společné mají však varování před závislostí na internetu pro děti od 12 let až po VŠ studenty. Studenti vysokých škol jsou navíc nekontrolovatelní (bydlí mimo domov, učí se samostatně) a nelze jim prakticky nic nařídit, jejich závislost tak bývá často hluboká.

Děti nejsou na internetu ohroženy jen kriminálními živly, ale jejich chování může mít dopady na jejich budoucí studium, zaměstnání, seznamování a vůbec na celý život. Nejvíce jsou ohroženy, pokud používají sdílená média, zejména sociální sítě s možností vkládat fotky, videa a texty. Pro děti jsou sítě určitou výhodou – nemusí bezprostředně reagovat, mohou skrývat určité rysy svého chování, nemusí nebo naopak chtějí být jen sami sebou, mohou se „přátelit" jen s jedinci se stejnými zájmy, názory a koníčky – jednoduše nemusí nic „řešit". Avšak často narazí na velké problémy a nic „řešit" se proměňuje v opak. Najednou se mohou objevit výhružky násilím, vydírání, pronásledování, urážky, nadávky. Snadno také uvěří (stejně jako dospělí) falešným zprávám a podle toho pak jednají. Děti se rády ztotožňují s někým, kdo mluví jejich jazykem, chová se podobně a má stejné názory (i když to vše může být a často také je, pouze divadlo). Firmy záměrně vyrábějí tzv. celebrity, aby propagovaly jejich produkty a pokud již nějaká celebrita existuje (tj. vypracovala se sama – díky hudbě, jako youtuber, sportovec apod.), tak se ji firmy snaží získat k ovlivňování svých zákazníků, a to jsou samozřejmě i děti. Pro děti, stejně jako pro jejich rodiče, je důležité vědět, jak funguje internet, média, sociální sítě, reklama a samozřejmě používat kritické myšlení.

Je třeba varovat také rodiče. V USA jsou již případy, kdy děti podávají žalobu na rodiče za to, že na FB vkládali jejich fotky, když byli malí. Na ruských serverech byly zaznamenány případy, kdy se objevily fotografie malých dětí, kterým je však dnes již třeba 20 let.

8 Doporučení

Naše vlastní chování pro nás představuje to největší nebezpečí. Všechno, co jsme kdy udělali v online světě se k nám může kdykoliv vrátit, a to v době nebo situaci, když to budeme nejméně čekat a potřebovat. Čím víc stop zanecháme, tím víc o nás budou jiní vědět. Jaké jsou tedy zásady chování v online světě:

→ nezadávat nikam žádný email, jméno, adresu (kromě nezbytných situací jako jsou online nákupy)

→ nereagovat hned na každou zprávu (počkat 2–3 dny, zda se to potvrdí)

→ omezit zábavu (zábava vede k nevědomému přijímání manipulativních názorů, protože během ní nejsou lidé ostražití a snadno podlehnou; to samé se týká reklamy), navíc hry jsou jen hry není to skutečný život

Doporučení

① Vytvořte doma (i ve škole) prostředí, kde může dítě přijít se svým problémem a mít jistotu, že nebude potrestáno a naopak dostane radu, co má dělat.

② Ptejte se dětí, co dělají na internetu, na sociálních sítích, jaké hrají hry, co je populární. Společně se dívejte do jejich mobilu, kontrolujte nastavení.

Časté používání zařízení vede k stále větší závislosti. Ta jsou za tím účelem vymyšlená, protože pak lze lidem lépe něco prodat nebo podsouvat různé názory. U dětí jde pak o závislost často velmi silnou – na youtuberech, hvězdičkách šoubyznysu, sportovcích.

③ Připravte děti (a také sebe) na nejistou budoucnost. Dnes je tady Facebook, Instagram a další, ale co bylo předtím jsme už zapomněli (MySpace). A co bude potom, nevíme. Očekávejte tedy, že problém nezmizí se zánikem nějaké služby.

④ Vysvětlete dětem, že musí být opatrné při zveřejňování čehokoliv z jejich života. Všechno může někdo zneužít.

Nemusíme za vším hned vidět hrozbu násilných trestných činů. Úplně postačí si uvědomit, že se na sociální síť mohou podívat učitelé na střední škole, kam se dítě hlásí, a zjistit si, jak se chová a jestli s ním není nějaký problém. Stejná situace se může objevit za dalších pár let při přijímání studentů na univerzitu. A nakonec dožene děti a studenty minulost, když se budou ucházet o zaměstnání. Tady už jde do tuhého, protože takové lustrace dělají firmy již dnes (ověřeno z praxe).

⑤ Naučte děti žít jejich vlastní život, ne život podle představ někoho jiného.

⑥ Veďte je k učení jazyků. Je potřeba učit se jazyky, aby si mohli ověřovat informace a podívat se, jaké názory mají jinde.

⑦ Umožněte jim cestovat a upozorněte je, aby si všímaly způsobu, jakým žijí a jak se chovají dospělí lidé i děti a mládež.

⑧ Používejte sami kritické myšlení a jděte dětem příkladem.

Závěrem

Kam se bude ubírat vývoj technologií a s tím změna chování lidí, nevíme. To, co nevíme, nemůžeme ovlivnit, ale můžeme se připravit na tyto rozsáhlé změny alespoň po psychické stránce. Další rozvoj internetu s sebou jistě přinese mnohá překvapení. Už teď je ale jasné, že to nebudou jen samé dobré zprávy. Spíše naopak. Dnes se třeba hodně mluví o tzv. internetu věcí, který má přinést lidem pohodlí a vyřešit za ně spoustu starostí. Například si vaše lednička může objednat z e-shopu jídlo, žárovka se sama zhasne, když opustíte dům, topení se naopak spustí, až se budete vracet. Všechno to vypadá skvěle až na ty možné důsledky. Opravdu chceme, aby kdokoliv věděl, co nakupujeme, jestli jíme zdravě nebo pijeme alkohol? Co když nám pak pojišťovna automaticky na základě těchto dat zvýší pojistku nebo ji odmítne uzavřít? Nebo třeba dodavatel elektřiny špatně zabezpečí data a zloděj se tak pohodlně dozví, kdy nejsme doma.
A podobných problémů bude celá řada.

Asi to vše nevypadá úplně nejlépe a mnozí třeba propadnou skepsi.
Ale pokud budeme dodržovat zásady bezpečného chování a nad věcmi a událostmi přemýšlet, můžeme žít vlastní život a riziko udržovat na přijatelné úrovni.