MEDIÁLNÍ GRAMOTNOST SE VYPLATÍ: VYKECÁVAČKA

OTÁZKY A ODPOVĚDI

1. Co je to Vykecávačka?

Vykecávačka je **vymyšlená aplikace**, která má sloužit ke **sdílení** zpráv, fotografií a příběhů s ostatními uživateli. Kdo bude v této aplikaci nejaktivnější, ten bude obdivovaný a může se stát „králem“ či „královnou“ Vykecávačky.

Problém však nastane ve chvíli, kdy ve snaze zalíbit se a pobavit své kamarády zveřejníme fotografie či informace, za které se později budeme stydět. Zde je třeba si uvědomit, že **co na internet vložíme, už ve většině případů nikdy nesmažeme**. Utváříme si svou **digitální stopu**, a to jak aktivně, tak pasivně. Aktivně svým vlastním přičiněním ve formě příspěvků a pasivně (což si často ani neuvědomujeme) ve formě záznamů serverů o našem chování, například na jak dlouho jsme navštívili danou sociální síť, z jaké IP adresy jsme tam vstupovali a třeba i GPS souřadnice místa, odkud jsme vloženou fotografii pořídili.

Kdo všechno se může dostat k informacím, které o sobě zveřejním na sociální síti?

K informacím, které publikujeme na sociální síti, se dostane primárně ten, komu udělíme souhlas sledovat náš profil a naše příspěvky. **Nastavení soukromí** je proto jedním z prvních kroků, které bychom měli udělat, když si zakládáme účet na sociální síti. Avšak ani to nám nezaručí, že se například naše video nedostane mezi výrazně širší okruh lidí, než bychom si přáli. Stačí, aby ho někdo z přátel sdílel na svém veřejném účtu (ke kterému má přístup každý), a toto video si již začne žít svým vlastním životem a my nad ním zcela **ztrácíme kontrolu**. Nesmíme také zapomínat, že informace o nás sbírají samotné sociální sítě, které je mohou sdílet se třetími stranami nebo využít pro vlastní účely. I tyto data navíc mohou neplánovaně uniknout.

2. Jak s těmito informacemi zacházejí samotné sociální sítě?

Sociální sítě o nás sbírají informace, které jim sami poskytneme. Jak při vyplnění osobního profilu, tak při samotném využívání sítě. Analyzují tak, jaké příspěvky a videa lajkujeme, koho sledujeme, jaké informace vyhledáváme, co nakupujeme nebo v jakou dobu sociální síť obvykle otevíráme.

Sociální sítě o nás také sbírají informace z jiných webových stránek a shromažďují naše **biometrická data** pomocí zveřejněných fotografií, na kterých jsme označeni. Kvůli shromážděným informacím následně dokáží vytušit i naši momentální náladu, potřeby a přání a za pomoci algoritmů a umělé inteligence nám nabízejí obsah, zboží a služby které by nás mohly zajímat. **K tomuto sběru dat však my sami dáváme provozovatelům sociálních sítí souhlas** již při založení účtu. Stačí si důkladně pročíst **smluvní podmínky**, resp. zásady používání dat, které jsou bohužel mnohdy nesrozumitelné nebo psané v jiném jazyce nežli v češtině.

3. Lze již jednou publikované věci na internetu zcela odstranit?

Bohužel ne. Pokud umístíme na sociální sítě nebo jinam na internet fotografii, video či článek, je ihned k dispozici ostatním lidem. Sociální sítě začnou náš příspěvek automaticky zobrazovat našim známým , případně dalším uživatelům, kteří jej mohou dále sdílet, stahovat či upravovat. Nad dalším šířením příspěvku tak velmi rychle ztrácíme kontrolu. Proto se vyplatí řídit starým českým příslovím „**Dvakrát měř, jednou řež**“ a obsah před zveřejněním raději vícekrát zkontrolovat.

Odstranění našeho obsahu by bylo možné jen tehdy, pokud jej dosud nikdo nečetl, nepřeposlal dále či nesdílel s dalšími uživateli. Příkaz k odstranění by tak musel přijít velmi rychle. V praxi lze stažení příspěvků využít například u Messengeru, WhatsAppu či Viberu. U dalších aplikací však kvůli sdílení příliš fungovat nebude.

4. Jaké informace nebo typy obsahu patří na sítích mezi ty nejvíc zneužitelné? (Nebo ty, kterých lidé následně nejvíce litují?)

Do obsahu, který je na internetu nejčastěji zneužitelný, určitě patří intimní fotografie, případně videa. **Intimní materiál** si mnohdy posílají mladí lidé pro zpestření svého vztahu. Často však nedomýšlejí, že se třeba jednou rozejdou ve zlém a zhrzený partner či partnerka se může mstít právě zveřejněním tohoto choulostivého obsahu na internetu.

Dále jsou to **fotografie z různých večírků a oslav**, kdy se aktéři opijí, případně usnou na lavičce v parku, a jejich vtipní „kamarádi" je zvěční na fotografii, kterou ještě týž večer vloží na sociální sítě pro pobavení ostatních.

V současné době se ještě objevuje fenomén zvaný **sharenting**, kdy rodiče na sociálních sítích publikují fotografie svých dětí a už nedomýšlejí, že se za ně jejich potomci mohou později stydět. Fotografie na nočníku či s umazanou pusou bývají v pubertálním věku důvodem k posměchu někdy vedoucímu až ke kyberšikaně.

5. Co dalšího můžeme udělat pro to, abychom eliminovali riziko, že o nás budou na sítích informace, které nás mohou poškodit?

Těmto případům se vyhneme primárně tím, že o sobě nebudeme zveřejňovat informace, za které bychom se později mohli stydět. Je lepší raději dvakrát promyslet obsah publikovaného textu, zveřejňované fotografie či videa a představit si, jak by se na to tvářila například naše babička.

Dalším možným způsobem je dostatečné zabezpečení účtů na sociálních sítích vytvořením **silného hesla** (má minimálně 12 znaků, ideálně však 21, a představuje kombinaci čísel, velkých a malých písmen a speciálních znaků), které nebudeme šířit. Děti však mají tendenci sdělovat své heslo nejlepším kamarádům, což může být právě kamenem úrazu.

Podstatným bezpečnostním prvkem je nastavení soukromí na sociálních sítích. Rozhodně není dobré mít veřejný účet, na který může nahlížet úplně kdokoli. Dále je vhodné **zvážit, koho si chceme vpustit do soukromého virtuálního života**. Mělo by se jednat o skutečné přátele a známé, s nimiž se chceme dělit o své názory, fotografie z našich životů a doporučovat jim zajímavé články.

Může se stát, že nás na sociálních sítích začne sledovat nebo nám pošle žádost o přátelství člověk, kterého vůbec neznáme nebo který se jmenuje jako náš známý, ale nemá profilovou fotku. V tom případě je lepší být na pozoru, jeho profil si prověřit (např. zjistit, zda máme nějaké společné přátele, kdy profil vzniknul nebo co je na něm publikováno) a důkladně zvážit, zda tuto žádost přijmout.

6. Co můžeme dělat, když už o nás někdo na sociálních sítích rozšířil informace, které nechceme, aby tam byly? (např. nějaké fotky)

V tomto případě je nejlepší **kontaktovat provozovatele sociální sítě** s prosbou o odstranění obsahu. Bohužel ne všem žádostem provozovatelé vyhoví. Pokud budeme mít štěstí, opravdu dojde ke smazání závadného obsahu. Nemáme ale nikdy jistotu, že jej nevyhledají webové vyhledávače v archivu. Můžeme se obrátit například na samotný Google a vyplnit *formulář* se **žádostí o odstranění obsahu**, nicméně je třeba se obrnit trpělivostí a důvod výmazu důkladně vysvětlit. Je nutné doložit i svou totožnost. Bohužel ani v tomto případě nemusí výmaz proběhnout, pokud naši žádost Google nevyhodnotí jako závažnou (naopak většině žádostí nevyhoví).

Pokud se však jedná o choulostivý obsah, který nás poškozuje, je možné **oslovit** přímo **policii**, která nám již s případem pomůže a urychlí jeho řešení. Jelikož je tato situace mnohdy psychicky náročná, nabízí se možnost kontaktovat též linky pomoci v krizi (Linka bezpečí, Linka důvěry Dětského krizového centra, Modrá linka a další).

7. Co se stane s našimi osobními daty, když si účet na sociálních sítích zrušíme?

Pokud se rozhodneme zcela **smazat účet** na Facebooku či Instagramu, budou trvale vymazány námi vložené fotografie, komentáře i zprávy, označení „To se mi líbí“ a přátelství. Facebook nám však dává 30 dní na to svůj krok ještě vrátit zpět. Po uplynutí této lhůty již vše nenávratně ztratíme, pokud si své příspěvky nezazálohujeme. Proces smazání veškerého obsahu z účtu může trvat **až 90 dní**, avšak ostatní uživatelé výše zmíněných sociálních sítí už k němu nebudou mít přístup.

Co se týče sociální sítě TikTok, zde je již přístup provozovatele odlišný. Po odstranění účtu ztratíme přístup ke všem námi publikovaným videím, to ale **nemusí znamenat, že je provozovatel smaže**. Informace, které jsou uložené mimo náš účet (např. chatové zprávy), mohou být i nadále viditelné pro ostatní uživatele. Před vymazáním účtu na TikToku tedy nejprve **doporučujeme smazat veškerá svá videa ručně**. Rovněž tato sociální sít nám dává 30denní lhůtu na to si svůj čin rozmyslet a vrátit své rozhodnutí zpět.

V každém případě bychom však měli počítat s variantou, že daná sociální síť může mít naše data stále umístěna na svých serverech, byť je nezveřejňuje. Nebo tyto informace mohou být archivované ve webových vyhledávačích.

8. Kam se mohu obrátit o pomoc v případě kyberšikany nebo sextingu?

V případě kyberšikany či sextingu doporučujeme dětem, aby se co nejdříve obrátily na dospělou osobu, které plně důvěřují. Ideální by bylo **svěřit se rodičům**. Avšak pokud jde o kyberšikanu ve škole, je možné obrátit se na třídního učitele. Pokud se dítě stydí a nemá odvahu kontaktovat někoho známého, může bezplatně zavolat na **Linku bezpečí (116 111)** nebo oslovit její pracovníky na chatu na webových stránkách *www.linkabezpeci.cz* či napsat e-mail na *pomoc@linkabezpeci.cz*.

Pokud se setkáme s kyberšikanou či sextingem, je důležité útočníkovi neodpovídat a rozhodně **neposílat vyžádané informace či fotografie a videa**. Komunikaci je potřeba **zálohovat** a útočníka neodstraňovat z kontaktů. Pokud bychom případ nahlásili policii (v některých případech už je to žádoucí), budou pak veškeré materiály sloužit jako důkaz a mohou pomoci k rychlejšímu dopadení pachatele.

Odpovědi vypracovala:

Michala Radotínská, odbornice na bezpečnost na internetu, CZ.NIC

Zdroje:

E-bezpečí: České děti v kybersvětě. 11. 6. 2019. Dostupné online na *https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/ceske-deti-v-kybersvete-2019*.

ZEMAN, M.: Instagram má problém. Unikly osobní údaje milionů influencerů. 21. 5. 2019. Dostupné online na *https://www.letemsvetemapplem.eu/2019/05/21/instagram-ma-problem-unikly-osobni-udaje-milionu-influenceru/*.

Doporučené odkazy:

Bezpečně na netu – vzdělávací projekt sdružení CZ.NIC věnující se rizikovým jevům na internetu

www.bezpecnenanetu.cz

Digitální stopa – vzdělávací projekt Národního úřadu pro kybernetickou bezpečnost

www.digistopa.cz

E-bezpečí – projekt zaměřený na prevenci, vzdělávání, intervenci a osvětu spojenou s rizikovým chováním na internetu

www.e-bezpeci.cz

Kraje pro bezpečný internet – e-learningové lekce, videospoty a vědomostní soutěžní kvíz

www.kpbi.cz

Doporučená literatura pro děti:

Vzdělávací komiks (pro čtenáře od 10 let):

VANĚK, J. a kol.: Jak na Internet. Bezpečně. CZ.NIC, Praha 2018.

Beletrie pro dívky (pro čtenáře od 12 let):

FEIBEL, T.: Like me – Každé kliknutí se počítá. Mladá fronta, Praha 2014.

Doporučená literatura pro dospělé:

DOČEKAL, D.; MÜLLER, J.; HARRIS, A.; HEGER, L. a kol.: Dítě v síti. Mladá fronta, Praha 2019.

KOŽÍŠEK, M.; PÍSECKÝ, V.: Bezpečně na internetu: průvodce chováním ve světě online. Grada, Praha 2016.

Poslední aktualizace: 07/2024