BEZPEČNOST (NEJEN) DĚTÍ V DIGITÁLNÍ DŽUNGLI

Jiří Kučík

jiri@kucik.cz

linkedin.com/in/jiri-kucik

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

AGENDA

- proč je IT bezpečnost důležitá
- digitální desatero pro rodiče
- jak na bezpečnost
- IT hygiena
- další informační zdroje

PROC TADY JSME?

MAME STRACH O SVE DETI...

ONLINE SVĚT JE DŽUNGLE

- online svět je úplně stejně rizikový jako reálný svět
- sociální sítě jsou jen nástroje na vydělávání peněz
- **<u>každý</u>** máme svůj inzertní (behaviorální) profil
- sociální sítě rozvracejí státy

JAK MOC NÁS ŠPEHUJÍ?

- clickclickclick.click

RIZIKA ONLINE ŽIVOTA

- ochrana dat není **celosvětově** vyžadována legislativou
- únik dat vede ke krádeži online identity
- kyberšikana
- kyberstalking
- kybergrooming

TÝKÁ SE TO I RODIČŮ?

- haveibeenpwned.com

ONLINE BEZPEČNOST SE TÝKÁ KAŽDÉHO!

PRINCIPY BEZPEČNOSTI

- pravidla bezpečného chování
- technické prostředky
- (ne)důvěra

CENA ZA BEZPEČNOST

- bezpečnost není zadarmo
- nejlevnější je co nejdříve se v bezpečnosti vzdělat
- užitečné je minimalizovat svou digitální stopu
- nejdražší je být pasivní

DIGITÁLNÍ STOPA

- aktivní: výsledek naší **vědomé** činnosti
- pasivní: metadata o naší činnosti
  - IP adresa
  - user agent
  - cookies
  - tracking data webových aplikací
  - analytická data lokálních aplikací

DIGITÁLNÍ DESATERO
PRO RODIČE

Dítě v síti

Učíme se žít v digitálním světě

- flowee.cz/ditevsiti
- manuál pro rodiče a učitele

PRAVIDLO 1

- nenechat děti v síti bez dozoru
- jinak skončí jako oběti predátorů

PRAVIDLO 2

- pochopit přítažlivost sítě pro děti
- zákaz sítě nic neřeší

PRAVIDLO 3

- omezit čas dětí strávený na síti
- omezení je individuální
- technické překážky je pro dítě výzva obejít

PRAVIDLO 4

- mít rád vlastní děti
- online svět je svůdný a invazivní

PRAVIDLO 5

- učit děti rozpoznávat nebezpečí na síti
- učit = vědět, rozumět
- rodič si musí aktivně rozšiřovat obzory

PRAVIDLO 6

- učit děti být i bez sítě
- vést je k fyzické aktivitě
- vést je ke čtení klasických knih

PRAVIDLO 7

- nespoléhat se jen na školství
- prověřovat si činnost kroužků s online náplní

PRAVIDLO 8

- nenechat děti usínat na síti
- syndrom FOMO

PRAVIDLO 9

- nenechat děti zbytečně ozařovat
- září všechno, co je bezdrátové

PRAVIDLO 10

- učit děti správně se chovat na síti
- zvyšovat jejich mediální gramotnost
- doporučovat jim seriózní zdroje informací a zpráv
- nutit je dodržovat IT hygienu a netiketu

IT HYGIENA

BEZPEČNOSTNÍ POVĚDOMÍ

- chovat se bezpečně (pravidla IT hygieny)
- chovat se slušně (netiketa)
- rozpoznat závadné chování
- rozpoznat podvodné jednání (phishing, smishing)
- omezovat vlastní digitální stopu
- rozpoznat dezinformace a fake-news

PRAVIDLA IT HYGIENY

- zabezpečení IT zařízení
- zabezpečení citlivých dat
- bezpečné používání hesel

JAK NA BEZPEČNOST (PODLE VĚKU DÍTĚTE)

DÍTĚ ŠKOLKOU POVINNÉ

- chce tablet a na něm pasivně konzumovat video (YouTube)
  - zásadně spolu s rodičem
  - využívat max. 1 hod. denně
- pokud chce hrát hry, tak jedině rozvíjející představivost a jiné mentální dovednosti (Minecraft)
- pokud potřebuje nějaký účet, tak k němu nesmí znát heslo

ZABEZPEČENÍ YOUTUBE

- vyzkoušejte YouTube Kids
- vytvářejte vlastní playlisty
- preferujte používání na chytré TV (není možnost prokliku na jiný obsah)

ŠKOLÁK (1. STUPEŇ ZŠ)

- obvykle má vlastní mobil
  - je bezpečnější, pokud nemá možnost si sám instalovat aplikace
- začne se dožadovat účtu na sociální síti
  - je bezpečnější, pokud nezná heslo k vlastnímu účtu
  - sledujte ho, buďte přáteli (ale pozor na fenomén Finsta)
  - striktní zákaz je kontraproduktivní, sledujte čas využití

ŠKOLÁK (1. STUPEŇ ZŠ)

- na sociální síti začne aktivně komunikovat (chat)
  - začne si budovat svoji digitální stopu
- učte ho nedůvěřovat cizím lidem online
  - nikomu nic online neříkat přes chat
  - žádosti o přátelství ověřovat osobním kontaktem
- pokud mobilní data, tak **pouze pro privátní geolokaci**

BEZPEČNOSTNÍ POVĚDOMÍ (1. ST. ZŠ)

- distanční online výuka vyžaduje po žákovi schopnost se sám prihlásit do potřebných aplikací a bezpečně je používat
  - výuka základního bezpečnostního povědomí žáka musí začít současně s vyžadováním této jeho schopnosti
  - žáci musí vědět, že heslo = identita
  - žáci musí vědět, že online aplikace zvětšují digitální stopu
- žáci musí být schopni rozpoznat závadné chování na síti

OCHRANA ONLINE IDENTITY

- bezpečně používat hesla

MINIMALIZACE DIGITÁLNÍ STOPY

- nebýt neustále připojen (WiFi, mobilní data, Bluetooth)
- používat neidentifikovatelná zařízení
- dodržovat pravidla IT hygieny
  - bezpečně používat web
  - bezpečně používat sociální sítě
  - bezpečně používat geolokaci

ŠKOLÁK (1. STUPEŇ ZŠ)

- objevuje hry
- vypněte mu na mobilu všechny notifikace
- vznikají závislosti (FOMO)
- objevuje se kyberšikana

SOCIÁLNÍ SÍTĚ

- není to jen Facebook…
- **Instagram** (= Facebook)
- WhatsUp (= Facebook)
- Messenger (= Facebook)
- **YouTube**
- Snapchat
- **TikTok**
- Roblox
- Clubhouse
- Twitter

ZABEZPEČENÍ FACEBOOKU

- 2FA přihlášení
- zabezpečit mobil, na kterém Facebook běží
- při používání se důsledně řídit pravidly pro osobní údaje na sociálních sítích
- zapnout schvalování příspěvku, kde vás někdo označí
- mít pouze ověřené přátele (osobně, telefonicky)
- skrýt seznam přátel před **úplně všemi**

ZABEZPEČENÍ TIKTOKU

- nastavit účet jako soukromý (jinak bude naprosto veřejný)
- nastavit, že komentovat mohou pouze přátelé
- nastavit omezený režim (dítě neuvidí nevhodný obsah na jiných účtech)
- vypnout možnost stahování videa

SLEDOVÁNÍ VYUŽITÍ SÍTĚ

- Android: Google Family Link
- Apple iOS/macOS: Screen Time
- Android, Windows, Apple macOS: KidLogger
- kromě měření času umožňuje i blokovat využití
  - není vždy úplně spolehlivé, blokaci lze obejít

BLOKOVÁNÍ VYUŽITÍ SÍTĚ

- nastavení domácího routeru pro připojení do internetu
  - informace v manuálu nebo u prodejce
- “otevírací” hodiny v konkrétní dny v týdnu
- lze i na konkrétní zařízení (MAC adresa mobilu)
- alternativou je chytrá zásuvka (přednastavené vyp/zapnutí) pro domácí router

KYBERŠIKANA

- online agrese
  - zveřejňování nevhodných fotek, šíření pomluv a vysmívání
    - průnik do cizího účtu a tam zveřejnění dehonestujícího obsahu
- nereagovat směrem k útočníkovi (**ani jako rodič!**)
- svěřit se (rodič, učitel, linka nebo schránka důvěry)
- hlásit policii

KYBERZLOČINY A POLICIE

- každý operátor a provozovatel obsahové služby v ČR má zákonnou povinnost uchovávat retenční data **po dobu 6 měsíců**
  - retenční data = záznam o datové komunikaci
- na PČR má smysl hlásit každý kyberzločin **co nejdříve**
- na PČR nejsou příliš v obraze (čest výjimkám!)
  - ve krajských městech tomu obvykle “rozumí”
  - pokud případ chtějí odložit, dožadujte se jeho přezkoumání “výše”

PUBERŤÁK (2. STUPEŇ ZŠ)

- má právo na soukromí
  - IT hygiena vč. správného používání hesel
- aktivně sledujte, koho dítě sleduje (influenceři)
  - vysvětlujte mu, proč je někdo nevhodný
- objevuje se kybergrooming

KYBERGROOMING

- psychická manipulace v online světě
- cílem útoku je nejč. získání fotek oběti se sex. obsahem
- útočník je vždy schován za ukradenou identitou
  - holky oslovují “normální chlápci”
  - kluky oslovují homosexuálové vydávající se za vyzývavé holky
- pokud možno nereagovat

STŘEDOŠKOLÁK

- začne se dožadovat možnosti placení platební kartou
- sociální sítě budou formovat jeho emoce
  - pod tvrdou palbou reklamy (na nakupování)
- objevuje se sexting a sextortion

ZABEZPEČENÍ PLATEBNÍ KARTY

- vyhrazená karta **pouze** pro online transakce
- svázaná s **vyhrazeným** bankovním účtem
- s nastaveným **nízkým** limitem na všechny transakce
- bezpečně uložená v trezoru (tzn. **není v peněžence**)
- na kartě v peněžence **vypnout** online transakce

MLADÝ DOSPĚLÝ

- na sociální síti bude pod tvrdou palbou **politické** reklamy
- doporučujte mu seriózní zdroje informací
- učte ho ověřovat fakta
- objevuje se kyberstalking
- internetové seznamky

IT HYGIENA

1. ZABEZPEČENÍ IT ZAŘÍZENÍ

- pravidelně aktualizovat sw
- používat pouze sw ze seriózních zdrojů
- pro běžnou práci nepoužívat admin účet
- ručně zamykat displej nepoužívaného zařízení
- šifrovat úložiště dat v zařízení

1.1 SERIÓZNÍ APLIKACE

- jsou součástí mobilu od jeho výrobce
- všechny ostatní jsou rizikové
  - kradou data (kontakty, zprávy, hesla, biometrie)
  - šmírují (zvuk, video, poloha); stalkerware
- Google Play (Android) vs. App Store (Apple iOS)

1.2 RIZIKOVÉ MOBILNÍ APLIKACE

- především ty zdarma pro Android
- především ty, které potřebují zpřístupnit nějaká data z mobilu
- veškerá zábava (hry, vylepšení her, úprava fotografií)
- “obyčejné” aplikace (svítilna, kalkulačka, lupa)
- fitness aplikace (počítadla kroků a kalorií)
- fake antivirus sw

2. ZABEZPEČENÍ DAT

- neukládat zbytečné data ke kontaktům
- neukládat geolokační metadata do fotografií (EXIF)
- nemít trvale zapnutá bezdrátová sdílení (Bluetooth, AirDrop)
- bezpečně používat web a e-mail
- bezpečně používat veřejnou WiFi
- osobní údaje nepatří na sociální sítě

2.1 BEZPEČNÝ WEB

- **nepoužívat** nezabezpečené web servery
  - jen ty s adresou https://…
- minimalizovat pasivní digitální stopu při prohlížení webu
  - vypínat/mazat cookies
  - používat anonymní režim prohlížení webu
  - **nebýt současně** přihlášen na sociální sítě a ke cloudovým službám
  - blokovat reklamy (uBlock Origin)

2.2 BEZPEČNÝ E-MAIL

- příznaky nebezpečného e-mailu (malspam, phishing, smishing)
  - obsah, který je přehnaně důležitý
  - obsah, který se mě vůbec netýká
  - obsah obsahuje pravopisné chyby
  - adresa odesílatele je ve skutečnosti jiná, než se jeví
  - odkazy ve skutečnosti míří jinam
  - přílohy s neznámými koncovkami souborů

2.3 BEZPEČNÁ WIFI

- zabezpečení domácího WiFi přístupového bodu (routeru)
  - aktualizovat sw
  - jiné než defaultní heslo pro administraci
  - administrace povolená pouze z domácí sítě
  - WPA2 šifrování
- bezpečné používání veřejné WiFi
  - před připojením nikam nezadávat žádné osobní údaje
  - používat šifrovanou VPN
  - bezpečně prohlížet web

2.4 OSOBNÍ ÚDAJE A SOC. SÍTĚ

- pokud možno žádné neuvádět
  - pokud to není možné, tak si je vymyslet (jméno, věk)
- žádné fotografie obsahující obličeje (vlastní i cizí)
- žádné fotografie vlastních dětí v nelichotivých situacích (sharenting)
- neidentifikovat obličeje ve fotografiích (vlastních i cizích)

2.5 ZABEZPEČENÍ GEOLOKACE

- geolokaci (využití polohových služeb, tracking)
  - povolovat pouze v konkrétních aplikacích (**nikoli ve všech**)
  - povolovat pouze při použití aplikace (**nikoli trvale**)
- vypnout tracking history (iOS: Významná místa, MyActivity.google.com)
- data z aplikací používajících geolokaci **nesdílet veřejně**
  - pokud sdílet, tak pouze vyjmenovaným kontaktům
- jen minimum aplikací potřebuje legitimně využívat geolokaci
  - zbytek je stalkerware

3. ZABEZPEČENÍ HESEL

- čím delší, tím bezpečnější (a nemusí obsahovat “divné” znaky)
- pokud není generované, tak vytvořené mnemotechnicky
- nepoužívat opakovaně
- mít v každém systému jiné
- pravidelně měnit (po 1-2 letech nebo po úniku)
- mit je bezpečně uložené

PŘÍKLADY ŠPATNÝCH HESEL

123456	111111
123456789	123123
qwerty	abc123
password	qwerty123
1234567	1q2w3e4r
12345678	admin
12345	qwertyuiop
iloveyou	

zdroj: 15 nejpoužívanějších hesel, Tripwire Inc.

3.1 ULOŽENÍ HESEL

- hlava (vlastní)
- zapečetěná obálka v trezoru (vlastním)
- správce hesel
  - aplikace: LastPass, KeePas, 1Password, Bitwarden
  - webový prohlížeč: Firefox, Chrome

3.2 POUŽÍVÁNÍ HESEL

- nikomu je nesdělovat
- vždy změnit, pokud mi ho někdo sdělí (a je moje)
- opatrnost při zadávání do systému
  - kamery
  - otisky na displeji telefonu

3.3 VÍCEFAKTOROVÉ OVĚŘENÍ

- pro přístup do systému nestačí jen znát uživatelské heslo
- je třeba ještě navíc
  - něco mít (např. SMS s jednorázovým kódem)
  - někým být (biometrický údaj, např. otisk prstu)
  - někde být (geolokační údaj, např. aktuální poloha)
- 2 faktory = 2FA = např. ověření heslem a jednorázovým kódem

DALSI INFORMACNI ZDROJE

DOKUMENTY A E-LEARNING

- Dítě v síti
- Rodina v síti
- @365tipu
- Říše za monitorem
  (knihy pro předškolní děti)
- On-line ZOO (komiks pro děti)
- Kyber trable (hra pro děti)
- Digitální stopa
- Zvolsi.info
- Kybertest
- Internetem bezpečně (kniha pro děti)
- Jak na internet bezpečně (komiks pro dospělé)
- #vbezpeci (pro děti a seniory)
- e-bezpečí
- NÚKIB osvěta pro rodiče a učitele
- O2 Chytrá škola
- Nenech to být
  (on-line schránka důvěry)
- Kraje pro bezpečný internet

NAUČNÁ VIDEA

- Jak na internet
- Nebojte se internetu
- Bezpečně online

FILMY A SERIÁLY

- #martyisdead
- V síti
- /sociální dilema_

o/o

DĚKUJI ZA POZORNOST