Bezpečnosť detí a tínedžerov na internete

Úrad na ochranu osobných údajov SR

Bezpečnosť na internete:

- Dostupnosť informácií všetkého možného druhu zažíva svoj doteraz najväčší rozmach. To je výborná vec, ale ako všetko aj kybersvet má svoju odvrátenú stránku.

- Skôr či neskôr bude Vaše dieťa s technológiami konfrontované, pretože v súčasnej dobe sa posúva hranica, kedy sa dieťa dostáva do kontaktu s kyberpriestorom.

- Počítače sa používajú už na základnej škole, ich využitie sa znásobilo práve v čase koronakrízy.

Bezpečnosť na internete:

Zamysleli ste sa nad tým ...

- Ako Vaše dieťa využíva počítač vo voľnom čase? Čo presne (aj na požičanom) mobile robí, aké mobilné aplikácie a webové stránky navštívi?
- Využíva Vaše dieťa sociálne siete alebo četové miestnosti, a akých ľudí tu stretáva?
- Aké riziká sú spojené s trávením času detí a tínedžerov na internete?

❑Niekedy aj nevhodne zobrazená reklama, či hra s explicitným až násilným obsahom, môže byť pre dieťa podnetom k šikane v kyberpriestore.

Rodičovská kontrola:

- Aké možnosti prevencie máte ako rodič v prípade voľnočasových aktivít Vášho dieťaťa na internete:

❑Jednou z možností je **Rodičovská kontrola (aplikácia).** V súčasnosti sú programy či aplikácie na rodičovskú kontrolu mobilu a počítača. Týchto nástrojov je na trhu veľa. Ponúkajú ich operátori, spoločnosti, ktoré prevádzkujú siete vyhľadávačov, aj výrobcovia mobilov. Stačí si vybrať podľa svojich preferencií. Aplikácie Vám umožnia mať neustály prehľad o aktivitách detí a pritom im ponechávajú dostatočnú voľnosť.

❑Aplikácia umožňuje **blokovať webové stránky aj kategórie stránok, ktoré by mohli obsahovať nebezpečný alebo nevhodný obsah**. Aplikácia deti navádza, aby sa zaujímali o to, prečo sa na stránku nedostali, porozprávali sa o tom s rodičmi, prípadne ich požiadali o prístup k stránke.

❑**Najdôležitejšia je vzájomná dôvera** a pravidelná komunikácia s deťmi, prípadne zabezpečenie prístupu do počítača Vášho dieťaťa, vrátane zabezpečenia jeho sociálnych sietí.

Rodičovská kontrola:

- Nástroje na kontrolu mobilu a počítača detí majú širokú paletu funkcií, vďaka ktorým aj technicky menej zdatní rodičia zaistia bezpečnosť detí na internete.
- Určitá forma kontroly je aj **možnosť obmedziť čas, ktorý dieťa trávi na zariadení**. V prípade malých detí by to malo byť maximálne 10 až 30 minút, mladším školákom stačí hodina denne, pri tých starších odporúčame nastaviť denný limit nie vyšší ako 2 hodiny. Limit sa dá v prípade, že dieťa zariadenie potrebuje v škole, predĺžiť.
- Program na kontrolu mobilu je tiež strážcom aplikácií, s ktorým **môžete určiť časový limit a rozpočet pre aplikácie i to, aké aplikácie si vzhľadom na svoj vek deti môžu nainštalovať**. Využíva sa systém s rôznou úrovňou kontroly. Kontroluje, či aplikácie, ktoré deti spúšťajú, sú vhodné pre nastavený vek.

Riziká:

- **Anonymita** - v kyberpriestore funguje anonymita a spoločnosti zastrešujúce sociálne siete nepreverujú skutočný vek užívateľa, ktorý sa zaregistruje.
- **Prístup k citlivým údajom** - ohrozené môžu byť aj Vaše financie, súkromné a citlivé informácie, pretože čokoľvek, čo používate online, alebo máte uložené v počítači, môže byť zneužité.
- **Zavádzajúce reklamy a odkazy** - zlý klik na nesprávnu linku v obsahu, ktorý sa tvári nanajvýš neškodne, respektíve kopírujúc službu, ktorú bežne využívate, a prístup do vášho e-mailu a bankového účtu môže byť v cudzích rukách.
- Pozor si treba dávať aj na nedôveryhodné odkazy**, ktoré môžu v sebe obsahovať škodlivý kód či vírus**, prípadne externý preklik na ďalšiu nebezpečnú stránku.

Kontrola sociálnych sietí:

- Súčasný trend využívania internetu:

❑**zdieľanie každodenného života s okolitým svetom** – fotky a videá zdieľané na sociálnych sieťach. Zdieľanie svojho bežného života mladých ľudí, bez toho aby vedeli, aký to môže mať na nich dopad.

❑Rovnakým problémom je aj **nahota** v kybernetickom priestore, ktorá je mnohokrát spúšťačom proti spoločenských aktivít a priťahuje predátorov a agresorov. V prípade, že sa objaví nahota, je dôležité vedieť s kým takéto osobné údaje zdieľam, mať kontá pod kontrolou a vedieť to čo najskôr zastaviť.

❑**Extra pozor na zoznamky,** na ktorých môže dieťa naraziť na sexuálne obťažovanie. Tejto téme bol venovaný dokumentárny film Českej republiky „**V síti**“.

Internetovú bezpečnosť netreba podceňovať z viacero dôvodov:

- Kyberútoky, kyberšikana, sexuálni agresori, za iných podmienok neprístupný obsah... to všetko na internete existuje a najlepším spôsobom ako sa pred tým ochrániť je **prevencia**. Prirodzene nedokážete byť dieťaťu neustále za chrbtom a sledovať jeho správanie online, ale môžete dieťa vzdelať a upozorniť na riziká, s ktorými sa môže stretnúť.
- **Základom je hlavne komunikácia!**

Kyberšikana:

- **Kybernetická šikana alebo kyberšikana je druh šikany, ktorý je realizovaný pomocou informačných a komunikačných technológií, najčastejšie cez internet a mobil:**

❑dehonestujúce blogy a stránky,

❑urážlivé a nenávistné správy na sociálnych sieťach (flaming),

❑zverejňovanie fotografií a vydieranie,

❑sexuálne obťažovanie cez posielanie správ, fotiek a videí so sexuálnym podtextom (sexting),

❑prenasledovanie (cyberstalking),

Kyberšikana:

- **Dieťa môže byť elektronicky šikanované, ak:**

❑nečakane prestane používať počítač,

❑sa zdá byť nervózne, neisté alebo smutné pri čítaní emailov alebo okamžitých správ, správ v mobile,

❑sa zdá byť nahnevané, depresívne alebo frustrované po odchode od počítača,

❑uniká do choroby,

❑nechce chodiť do školy alebo medzi ľudí,

❑vyhýba sa rozhovoru o tom, čo robí na počítači,

❑uzatvára sa pred rodinou a priateľmi, a súčasne popiera, že by sa niečo dialo,

❑uniká do sveta fantázie, počítačových hier.

Kyberšikana:

- **Dieťa môže elektronicky šikanovať, ak:**

❑ rýchlo vypína obrazovku alebo zatvára programy v počítači, keď sa priblížite,

❑ prehnane sa smeje pri používaní počítača,

❑ trávi čas s kamarátmi pri počítači, prehnane sa smejú, ale nechce prezradiť, čo robia,

❑ vyhýba sa rozhovoru o jeho aktivitách na počítači,

❑ používa niekoľko falošných účtov a adries.

Ochrana dieťaťa pred kybernetickým únikom:

- **Odporúčame**: Používanie **silných hesiel** pre individuálny online účet. Je nevyhnutnosťou, aby všetky deti pochopili a porozumeli prečo je používanie **jedného hlavného** hesla pre všetky účty veľmi **nebezpečné**.
- Všetky ďalšie účty spojené s týmto rovnakým heslom sú ohrozené a dávajú nebezpečným aktérom naše poverenie narábať s našimi dátami a osobnými informáciami.
- V momente, keď si uvedomíte, že došlo k úniku Vašich údajov, je zvyčajne príliš neskoro na to, aby ste predišli hroziacim škodám – napríklad ukradnutie identity alebo hacknutie e-mailového účtu.

Ako vytvoriť silné heslo?

- mali by obsahovať 12 alebo viac znakov,
- kombinácia písmen a číslic,
- vyhýbať sa heslám za použitia mien, dátumov narodenia alebo iných osobných údajov,
- striedanie veľkých a malých písmen.

Chráň si svoje:

- Každá informácia (napr. aj fotka), ktorú zdieľate online, má potenciál k predaju, zneužitiu alebo úniku. Je veľmi dôležité, aby deti pochopili, aké údaje a informácie je vhodné v tomto priestore zdieľať. **Anonymita im dáva vysoký stupeň bezpečia.**
- V súčasnosti je veľmi dôležité aby deti boli veľmi obozretné v tom, koľko a aké osobné informácie zdieľajú v online priestore.
- **Sociálne siete**, ako Instagram či iné platformy podvedome nabádajú k „socializácii", čo nepriamo a často neuvedomelo núti mladých ľudí k zdieľaniu najrôznejších informácií z ich života, ktoré by cudzím ľuďom pri osobnom kontakte nikdy neposkytli.

Rodičia, chráňme identitu dieťaťa:

- **Pravidelne zdôrazňujte** a **vysvetľujte** svojim deťom, aby nikdy neposkytovali prostredníctvom e-mailu, Instagramu, Facebooku alebo na iných sociálnych sieťach **žiadne osobné údaje**, ako sú **meno, adresa bydliska alebo telefónne číslo.**
- Rozprávajte sa so svojimi deťmi o online rizikách, o bezpečnej interakcii s cudzími ľuďmi prostredníctvom informačných technológií a zdieľaní poznámok a obrázkov v kybernetickom priestore.
- Dohľadajte edukačné pomôcky, ktoré môžu pomôcť deťom rôznych vekových kategórií pochopiť ako chrániť svoje osobné údaje a aké **následky má odcudzenie identity.**

Rodičia, venujte chvíľku svojho času aj k zabezpečeniu informačných technológií:

- Používanie softvérového zabezpečenia, ktoré sa automaticky aktualizuje, **udržuje** Vaše technológie v relatívnom **bezpečí a znižuje pravdepodobnosť infikovania škodlivým softvérom.**
- Pravidelne si spolu s deťmi kontrolujte aktualizácie Vašich technológií.
- **Pravidelná aktualizácia bezpečnostného softvéru** Vašich technológií môže **chrániť** Vašu rodinu pred **podvodníkmi, hackermi** a **inými online hrozbami**, ktoré môžu ohroziť Váš softvérový systém, **bezpečnosť Vašich osobných údajov** a s tým spojenú aj **finančnú bezpečnosť** Vašej rodiny.

Wi-Fi a VPN:

- **Nezabezpečené siete Wi-Fi** sú **veľkým rizikom**.
- Väčšina miest ponúka zákazníkom bezplatný prístup k sieti Wi-Fi – od nákupných centier cez fitnes centrá až po verejnú dopravu; čo je lákavou alternatívou k jednoduchému pripojeniu na internet.
- Problém je v tom, že tieto verejné siete nie sú zabezpečené. Sú **zraniteľné**, a preto poskytujú vynikajúci priestor pre pôsobnosť rôznym počítačovým zločincom a hackerom.
- Hackeri, zvyčajne zneužívajú nezabezpečené siete, aby spustili rôzne typy útokov a zachytili všetky **Vaše údaje a informácie**, ktoré poskytujete, keď ste na takúto sieť pripojení.

Wi-Fi a VPN:

- VPN zabezpečuje bezpečné internetové pripojenie pomocou šifrovania, ktoré **chráni Vaše osobné údaje pred tretími stranami**.
- Ako osvedčený postup vždy používajte službu VPN na zabezpečenie bezpečnosti technológií Vašej rodiny a **komunikujte so svojimi deťmi**, kedy a ako ich používať, aby **mohli zostať v bezpečí aj v online priestore** bez ohľadu na to, kde sa nachádzajú.

Ako spoločne zabojovať proti kyberšikane?

- Naučte svoje deti **rozlišovať**, čo zverejňujú na internete, **premýšľať o dopade** týchto správ na ostatných a o dôsledkoch, ktoré tieto príspevky môžu mať, ak nie sú pozitívne alebo môžu byť vnímané aj ako hanlivé.
- Virtuálna komunikácia so sebou prináša **veľa nástrah**:

❑Pretože v nej vieme pokračovať bez toho, aby sme interaktívne vnímali osobu na druhej strane, prípadne jej pocity alebo postoje.

❑Takáto sociálna anonymita je v skorom veku dieťaťa nežiaduca pre jeho empatický vývoj, preto sa neodporúča deťom mladším ako 12 rokov aktívne využívať tieto komunikačné platformy.

Ako spoločne zabojovať proti kyberšikane?

- Udržiavajte si **pravidelnú otvorenú komunikáciu** s dieťaťom **o všetkom**, čo sa deje v jeho virtuálnom priestore.
- Je na nás, rodičoch, aby sme svoje deti **učili, ako bezpečne surfovať** po svete online tak, aby mali dostatočné znalosti a návyky, ktoré potrebujú na bezpečné fungovanie a **ochranu seba a svojich dát**.

Zásady bezpečnosti na internete, odporúčame:

- **Nedeliť sa s nikým o svoje osobné údaje, ani svojho dieťaťa a ani nikoho iného**. Napríklad **dátum narodenia, e-mailovú adresu, rodné číslo, heslá či telefónne číslo.**
- Dávať si pozor na zverejňovanie **svojej polohy**, v tejto súvislosti odporúčame prekontrolovanie nastavenia o zdieľaní aktuálnej polohy v mobilnom telefóne.
- **Rozmyslite si, aké fotky zverejňujete a posielate**. Tínedžeri, **neposielajte nikomu, ani kamarátom, intímne fotky či videá**!

- **Chráňte si zariadenie.** Nielen fyzicky, aby mobil nespadol, ale aj heslom**.** Odporúčame si nastaviť **čo najzložitejšie heslo**, **kresbu alebo používajte overenie odtlačkom prsta**. Heslo **nikomu nedávajte** a mobil si vždy zamknite, keď ho nepoužívate. Ideálne telefón nikomu nepožičiavať.

Zásady bezpečnosti u detí na internete:

- **Odporúčame,** ak sa Vaše dieťa pripája na internet v škole, u kamaráta alebo na akomkoľvek inom cudzom počítači, **informujte ho o následnom odhlásení z predmetného konta.**
- Pripájajte sa cez anonymný režim, nenechajte zariadenie ukladať údaje a vždy sa po skončení práce odhláste zo všetkých účtov. Režim inkognito podporujú viaceré prehliadače:

❑ V Chrome ho zapnete kliknutím na ikonu troch bodiek v pravom hornom rohu prehliadača, kde zo zoznamu vyberiete možnosť „Nové okno inkognito“.

❑ Vo Firefoxe je postup podobný, akurát kliknete na ikonu s tromi vodorovnými čiarami.

- V zariadení si nainštalujte antivírusový program, ktorý Vás chráni pred zlými aplikáciami a hackermi.
- **Odporúčame, pred inštaláciou aplikácie si overiť recenzie a spokojnosť jej užívateľov** - to Vám napovie, či je to dobrá a bezpečná aplikácia.

Záver:

Ďakujeme za pozornosť ☺