



Rodičovská príručka pre ochranu detí na internete



UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLOGIE™

Úvod

Deti sú to najcennejšie, čo máme. Sú naša budúcnosť. V spoločnosti ESET to dobre vieme, keďže sme tiež rodičmi, presne ako vy. Aj my cítime potrebu viesť ich životom a chrániť ich pred zlom. Táto zodpovednosť však dnes predstavuje obrovskú výzvu.

Mobilné zariadenia sú čoraz dostupnejšie a možnosť ich využitia je aj vďaka ich pripojeniu na internet takmer neobmedzená.

Táto brožúrka slúži ako pomôcka na to, aby vám i vašim deťom pomohla pohybovať sa na internete tak, aby bol pre vás vždy zdravým a bezpečným prostredím.



Kto by mal s deťmi hovoriť?

Bez ohľadu na to, aké nepríjemné to bude, musíte to byť vy.

Počas detstva sa vaša dcéra alebo syn budú stretávať s ľuďmi, ktorí v ich živote zohrajú veľmi dôležitú úlohu. Môžu to byť napríklad príbuzní, priatelia či učitelia.

Nikto z nich však nemôže nahradiť vašu úlohu rodiča. V očiach dieťaťa ste to práve vy, kto pozná všetky odpovede a dokáže mu pomôcť, keď si nie je istý, čo má urobiť.

Práve teraz. Alebo čo najskôr.

S vyšším vekom dieťaťa prichádzajú aj nové problémy.

Ohľaduplná a dobre mienená rada v každej z týchto nových situácií môže byť tým rozhodujúcim krokom, ktorý vaše dieťa v budúcnosti posunie správnym smerom. Platí to zvlášť vtedy, keď je reč o internete.

S deťmi by ste sa o online bezpečnosti mali začať rozprávať od chvíle, kedy prejavia už prvý záujem o smartfón, tablet, počítač alebo o internet ako taký. Všetky zásady bezpečnosti z reálneho života, ktoré sa učia od vás alebo zo školy, treba premietnuť na život digitálny.



Rodičia svoje deti vzdelávajú, ale aj sa od nich učia



Máte pocit, že vaše deti vedia toho o počítačových technológiách viac ako vy? Zďaleka nie ste jediným rodičom, u ktorého sa objavuje táto neistota.

Dnešné deti sa už akoby narodili so smartfónom v ruke a s pokročilými technologickými znalosťami. Veľa dospelých sa však s týmito vecami začalo zoznamovať až v neskoršom veku.

To však neznamená, že by práve dieťa malo mať prístup ku všetkým počítačom a podobným zariadeniam v domácnosti. Hoci

dieťa dokáže s internetom pracovať, nemusí rozumieť tomu, aké dôsledky môže mať konkrétna online akcia, ktorú chce vykonať.

Nie je potrebné, aby ste ako rodič vedeli o každej novinke digitálneho sveta a ešte aj vo väčšej miere, než vaše deti. Mali by ste však deti pripraviť na situáciu, kedy ich:

- osloví niekto cudzí,
- dostanú sa k zaujímavým informáciám, ktoré však nemusia byť pravdivé,
- chcú si nainštalovať aplikáciu, ktorá od nich požaduje osobné údaje, chce sledovať ich polohu alebo vyžaduje iné informácie, ktoré s funkciou samotnej aplikácie nijako nesúvisia.

Dôležité je, aby ste dieťa zapojili do debaty. Vytvorte preto prostredie, v ktorom deti budú voľne klásť otázky a spoločne budete preberať všetky nové informácie.



Čo robiť, keď dieťa dorastie do uvedeného veku?

Na tieto aktivity si ako rodičia vyčleňte čas tak, aby ste ich mohli robiť spolu s deťmi.

DO 10 ROKOV

1. Sprevádzanie detí počas prvých skúseností na webe

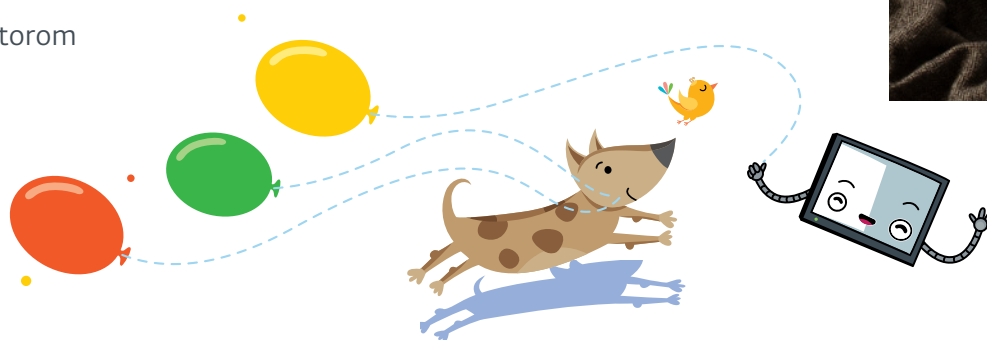
Keď budú vaše deti robiť prvé kroky na webe, určite buďte pri tom. Prvý kontakt dieťaťa s internetom je vhodná príležitosť na to, aby ste si k nemu sadli a sprevádzali ho dobrodružstvami detských webstránok, ktorých obsah ho môže zaujímať.

2. Určenie podmienok používania internetu

Stanovte základné pravidlá používania internetu. Vhodné je dohliadať na počet hodín strávených online a tiež určiť čas, v ktorom bude používanie webu povolené.

3. Buďte dobrým príkladom

Deti si zvyčajne berú príklad zo správania rodičov a toto pravidlo platí nielen v reálnom živote, ale aj online. Ak sa členovia rodiny správajú pozitívne, bezprostredne sa to prenesie aj na dieťa. Rovnako, ak sa členovia rodiny venujú svojim mobilným zariadeniam na miestach a v časoch, kedy to nie je vhodné, bude to dieťa považovať za prípustné a bude chcieť používať svoj smartfón tiež. Napríklad pri spoločnej večeri.



OD 11 DO 14 ROKOV

1. Používanie nástrojov rodičovskej kontroly

Používajte existujúcu technológiu a využite ju vo svoj prospech. Nástroje ESET Parental Control umožňujú blokovať webstránky alebo dokonca kategórie stránok, ktoré obsahujú potenciálne nevhodný materiál. Umožňujú tiež nastaviť časové obmedzenie surfovania na internete alebo hrania hier. Dieťa bude zároveň môcť požiadať o povolenie navštíviť niektoré stránky alebo získať viac času na hranie, ak si urobí domáce úlohy.

2. Poučenie o nezdieľaní informácií odhaľujúcich identitu

Dôležité je deťom veľmi jasne povedať, že vo virtuálnom svete nie je každý človek priateľ, a že niektorí ľudia im môžu dokonca chcieť ublížiť. Vysvetlite im, prečo nie je bezpečné zdieľať informácie ako sú adresa, telefón,

škola alebo napríklad mimoškolské aktivity. Sú to informácie, ktoré sa prostredníctvom internetu môžu dostať doslova ku komukoľvek. Stačí ak ich napríklad kamarát tiež vyzdieľa na internete. Dieťa by si malo tiež pýtať povolenie pred zdieľaním akýchkoľvek fotografií na internete. Aj keď fotografia vyzerá na prvý pohľad nevinne, dieťa si nemusí všimnúť, čo všetko prezrádza jej pozadie. Na fotke môžu byť zachytené vaše domáce cennosti alebo čokoľvek iné, čo nie je určené pre cudzie oči.

3. Vedenie otvoreného dialógu

Povzbudzujte svoje deti v tom, aby sa s vami rozprávali otvorene a voľne kládli otázky o tom, na čo na internete narazili. Ak je to možné, počítač neumiestňujte do detskej izby, ale do miestnosti, kde trávi čas celá rodina, aby tak bol pod dohľadom.



OD 15 DO 18 ROKOV

1. Heslá by nemal poznať nikto iný

Vieme, že s dospievajúcimi deťmi je to ťažké, niekedy dokonca veľmi ťažké. No uistite sa, že rozumejú osvedčeným postupom používania hesiel. Koniec koncov, ide o niečo podobné ako kľúče od domu. Rešpektujte súkromie svojich dospievajúcich detí, ale zároveň dbajte na to, aby svoje heslá nikdy neposkytli cudziemu človeku a ani ich nikomu „nepožičali“ osobne ani cez internet.

2. Okamžité hlásenie prípadov prenasledovania a kyberšikany

Spomínate si na šikanu vo svojej triede? Na toho veľkého spolužiaka, čo značne znepríjemňoval život tým slabším a neoblúbeným? V súčasnosti mnohí z nich prešli na moderné technológie a anonymne číhajú na svoje obete na internete. Nezmenila sa však skutočnosť, že chcú iným psychicky ubližovať. Deti preto treba poučiť, aby na kyberšikanu (ohováranie na sociálnych sieťach, uverejňovanie posmešných,

nepravdivých statusov, či fotografií, vyhrážanie sa...) nereagovali, nič nevymazávali a aby okamžite informovali vás rodičov, ak sa s niečím takým stretnú. Vy ako rodič by ste v prípade zistenia kyberšikany mali situáciu podľa závažnosti riešiť okamžite aj v spolupráci so školou, kľudne aj podaním trestného oznámenia.

3. Finančné online transakcie sú iba pre dospelých

S nakupovaním na internete by nemal byť problém, pokiaľ postupujete opatrne, napríklad keď nakupujete u overených obchodníkov. Vedeli ste, že každý e-shop musí mať na stránke prevádzkovateľa, konkrétnu firmu so všetkými kontaktnými i fakturačnými údajmi? Rovnako aj reklamačný poriadok a pravidlá vrátenia tovaru. Kým deti neporozumejú potrebným preventívnym opatreniam, ktoré treba prijať pri odosielaní osobných a finančných informácií, mali by nakupovať iba pod dohľadom rodičov.



Slovník kybernetickej bezpečnosti

Doma alebo v škole

Hoci ako rodič máte rozhodujúcu zodpovednosť za kybernetickú bezpečnosť dieťaťa, neznamená to, že všetko musí ostať len na vašich pleciach. Zistíte, aké programy alebo kurzy ponúka škola, ktorú vaše dieťa navštevuje, a či sú medzi nimi aj lekcie zamerané na bezpečné používanie internetu. Ak vhodný kurz navyše vedie obľúbený učiteľ, môže byť naozaj vplyvným vzorom pre dospievajúce deti, ktoré odmietajú počúvať svojich rodičov. Škola môže stavať na základoch kybernetickej bezpečnosti, ktoré ste dali svojmu dieťaťu už predtým vy, a posunúť jeho vedomosti na ďalšiu úroveň.

Rodičovská kontrola

Predstavte si, že máte program, ktorým môžete nastaviť konkrétne časy a hodiny, kedy bude mať vaše dieťa prístup na internet, obmedziť typy stránok, ktoré môže navštevovať, povoliť mu alebo obmedziť hranie hier, alebo sledovať jeho presnú polohu. Ide o softvér rodičovskej kontroly, ktorý slúži ako účinný nástroj na kontrolovanie toho, čo váš syn alebo dcéra robí online.

Samozrejme je potrebné nechať nejaké slovo aj deťom. Pretože ak budú mať pocit, že sami nemajú kontrolu nad ničím a obmedzenia sú príliš tvrdé, iba ich to prinúti pravidlá obchádzať.

Sociálne siete

Predstavte si všetkých spolužiakov, priateľov a známych, ktorých ste v živote stretli. Teraz si predstavte väčšinu z nich v jednej miestnosti, ako hovoria o tom, čo práve robia, a ukazujú vám fotografie z dovolenky alebo obľúbené video. Takto dnes v podstate fungujú sociálne siete, ktoré umožňujú používateľom organizovať podujatia, komunikovať s ostatnými individuálne alebo v skupinách, a pozerať si, čo sa im páči.

Tento mikrokosmos, ktorý si vytvoríte, je len malou súčasťou nadstavby tvorenej stovkami miliónov používateľov, s ktorými môžete podľa želania navzájom komunikovať. Všetky tieto výhody však so sebou prinášajú aj niekoľko rizík. Napríklad, že do skupiny prenikne niekto, kto nemusí mať práve najčistejšie úmysli. Preto poučte svoje deti, aby potvrdili priateľstvo len tým ľuďom, ktorých skutočne poznajú.

Aké sú hlavné hrozby?

Malvér

Malvér je skrátený názov pre škodlivý softvér. Cieľom tohto typu aplikácií je poškodiť rôznymi spôsobmi počítač. Niektoré z nich zašifrujú súbory v počítači, iné slúžia na špehovanie alebo sťahovanie ďalších nebezpečných aplikácií do počítača.

Vo väčšine prípadov sa počítač infikuje v dôsledku nejakej chyby, ktorej sa dopustí používateľ (alebo jeho deti), keď sa nechá oklamať útočníkom.

Spam

So spamom ste sa už určite stretli. Označuje sa tak každý nevyžiadaný e-mail, ktorý denne dostávate do doručenej pošty. Tieto správy zvyčajne obsahujú inzerciu pozývajúcu vás na návštevu určitých stránok s „úžasnými“ ponukami.

Podvodné správy

Podvodné správy, tzv. scam, predstavujú podvodné činy vykonávané prostredníctvom internetu. Nadobúdajú rôzne podoby. Môžu mať napríklad formu spamu, ale môžu tiež využívať techniky sociálneho inžinierstva. V tom druhom prípade útočníci ponúkajú niečo na predaj, vystupujú ako vaši kolegovia alebo sa dokonca vydávajú za vašu banku, no chcú od vás iba získať dôverné informácie. Falošné správy šírené cez internet, ktoré vyžadujú vaše meno používateľa a heslo na sociálnej sieti, sú tiež príkladom scamu.

Kyberšikana

Toto nepriateľské správanie je zamerané najmä na deti. Obeti sa zvyčajne v kybernetickom priestore vyhrážajú alebo ju ponižujú jej rovesníci, pričom sa to často deje medzi dospievajúcou mládežou. Dieťaťu to môže potenciálne ublížiť a spôsobiť emocionálnu traumu. Kyberšikana sa zvyčajne odohráva cez internet, ale ani mobilné telefóny a herné konzoly nie sú proti tomuto škodlivému správaniu imúnne.

Grooming

Ide o situáciu, v ktorej sa dospelý človek snaží vzbudiť u dieťaťa pocit dôvery a citového prepojenia, aby ho následne mohol sexuálne zneužiť. V mnohých prípadoch dospelí predstierajú, že sú deti, aby sa im podarilo nadviazať blízky vzťah a následne sa mohli pokúsiť o osobné stretnutie. Pre rodiča je dôležité, aby mal dobrý prehľad o tom, s kým a ako dieťa komunikuje online.

Sexting

Pomenovanie sexting vzniklo zlúčením dvoch anglických slov, sex a texting, čiže odosielanie šteklivých správ. Ako naznačuje samotný názov, v začiatkoch sa tak označovali e-mailové správy s erotickým textom. V rámci technologického pokroku sa tak neskôr začalo označovať aj odosielanie fotografií a videí a stalo sa bežnou praxou, keďže väčšina mládeže a detí má svoje mobilné zariadenia vždy so sebou.

Krádež informácií

Všetky informácie, ktoré prechádzajú webom bez potrebných bezpečnostných opatrení, sa môžu dostať do rúk tretej strany. V mnohých prípadoch je práve toto účelom útoku. Zloději sa zvyčajne zameriavajú na krádež vašich osobných údajov alebo osobných údajov vášho dieťaťa. Nesprávnymi krokmi môže v tomto prípade maloleté dieťa spôsobiť stratu rodinných peňazí, prípadne môže dôjsť k odcudzeniu identity člena rodiny.



Návrhy na záver

1. Používajte nástroje rodičovskej kontroly

Môžete ich používať v prehliadačoch, ako aj v antivírusovom softvéri. Nájdete ich v balíku [ESET Internet Security](#) alebo tiež ako samostatnú aplikáciu [ESET Parental Control pre Android](#). Tento typ nástrojov je k dispozícii aj pre herné konzoly, ako sú Nintendo Wii a Xbox 360.

2. Nedovoľte, aby dieťa odosielalo cez internet dôverné informácie

Citlivé informácie by sa nikdy nemali vyžadovať prostredníctvom e-mailu alebo četu. Banky od vás nežiadajú týmto spôsobom údaje o účte a rozhodne nepožadujú uvedenie PIN kódu. Dôležité je, aby ste o tomto pravidle poučili aj svoje deti.

3. V prípade stalkingu (prenasledovania) neodpovedajte na správy a ani ich nemažte

Ak je dieťa obeťou kyberšikany, nemalo by šikanu oplácať. Vysvetlite deťom, že ten, kto ich takými správami prenasleduje a obťažuje, ich chce vyprovokovať presne k takej reakcii. Chcete totiž vidieť, ako im tým ubližuje. Ak sa stretnete s takouto situáciou a stane sa to znova, informujte príslušné orgány. Nikdy však také správy nemažte, budú slúžiť ako dôkaz.

4. Nie všetko, čo vidíte na internete, je pravda

Nie všetky informácie, ktoré nájdete na webe, pochádzajú zo spoľahlivého zdroja. Preto je dôležité, aby také informácie dieťa rozpoznalo. Vytvorte si blog a zverejnite tam svoj názor, aby ste ukázali, aké jednoduché je získať priestor online a manipulovať s obsahom príspevku.

5. Ved'te otvorený dialóg

Spôsob, akým komunikujete so svojimi deťmi, zohráva v ich bezpečnosti kľúčovú úlohu. Namiesto trestania je oveľa produktívnejšie povzbudiť ich, aby hovorili o tom, čo ich baví, čo na internete sledujú, ale aj čoho sa boja a čo ich trápi. Či je reč o internete alebo reálnom živote, pozitívne prostredie a otvorený dialóg môžu byť kľúčom k úspechu, pokiaľ ide o ich osobné blaho.

6. Ak niečo zverejníte online, zostane to tam navždy

Poučte svoje deti, že všetko, čo zverejnia online, tam už navždy aj zostane. Navyše nad daným obsahom stratia kontrolu, pretože ho bude môcť zdieľať ktokoľvek, vrátane úplne cudzích ľudí. Dobrým pravidlom je, aby nezdieľali žiadne fotografie, statusy ani iný obsah, ktorý by nechceli ukázať napríklad vám, starej mame, riaditeľke školy alebo pani učiteľke. Platí to pre všetky formy online prostredia – sociálne siete, okamžité správy, blogy či komentáre.

5 ďalších tipov pre rodičov

- 1:** Vytvorte dieťaťu vlastné používateľské konto. Tento prvý krok vám umožní účinne kontrolovať jeho online aktivity. Rolu správcu systému by mala vždy mať dospelá osoba.
- 2:** Pravidelne aktualizujte svoj operačný systém a všetky programy, ktoré máte nainštalované. Antivírusový softvér a nástroje rodičovskej kontroly sa vám v on-line režime budú aktualizovať automaticky.
- 3:** Monitorujte dieťaťu históriu prehľadávania. Ak ju odstráni, je to dobrý dôvod na rozhovor. Posúdiť však opodstatnenosť dôvodu vymazania histórie môže byť veľmi komplikované. Najlepšie bude dohodnúť sa vopred s dieťaťom na pravidle, že históriu vyhľadávania budete vymazávať vždy spolu.
- 4:** Kontrolujte webovú kameru a dbajte, aby bola v čase nepoužívania deaktivovaná alebo zakrytá (ak je vstavaná).
- 5:** Skontrolujte dieťaťu nastavenia na sociálnych sieťach. Ak je profil zdieľaný verejne bez obmedzenia, môže to ohroziť bezpečnosť mladého človeka.



Záver

V súčasnej dobe zakázať deťom prístup k technológiám nie je riešením. Patria do každodenného života a sú čoraz dôležitejšie pre ich rozvoj. Namiesto zákazov a obmedzení pomôžte deťom, aby ich dokázali bezpečne používať, a zapojte sa do interakcie medzi dieťaťom a zariadením. Treba tiež povedať, že mnohé z týchto rizík sa môžu týkať aj dospelých a mnohé z preventívnych opatrení, ktoré sú tu popísané, by mali byť samozrejmosťou v každej situácii a v každom veku.

Za bezpečnosť detí je zodpovedný každý a tipy uvedené v tomto dokumente pomôžu dospelým chrániť informácie, systémy a integritu maloletých. Ďalšie informácie nájdete na našich webových lokalitách a sociálnych sieťach:

www.eset.sk

www.welivesecurity.com

Staňte sa naším fanúšikom na stránke

<https://www.facebook.com/ESETnaSlovensku/>

