

RIZIKOVÁ KOMUNIKACE DĚTÍ ČASTO ZAČÍNÁ NA VEŘEJNÝCH PLATFORMÁCH. TO NEJNEBEZPEČNĚJŠÍ SE ALE MŮŽE ODEHRÁT V SOUKROMÍ

Kamil KOPECKÝ

Rizikový kontakt dítěte s neznámým člověkem na internetu nemusí probíhat a zůstat pouze na jedné platformě - z online her, sociálních sítí nebo dalších služeb se může postupně přesouvat do soukromých messengerů, kde komunikace získává intimnější charakter a může přejít v manipulaci, nátlak, sexualizovanou komunikaci nebo sextortion. Případy z poradny E-Bezpečí ukazují, že důležitější než samotný název aplikace je cesta, kterou komunikace prochází, a schopnost dítěte rozpoznat varovné signály bez ohledu na konkrétní platformu.

Když mluvíme o bezpečnosti dětí na internetu, velmi často se soustředíme především na sociální sítě, jako jsou TikTok, Instagram nebo Facebook. Jenže **skutečná riziková komunikace často neprobíhá pouze tam**. Kontakt může vzniknout na sociální síti, v online hře, v herním chatu, na komunitní platformě nebo prakticky kdekoli, kde spolu mohou uživatelé komunikovat. Následně se ale může přesunout do soukromého prostoru - na WhatsApp, Snapchat, Telegram, iMessage, Discord či jinou komunikační službu. A právě tam se může začít odehrávat ta nejrizikovější část celé komunikace.

Z veřejného prostoru do soukromého chatu

Přesun komunikace mezi platformami je dnes zcela běžný. Děti se s někým seznámí při hraní hry, začnou si psát, později si vymění kontakt na jinou aplikaci a pokračují tam. Samozřejmě na tom není nic špatného. Problém nastává ve chvíli, kdy **člověk na druhé straně začne získanou důvěru zneužívat**. Může se snažit dítě izolovat od ostatních, požadovat další osobní informace, fotografie či videa, postupně sexualizovat komunikaci nebo vytvářet emocionální tlak. Z hlediska bezpečnosti proto není důležité pouze to, na jaké platformě dítě je, ale také kam se komunikace přesouvá a co se během ní začíná dít.

Hry jsou také komunikačním prostředím

Do diskuse o ochraně dětí na internetu bychom proto neměli zahrnovat pouze klasické sociální sítě. Online hry a herní platformy jsou dnes zároveň sociálním prostředím, ve kterém děti komunikují, navazují vztahy, vytvářejí skupiny a přátelství. A právě zde se mohou setkat také s lidmi, které ve skutečnosti neznají.

Dobře to ukazuje jeden z případů, který letos řešila poradna E-Bezpečí. Třináctiletá dívka komunikovala s jednadvacetiletým mužem z Rumunska prostřednictvím **Robloxu** a **Snapchatu**. Podle jejího popisu jí muž vyhrožoval smrtí, přál jí znásilnění a opakovaně ji nabádal, aby se zabila. Obtěžování přitom nebylo omezeno na jediný účet – muž měl podle dívky vytvořit více než padesát dalších účtů, prostřednictvím kterých v kontaktu pokračoval. **Velká část komunikace probíhala na Snapchatu**, přestože kontakt souvisel také s Robloxem. Tento případ dobře ukazuje, že komunikace dětí často neprobíhá uvnitř jedné jediné aplikace. Může začít ve hře a pokračovat třeba na messengeru, případně se přesouvat dál. Blokování jednoho účtu navíc nemusí problém ukončit, pokud pachatel zakládá další profily a opakovaně se vrací.

Riziková komunikace může začít i přímo v messengeru

Ne vždy musí kontakt vzniknout na veřejnější platformě a následně

se přesunout do soukromého prostředí. Někdy začne přímo tam. Poradna E-Bezpečí například řešila případ **dvanáctileté dívky, která (podle jejího tvrzení) na WhatsAppu omylem napsala na neznámé telefonní číslo**. Na druhé straně byl pětatřicetiletý muž. Zpočátku podle jejího popisu komunikace působila relativně běžně a dívka se snažila zjistit, s kým si píše. Muži uvedla, že je jí šestnáct let, a poslala mu fotografii jiné šestnáctileté dívky nalezenou na internetu. Ani informace, že komunikuje s nezletilou dívkou, muže neodradila. Naopak začal požadovat nahé fotografie a otevřeně sexualizoval konverzaci. Dívce podle jejího popisu vysvětlil, že fotografie chce pro své vlastní sexuální uspokojení. **Ve skutečnosti přitom komunikoval s dvanáctiletým dítětem.**

Tento případ názorně ukazuje, proč **nelze při debatě o bezpečnosti dětí ignorovat messengery**. WhatsApp je především běžný komunikační nástroj pro rodiny, spolužáky, školy, sportovní oddíly a přátele, současně ale umožňuje soukromou komunikaci mezi lidmi, kteří se vůbec neznají. Důležitý proto není pouze název aplikace, ale především **charakter samotné komunikace**.

Přesun mezi platformami může odkrývat další informace

Přechod z jedné platformy na druhou navíc nemusí znamenat pouze změnu komunikační aplikace. Může zároveň znamenat, že útočník získává další informace. Na jedné platformě může získat pouze přezdívku, na jiné získá fotografii, na messengeru telefonní číslo a na Instagramu může najít jméno, přátele, školu nebo seznam sledujících... a samozřejmě i fotografie. Informace se tak mohou postupně skládat do poměrně přesného obrazu identity dítěte.

Velmi názorně to ukazuje případ patnáctiletého chlapce, který letos také řešila poradna E-Bezpečí. Chlapec se seznámil s neznámou osobou na jedné z veřejných online platforem. Komunikace následně přešla přes další službu na **iMessage**. Zpočátku si oba vyměnili běžné fotografie. Protistrana mu poté napsala, že se jí líbí, a požádala ho o jeho **Instagram**. Chlapec svůj účet nejprve poskytnout nechtěl. Když ale druhá osoba začala reagovat

agresivně, nakonec ustoupil. Právě Instagram se později stal důležitou součástí vydírání, protože útočník získal přístup k informaci, kdo chlapce sleduje. Následně začal požadovat intimní fotografie. Chlapec je poslal a komunikace se postupně změnila v sexuální vydírání – sextortion.

Když se později podíval do telefonu, našel zprávy obsahující jeho vlastní intimní fotografie, snímek jeho instagramového profilu a seznam lidí, kteří jej sledují. Útočník mu oznámil, že pokud nebude spolupracovat, materiály rozešle jeho kontaktům. Chlapec pod tlakem koupil dárkovou kartu v hodnotě 20 dolarů. Protistrana mu dokonce poslala video, které mělo dokazovat, že fotografie maže, po předání kódu ale vydírání neskončilo. Následoval nový požadavek – tentokrát na 500 dolarů. Chlapec následně komunikaci ukončil a účet zablokoval, útočníci se jej ale ještě několikrát pokusili kontaktovat z dalších účtů.

Tento případ velmi přesně ukazuje typickou cestu: **první kontakt → získání důvěry → přesun komunikace → získání dalších informací → sexualizace komunikace → intimní materiál → výhrůžka zveřejněním → finanční požadavek.**



Sextortion často pracuje se strachem ze zveřejnění

Podobný mechanismus se v poradně E-Bezpečí objevuje opakovaně. V dalším případě navázal osmnáctiletý uživatel kontakt s údajnou ženou prostřednictvím **erotické seznamky** a komunikace se následně přesunula na **Telegram**. Protistrana začala posílat vlastní fotografie a požadovala fotografie a video také od mladého muže. Jakmile intimní materiál získala, charakter komunikace se zásadně změnil. Uživateli byla zaslána vytvořená koláž obsahující jeho jméno, telefonní číslo a nepravdivé tvrzení, že je hledán v souvislosti se sexuálním obtěžováním. Následoval požadavek na zaplacení 100 dolarů prostřednictvím dárkové karty.

Stejný princip se objevil i v jiném případě dospělého uživatele. Muž si začal psát s údajnou ženou prostřednictvím **seznamovací**

služby, která komunikaci přesunula na **WhatsApp**, tvrdila, že je z USA a právě pobývá v Praze. Komunikace postupně přešla k sextingu. Protistrana si vyžádala intimní video, následně dohledala mužův facebookový profil a jeho kontakty a začala vyhrožovat, že video rozešle jeho přátelům, pokud okamžitě nezaplatí.

Tyto případy se sice netýkají pouze dětí, ale velmi dobře ukazují způsob, kterým sexuální vydírání funguje. Útočník nepotřebuje znát oběť osobně. Potřebuje získat materiál, kterého se oběť obává, a současně vytvořit dojem, že jej může velmi snadno rozšířit mezi konkrétní lidi.

Každá další platforma může odkrýt další část identity

To je důležité i pro prevenci. Pokud dítě někomu poskytne informace o svém účtu na jiné platformě (typicky nějaké veřejné), nemusí mu tím dávat pouze možnost komunikovat pomocí dalšího kanálu. Může mu zároveň zpřístupnit celé jméno, fotografii, seznam přátel, spolužáky, školu, rodinu, místo bydliště, zájmy nebo další sociální profily.

Jednotlivé informace samy o sobě nemusí být problém. Jejich propojením ale může vzniknout poměrně přesný obraz identity dítěte. Právě proto může mít zdánlivě nevinná otázka „Nemáš Instagram?“ nebo „Napiš mi na WhatsApp“ v určitém kontextu mnohem větší význam, než se na první pohled zdá.

Při regulaci sociálních sítí nesmíme zapomenout na messengery a hry

Současné diskuse o ochraně dětí se velmi často zaměřují na věkové hranice sociálních sítí. Je to legitimní a důležité téma. Pokud se ale debata zúží pouze na klasické sociální sítě, část problému nám unikne. **Děti totiž nekomunikují pouze na Instagramu nebo TikToku, ale také na WhatsAppu, Snapchatu, Discordu, iMessage, v Robloxu a v celé řadě**

dalších her a komunikačních služeb.

A komunikace mezi těmito prostředími velmi snadno přechází. Proto bychom se neměli ptát pouze: „**Má dítě používat tuto sociální síť?**“ Stejně důležitá je otázka: „**Ví dítě, jak se zachovat, když ho někdo osloví, požádá ho o přesun komunikace jinam nebo začne vyvíjet nátlak?**“

Děti nelze kontrolovat 24 hodin denně

Bezpečnost dětí na internetu nelze postavit na permanentní kontrole. Rodič nemůže být s dítětem 24 hodin denně, číst každou zprávu, sledovat každý herní chat, kontrolovat každého spoluhráče ani vědět o každém novém kontaktu. A čím je dítě starší, tím méně je taková kontrola realistická.

Právě proto musí prevence směřovat k tomu, aby **dítě postupně dokázalo rizikovou situaci rozpoznat samo**. Mělo by vědět, že člověk na internetu nemusí být tím, za koho se vydává, že nemusí vyhovět požadavku na přesun komunikace jinam ani posílat fotografie nebo videa, které posílat nechce. Mělo by umět zpozornět ve chvíli, kdy někdo komunikaci sexualizuje, požaduje utajení, vytváří tlak nebo vyhrožuje. A především by mělo vědět, že při problému může komunikaci ukončit, uchovat důkazy a obrátit se na důvěryhodného dospělého. U závažného vyhrožování nebo vydírání je namístě obrátit se také na policii.

Nestačí zakazovat. Dítě se může přesunout jinam

Pravidla a omezení mají své místo. **Problém nastává ve chvíli, kdy se z prevence stane pouze seznam zákazů: nesmíš na TikTok, nesmíš na Instagram, nesmíš si psát s cizími lidmi.** Pokud dítě nerozumí důvodům, které za těmito pravidly stojí, nemusí zákaz vést k bezpečnějšímu chování. Může vést pouze k tomu, že se **dítě přesune jinam. A nová platforma nemusí být**

bezpečnější. Může mít horší moderaci, menší možnosti nahlašování, slabší ochranu nezletilých nebo může být pro rodiče prakticky neznámá. Proto je důležité děti zbytečně nestrašit a nespoléhat pouze na zákazy. Místo toho je potřebujeme naučit principům, které budou fungovat bez ohledu na to, jak se konkrétní aplikace jmenuje.



Digitální výchova musí začít ještě před prvním telefonem

Prevence by navíc neměla začínat až ve chvíli, kdy nastane první problém. Měla by začít ještě předtím, než dítě dostane svůj první vlastní telefon nebo první účet v online službě. Když dítě poprvé začne samo chodit přes silnici, také nečekáme, až ho málem srazí auto. Předem mu vysvětlujeme, jak funguje semafor, kde může přecházet, na co se musí dívat a co má dělat v nebezpečné situaci.

Podobně bychom měli postupovat také v online prostředí. Ještě před prvním vlastním telefonem by dítě mělo znát základní zásady bezpečného chování na internetu, tedy například, kdo ho může kontaktovat, co o sobě nemá bez rozmyslu sdílet, co má dělat při nátlaku, komu se může svěřit a jak pozná, že se komunikace začíná měnit v něco nebezpečného.

První telefon by proto neměl být začátkem digitální výchovy (ta musí začít daleko dříve). Měl by být až jedním z jejích milníků.

Neučme děti seznam aplikací. Učme je principy bezpečného chování na internetu

Konkrétní komunikační aplikace a nástroje se neustále mění, některé vznikají, jiné zanikají (starší z nás si pamatují v minulosti velmi populární služby ICQ, Miranda, Skype nebo třeba Omegle). To, co používají děti dnes, nemusí používat za pár let - zcela jistě

budou používat něco nového, populárního, zajímavého. **Principy rizikové komunikace ale zůstávají velmi podobné: někdo se snaží navázat kontakt, získává důvěru, přesouvá komunikaci do soukromí, zjišťuje další informace, začíná vyvíjet tlak, požaduje fotografie, peníze nebo určité chování a může přejít i k výhrůžkám.**

Proto je důležité s dětmi probírat tato témata: **Kdo se mnou komunikuje? Co o mně ví? Co po mně chce? Proč chce, abychom komunikovali někde jinde? Je mi tato komunikace příjemná? Mohu ji kdykoli ukončit? A komu to řeknu, když se něco pokazí?**

Rodiče nemohou chránit děti každou minutu jejich online života. Mohou je ale připravit tak, aby v okamžiku, kdy u nich nebudou, dokázaly rizikovou situaci rozpoznat a požádat o pomoc.

Pro E-Bezpečí
Kamil Kopecký