

PRAXE Z PRVNÍ LINIE: JAK ŘEŠÍME KYBERŠIKANU, SEXTING A DALŠÍ ONLINE RIZIKA V NAŠÍ PORADNĚ

Pavel SCHWEINER

Digitální technologie se staly neoddělitelnou součástí našich životů, přinášejí nám neomezené možnosti komunikace, vzdělávání i zábavy. S rostoucí digitalizací však úměrně narůstá i škála rizik, kterým jsou uživatelé – od dětí až po dospělé – vystaveni. E-Bezpečí (Univerzita Palackého v Olomouci- Institut výzkumu a vzdělávání v oblasti digitálních technologií a kyberbezpečnosti) se dlouhodobě zaměřuje na řešení těchto incidentů v poradně www.napisnam.cz. Ne jinak je tomu i v roce 2026

Nejčastějšími typy problémů, o které se lidé obrací na naši poradnu jsou Kyberšikana a Sextortion, které tvoří významnou část všech případů. Žel nezaostává ani problém týkající se sdílení intimního materiálu „Sexting“. Níže uvádíme syntézu nejčastějších problémů, se kterými se na naši poradnu obracejí oběti digitálních útoků.

Anonymizovaný přepis některých případů z poradny:

„Dobrý den, stal jsem se obětí kyber vydírání. Byl jsem zlákan dotyčnou osobou na messengeru k ukázání intimních partií. Teď mě vy vydírá a vyhrožuje mi, že dané fotografie a video bude sdílet veřejně i mé rodině a přátelům a i do

práce. Pokud zaplatím peníze. Nevím co dál dělat. (vek 26)“

„Byl jsem na seznamce a dala mě lajk jedna holka ale nebyla to holka byl to kluk a vydával se za holku chtěl abych mu posla instagram a pak jsme byli na telegramu potom chtěl videt fotku jak vypadám tak jsem ji poslal a on to zneužil (vek 19)“

„dobrý den byl jsem na ome.tv tam jsem potkal jednu holcinu a ta chtěla jit volat na whatsapp tak sem sel puvodne jsem si myslel ze je to jen nejaka holka ktera se chce tez zabavit ale pote jsem zjistil ze cely hovor nahravala a tedka vyhrozuje ze to rozesle uz to par lidem pry poslala (vek 17)“

Důležité je nikdy neplatit. Požadavek na peníze je pouze začátek a útočník bude své požadavky stupňovat. **Zajistěte si důkazy (screenshoty komunikace, URL profily útočníka)**, komunikaci přerušete, útočníka zablokujte.

Jak už bylo uvedeno v poradně řešíme i rizika spojená se SEXTINGem, dobrovolné i nedobrovolné sdílení intimního obsahu (sexting) nese vysoké riziko. Takový materiál se často stává nástrojem šikany, pomsty nebo se nekontrolovaně rozšíří v kyberprostoru.

„Stala se mi neprijemna vec, pred nekolika lety jsem mela internetového pritele, kdy jsme si posilali intimni fotky, bohuzel jsem zjistila, ze tyhle fotky ted behaji po internetu, da se proti tomu nejak branit? Uz je to 5 let zpatky, ja jsem vsechno ze svoji minulosti smazala, a vim, ze jsem to delat nemela, bohuzel jsem byla poblaznena. (vek 27)“

„Můj bývalý se přiznal k šíření videa kde jsme provozovali sexuální aktivitu k zveřejnění jsem mu nedala souhlas a poté mě nabádal k sebevraždě jak to mohu řešit?“

„dobrý den,dva roky zpatky jsem svemu spoluzakovi poslala nahou fotku.Je mi to ted moc lito ale nic s tim nemuzu udelat,jsem nezletila ale nemohu to resit s rodici a bojim se to resit s policii.Ten spoluzak to ukazal jeho

kamaradovi u nas ve tride, furt se posmival atd...Řekla jsem to učitelce a ta mi poradila ať to jdu řešit s policií, ale ja vazne nemuzu, bojím se ze by to treba zverejnil na socialni site.... (vek 15)“

„Dobrý den, jsem v jedné dost divné a pro mě stresující situaci, ale nevím jestli je to vhodné to řešit zde. Je mi 16, a nějakou dobu jsem používal snapchat pros sexting, výměnu fotek atd...Vůbec nevím jestli to bylo nelegální nebo jak... Plus, jsem jednou dostal od někoho porno video, které jsem potom později přeposlal nějakému člověku (myslel jsem, že je to normální video normálně dospělého herce, ale zpětně si říkám že vůbec nevím, asi jsem to fakt podělal.) před pár dny jsem dostal ban v aplikaci za `sexual content involving minor`. Od té doby jsem úplně v háji a nevím co mám dělat a co si myslet. Bojím se, že se zapojí policie, a z představy ci to vidí bylo je mi nazvraceni. Co mám dělat? Měl bych sám nějak kontaktovat policii i když ani nevím co jsem udělal, abych nějak vysvětlil situaci? Jak je to z právního hlediska? (vek 16)“

„asi před rokem se mi stalo to, že jsem s jedním klukem měla sexuální kontakt a on si me nevědomě natočil a fotil. Zaprvé už to bylo před rokem tak nevím jestli se s tím dá ještě něco dělat, a za druhé moc nevím jak se situace má protože mi všichni říkají něco jiného. Ze všech stran a do ted kdybych se někoho zeptala tak mi řeknou že to video dal všude a poslal všem ale on tvrdí že ne. Nevím co mám dělat protože nevím jestli to někde není ještě a začíná mě to psychicky dohánět. (vek 16)“

Sexting je vysoce rizikový především proto, že jakmile intimní obsah odešlete, ztrácíte nad ním trvalou kontrolu, což z něj činí ideální nástroj pro vydírání, nebo mstu ze strany bývalých partnerů. Takto sdílený materiál může být zneužit k destruktivní kyberšikaně s devastujícími dopady na psychické zdraví, přičemž jeho šíření zanechává nezvratnou „digitální stopu“, která může v budoucnu komplikovat profesní i osobní život. Z právního hlediska navíc hrozí u nezletilých závažné následky spojené s šířením dětské pornografie, a to i v případech, kdy byl obsah odeslán dobrovolně, což z něj dělá nebezpečnou hru, při níž osobní důvěra

v digitálním prostoru často selhává.

KYBERŠIKANA představuje opakované a úmyslné útoky prostřednictvím digitálních technologií. Často přechází z online prostředí do reálného světa (škola, pracoviště).

„Dobrý den, nějaký kluk mi psal hnusné zprávy a hlasovky a nadával mi , a ptal se kde bydlím a já jsem si ho zablokoval ale nevím co dál a nechci aby to věděli rodiče psal mi kolik mu je a jak se jmenuje . Nevím jestli s tím na policii nebo tak nevím takže bych potřeboval porad a psal mi jak ať držím picu že jsem kokot a tak potřeboval bych poradit prosím děkuju . (vek 12)“

„Dobrý den, obracím se na Vás v kritické situaci. Stal jsem se obětí masivní kyberšikany a šíření ponižujícího videa, o jehož existenci jsem donedávna vůbec nevěděl.

Video bylo natočeno pod nátlakem a násilím před 14 lety ještě na Ukrajině. O existenci záznamu jsem nebyl informován. Podle mých informací bylo video nahráno na internet nebo se začalo masivně šířit kolem poloviny března 2026. Obsah videa je lživý a zinscenovaný pod hrozbami s cílem mě ponižit. Kolegové mi sdělili, že se ve videu objevuje motiv nebo zmínka o `včelách` (včely). K šíření dochází v xxxx mezi mými kolegy v práci a v ubytovně. Já sám ho nemohu najít, ale vím, že se šíří v soukromých skupinách. Mojí jedinou prioritou je technické zastavení šíření videa a jeho odstranění, abych mohl v klidu žít a pracovat. Potřebuji pomoc s vyhledáním a odstraněním tohoto videa z internetových platforem. Prosím o radu, jak postupovat diskrétně, aby se situace dále nevyostřovala.“

U kyberšikany je klíčová dokumentace. Ukládejte si zprávy, záznamy obrazovek a svědectví. Pokud instituce (škola, zaměstnavatel) situaci neřeší, je nezbytné obrátit se na vyšší orgány či právní pomoc.

Postupně se dostáváme k dalšímu poměrně rozsáhlému problému a tím jsou **ONLINE PODVODY**, „výhodné“ investice. Podvodníci využívají techniky sociálního inženýrství, zneužívají deepfake

technologie a manipulují oběti k finančním převodům nebo prozrazení osobních údajů. Ve stručnosti uvedu časté online formy podvodného jednání:

Vishing (hlasový podvod): Pachatel vydávající se za Policii ČR zneužívá strach oběti k získání osobních dat.

Deepfake investiční podvody: Zneužití tváří známých osobností k vylákání investic.

Recovery Scam: Opakované podvody na lidech, kteří již jednou o peníze přišli a zoufale hledají cestu zpět.

A co zachytila naše poradna?

„Dobrý den, dnes mi volalo neznámé číslo. Paní se představila jako důstojnice pražské kriminálky. Říkala, že se mi pokusil jakýsi Horvát vybrat účet v bance, kterou ani nemám. Ptala se, jestli ho neznám, což neznám. Pak jen ověřovala již známé údaje - jméno a bydliště. Chtěla taky znát datum narození, což jsem ji žel v tom rozrušení prozradil. Nakonec jsem hovor ukončil s tím, že půjdu na místní policii a vyřeším to s nimi. Ona s tím souhlasila, jen že jim pošle všechna patřičná data. Tím byl hovor ukončen. Na policii jsem volal, tam mi řekli, že s největší pravděpodobností šlo o podvod. Mé telefonní číslo už měli, stejně tak i adresu a jméno. Teď jim přibylo i datum narození. Je to pro mě nebezpečné, mohou si na mě vzít například nebankovní půjčku? (vek 30)“

„Dobrý den, potřeboval bych se zeptat na něco, co se stalo mým rodičů. Otec uvěřil deepfake videu (Nedělní partie - Babiš slibuje v přímém přenosu zisk při investici do NB - moderátorka Tománková v přímém přenosu investuje, vydělává..). Otec naletěl, zaregistroval se - uvedl emailovou adresu a telefonní číslo. Poslali mu email, který otevřel (nevím už, jestli byla součástí příloha či nikoli..). Neustále mu volá číslo s UK předvolbou, nezvedá to, takže k dalšímu kontaktu nedošlo. Máme samozřejmě strach, jakým způsobem by mohlo být ohroženo bezpečí jejich účtu. Z jiného počítače jsem jako disponent pro jistotu převedl

peníze na jiný účet, ke kterému nemají internetové bankovníctví a PC pro jistotu používat nebudou než jej zkontroluju. Zajímalo by mne, jakým způsobem v tomto případě podvodníci postupují, chtěli postupovat...určitě s tímto videem máte nějaké zkušenosti...jestli otce chtěli přesvědčit, aby peníze sám poslal nebo se mám obávat nějakého viru v počítači...“

„Dobrý den. Mam kamaradku, ktera naletela podovodnikum s kryptomenama. Je to velmi inteligentni a schopna zena. v jinych oblastech. ale tady jakoby mela slepou skvrnu. opakovane jim napolilala velke castky. vzdy po slibech, ze poslanim dalsi castky zachrani ten zbytek a vydela penize zpet. mluvil s ni manzel, bratr, i dalsi. ale ona tomu porad veri. situace je velmi vazna. Hledam odbornika psychologa/psychiatra, kteri se teto lecbe zavislosti venuji. potrebuji odbornika na ten Recovery Scam. (vek 48)“

Online podvody jsou nebezpečné zejména svou rafinovaností, neboť útočníci mistrně využívají techniky sociálního inženýrství, jako je manipulace, vyvolávání strachu nebo falešný pocit naléhavosti, čímž obcházejí technické zabezpečení přímo přes lidskou důvěřivost. Aby uživatel nenaletěl, je klíčové dodržovat digitální hygienu: nikdy neklikejte na podezřelé odkazy v nevyžádaných e-mailech či zprávách, vždy si ověřujte identitu odesílatele (např. voláním na oficiální číslo instituce), používejte dvoufázové ověření u všech důležitých účtů a při jakékoli finanční transakci či požadavku na osobní údaje zpomalte a kriticky přemýšlejte, zda situace nepůsobí nepřírozeně či nátlakově.

Naše poradna se nevyhnula ani šíření **RADIKÁLNÍ IDEOLOGÍÍ**.

„Dobrý den, prosím o radu, zda se dá `zkontrolovat` profil jednoho žáka SŠ, xxx - dlouhodobě zastánce nacismu, Hitlera, popírání holocaustu, ve škole se hlásí hajlováním, antisemita, projevy i v písemných pracích apod. Před cca 2 lety na soc. síti zveřejnil fotku jedné učebny naší školy s popiskem ...to nutkání pořídít si střelnou zbraň... . Toho času řešeno domluvou, došlo k utlumení těchto projevů, nyní opět v hodinách silně pronacistické projevy i názory,

na toaletě v suterénu školník objevil jeho zákoutí, něco jako `hnízdo`. Pravděpodobně místo šatní skřínky, ale tu má k dispozici, tudíž nevíme proč má tendenci se zdržovat na WC. Zjistili jsme vazbu na dalšího, stejně smýšlejícího jedince, spolužáka ze ZŠ. Jedná se o bratra jiné naší žákyně, která je z bratrovy strany vystavena i fyzické agresi (kroucení rukou, údery). Rodiče informování o ubližování, ale pro zletilost bratra to řeší domluvou. Vzhledem k dění na školách máme obavu, zda by nemohlo dojít, i později, k nějaké touze po pomstě apod. směrem ke škole. XXX se chová zvláštním způsobem, třída z něj má strach, ale nemáme nic konkrétního v ruce, pro podání oznámení na PČR. Mohu požádat o radu? Moc děkuji za Vaši pomoc.“

„Dobrý den, v naší škole - konkrétně u žáků 8. třídy - dochází k tomu, že si ve škole o přestávkách hrají `na ministry`, konkrétně např. na ministra Macinku, pravděpodobně sledují jeho sociální sítě a napodobují styl jeho komunikace. Nedávno např. naši osmáci říkali spolužačkám, ať si vezmou Xanax na uklidnění, a když se žákyně bránily, žáci řekli, že jsou ví, že jsou hrozní a smáli se. Opakovaně také říkají o spolužácích, že jsou `méněcenní` a že to viděli na internetu říkat ministra, tak to můžou říkat taky. Spolužákovi z vedlejší 7. třídy 2 osmáci řekli, že je `hovado a křivá svině` s tím, že to můžou říkat, protože to říkají ministři a je to normální. Stejně tak používají další urážky, třeba o spolužačkách, že jsou slepice, krávy a prasata, a že to opět viděli u ministra na nějaké síti. Nevíme, jak postupovat, běžné vysvětlování principů slušného chování nepomáhají, stejně jako sankce. Vůbec netušíme, jak postupovat. Poradíte? (vek 14)“

Pronacistické projevy žáků a glorifikace násilí představují závažné selhání v oblasti školní kultury i morálních hodnot, které přímo ohrožuje bezpečné prostředí třídy. Napodobování agresivní rétoriky veřejně známých osobností a přebírání jejich urážlivého slovníku vede k nebezpečné dehumanizaci spolužáků, kdy jsou oběti označovány za méněcenné či nehodné respektu. Takové chování nejenže podkopává základy demokratické diskuse a vzájemné tolerance, ale v extrémních případech může přerůst v otevřenou

šikanu, fyzickou agresi a radikalizaci, která vyžaduje okamžitou a důslednou intervenci pedagogů i vedení školy.

Prevenici radikalizace a nenávistných projevů ve škole nelze zajistit pouhými zákazy, ale vyžaduje systematický přístup založený na **aktivní edukaci a budování bezpečného klimatu**. Základem je **mediální gramotnost**, která žáky učí kriticky hodnotit obsah na sociálních sítích, rozpoznat techniky manipulace a chápat, že agresivní rétorika politiků či influencerů není návodem pro osobní komunikaci. Klíčová je také **otevřená komunikace** mezi pedagogy, žáky a rodiči, kdy se neřeší pouze sankce, ale i příčiny frustrace žáků, a podpora **emoční inteligence a empatie**, které jsou jedinou účinnou protiváhou k násilným a nenávistným ideologiím.

ONLINE HRY jsou fenoménem, který nabízí prostor pro socializaci a rozvoj strategického myšlení, ale zároveň představují specifické digitální prostředí, kde se uživatelé, zejména děti, mohou setkat s řadou rizik.

„Synovi píše jeho 13ti letý kamarád pod účtem policie na třídní skupinu na WhatsApp a už si měnil i heslo na robloxu a stejně mu tam leze a mizí mu věci z té hry. A vím, že to policie není. A i si ho zablokoval a on stejně mu dělá zlé věci z jiného čísla (vek 10)“

„Na Whatssapu je jedna skupina adopt me což je vlastně roblox hra Na té skupině jsem správcem a objevil jsem tam nějakého člověka okolo 30-40 let. Na té skupině jsou převážně holky kterým je 7-14 let a tento starší člověk se dopustil myslím že groomingu. Psal holkám něco že jsou krásné a že prostě by si dali sraz v Brně atd. Jako správce jsem člověka vyhodil a upozornil členy na bezpečnost na internetu. I když byl vyhozen snaží se prý holky kontaktovat. Holky si ho blokují a zprávy mažou. Co víc mohu udělat? (vek 15)“

„Měla sem takovou hru zepeto a jedna holka si koupila diamanty říkala že když ji dám účet tak mi dá její účet a budu tam mít i ty diamanty mě to netrklo a já ji dala e-mail a heslo teď je na mém účtě všem píše a dělá ze to sem já

(vek 14)“

Online hry představují specifické riziko především kvůli anonymitě, která pachatelům umožňuje maskovat identitu a zneužívat důvěřivost uživatelů k tzv. groomingu, kyberšikaně či krádežím herních účtů prostřednictvím manipulace. Aby se uživatelé rizikům vyhnuli, je zásadní striktně chránit soukromí, nikdy nesdílet osobní údaje ani přihlašovací hesla, aktivovat dvoufázové ověření a v případě nátlaku či podezřelého chování ostatních hráčů okamžitě komunikaci ukončit, osobu nahlásit a blokovat. Klíčem k bezpečí je digitální obezřetnost a vědomí, že herní prostor by měl zůstat zábavou, kde jakýkoli požadavek na intimitu či sdílení citlivých dat představuje varovný signál k okamžitému odchodu.

Sebepoškozování a duševní zdraví. Digitální svět může být katalyzátorem psychických potíží. V případech, kdy uživatel vyjadřuje úmysl ublížit si, je nutná okamžitá intervence.

„Mám chuť si něco udělat (vek 22)“

„Kamaradka XXXX mi začala psát ze se chce zabit, ze je už ze vsecho unavena ze nikdy byla skoro znasilnena, uz se zkusila zabit v 9, psala ze o pulnoci se predavkuje ale prestala odepisovat uz driv, neni z ceska myslim (vek 14)“

„Taky se nedokáží vůbec, vůbec soustředit ve škole, protože myslím na to jaké dostanu známky a co bude doma. Prosiim pomocte. Strašně se ho bojím. A už nevím co mám dělat. Jako jediný řešení vidím asi tu sebevraždu. Dekuji. (vek 13)“

Prevence a včasná pomoc jsou pilíři bezpečného pohybu v digitálním prostředí. Pokud se ocitnete v situaci, která vás stresuje nebo ohrožuje, **neřešte ji sami**. E-Bezpečí a jeho poradna www.napisnam.cz je zde pro vás, aby poskytla metodickou podporu, právní doporučení a pomoc při řešení krizových stavů.

Pokud se ocitnete v situaci, která vás stresuje, ohrožuje nebo se týká kybernetické kriminality, **neřešte ji sami**. Existuje řada institucí a linek, které vám poskytnou odbornou pomoc, anonymní poradenství či právní podporu (např. : **Linka bezpečí (116 111)**):

Bezplatná, anonymní pomoc pro děti a mládež do 26 let v krizových situacích).

Pamatujte, že sdílení problému s odborníkem je prvním a nejdůležitějším krokem k jeho úspěšnému vyřešení. Nikdy v problémech nezůstávejte sami, existují cesty, jak vaši digitální bezpečnost a duševní klid opět obnovit.

Poděkování

Online poradna E-Bezpečí funguje díky podpoře partnerů, kterým patří naše poděkování za dlouhodobou spolupráci a důvěru. Mezi podporovatele patří **Ministerstvo vnitra ČR, Statutární město Olomouc, Olomoucký kraj, O2 Czech Republic.**

E-Bezpečí
Pavel Schweiner s využitím AI
Univerzita Palackého v Olomouci