EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Metodika kybernetické bezpečnosti pro pedagogy SŠ

Centrum Informační Společnosti

Ve spolupráci s ba consulting - cz s.r.o.

OBSAH

VYSVĚTLIVKA:

Důležité: ⇨⇨⇨

ÚVOD

V dnešní době platí, že klíčové informace mohou mít cenu zlata. Neexistuje organizace (komerční subjekt nebo orgán veřejné správy), která by nějakými důležitými informacemi nedisponovala. Výrazný nárůst zavádění a používání informačních technologií vede k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb. Tím ale narůstá závislost společnosti na těchto technologiích.

Se vzrůstající závislostí společnosti na informačních technologiích stoupá riziko jejich zneužívání, které může vést ke značným škodám. Obecným trendem na celém světě je kvalitní ochrana informačních technologií před útoky, které by mohly ohrozit jejich fungování. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru, a to jak v národním, tak v globálním měřítku. V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu.

S obrovským rozvojem technologií dnes lidstvo přechází do pátého rozměru, do virtuálního světa. Všechno, co se dnes děje v naší realitě, doprovázejí také aktivity ve virtuálním kyberprostoru. Proto se celosvětovým problémem stávají i rostoucí kybernetické útoky. Útoky proti informačním technologiím jsou stále sofistikovanější a komplexnější. Zajištění kybernetické bezpečnosti jednotlivých států je jednou z klíčových výzev současné doby. Bezhraničnost a všudypřítomnost kybernetických hrozeb vyžaduje intenzivní mezinárodní spolupráci a také intenzivní úsilí při zajišťování kybernetické bezpečnosti jednotlivých států. Oblast kybernetické bezpečnosti je a bude jedním z určujících aspektů bezpečnostního prostředí vyspělých zemí. Stále větší část ekonomických aktivit se přesouvá do prostředí internetu – do kyberprostoru. Vznikem sociálních sítí se z nejznámější části kyberprostoru (internetu) stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.

Stejně tak jako informační a komunikační technologie (dále též jen „ICT"), i kybernetická bezpečnost podléhá neustálému a velice dynamickému vývoji. Příkladem může být samotné zaměření kybernetické bezpečnosti, která se z původně výlučně technické disciplíny vyvinula ve strategický koncept[1], který pronikl do různých oblastí lidského života, oblast práva nevyjímaje. Tento vývoj spolu s výše uvedeným dopadem kybernetické bezpečnosti na všechny subjekty moderní informační společnosti se pak následně odráží i v tom, co je pod pojmem „kybernetická bezpečnost" chápáno.

Cílem této metodiky je poskytnout základní přehled o problematice kybernetické bezpečnosti. Publikace je především určena pro pedagogické pracovníky, ale vzhledem ke globálnímu tématu ji může využít i široká veřejnost. Dokument pomáhá učitelům a ředitelům se připravit na výzvy, které je ve škole v 21. století čekají. V reakci na koronavirovou krizi obsahuje i část zaměřenou na bezpečnou online výuku, je aktuální i v rámci běžné výuky. Zaměřuje se především na praxi a nabízí konkrétní řešení a doporučení.

[1] GEERS, Kenneth. *Strategie Cyber Security* [online]. Tallinn: CCD COE Publication, 2011, s. 9. [cit. 23. 12. 2018]. ISBN 978-9949-9040-7-5 (pdf). Dostupné z: http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF

1. KYBERNETICKÁ BEZPEČNOST

Ačkoliv je kybernetická bezpečnost aktuálně velice používaným pojmem, existuje velké množství nej různějších, mnohdy téměř až protichůdných, definic tohoto pojmu. Jednou z příčin tohoto stavu je mj. i to, že pojem kybernetické bezpečnosti se stal tzv. multioborovým fenoménem, který je hojně používán napříč jak technickými, tak i humanitními obory.[2]

Nejčastěji bývá pojem kybernetické bezpečnosti obecně definován jako *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru"*[3] Příkladem praktické aplikace této definice může být definice uvedená v Národní strategii kybernetické bezpečnosti na období let 2015 až 2020, ve které je kybernetická bezpečnost definována jako *„souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost"*[4] *A* Tato definice však vyžaduje vymezení dalšího stěžejního pojmu, kterým je kybernetický prostor, neboli kyberprostor.

Obdobně jako u pojmu kybernetické bezpečnosti, i pojem kyberprostoru (cyberspace) je možné definovat různými způsoby. Nejčastěji používanou definicí kybernetického prostoru, kterou například obsahuje i česká právní úprava kybernetické bezpečnosti, je definice, která kyberprostor vymezuje jako digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací. Setkat se však lze i s definicemi, které kybernetický prostor pojímají více z technického hlediska, přičemž příkladem může být definice, podle které je kybernetický prostor oblastí počítačových sítí včetně uživatelů „za nimi", ve kterých jsou online uloženy, sdíleny a komunikovány informace, přičemž zmíněné počítačové sítě zahrnují jak vlastní počítačové systémy, které data zpracovávají či uchovávají, tak i systém a infrastrukturu, umožňující tok těchto dat.

Kybernetická bezpečnost (CyberSecurity) je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů, tak i sítí. Cílem informační bezpečnosti je ochrana Informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné a produktivní jeho předpokládaným uživatelům.

Pojem kybernetické bezpečnosti bývá často uváděn v souvislosti s informační či počítačovou bezpečností, mnohdy jsou dokonce tyto pojmy zaměňovány či používány jako synonyma. Jedná se však o rozdílné pojmy, které není možné zaměňovat, a to zejména z důvodu odlišného předmětu ochrany. Jak již bylo výše uvedeno, účelem kybernetické bezpečnosti je ochrana tzv. kybernetického prostoru, příp. lze také hovořit o ochraně služeb informační společnosti. Tato ochrana se skládá ze tří základních složek – z ochrany dostupnosti, ochrany integrity a ochrany důvěrnosti. Také informační bezpečnost vychází z této triády, nicméně předmětem ochrany jsou v tomto případě informace, a to nejen ty, které

[2] HARASTA, Jakub. *Právní aspekty kybernetické bezpečnosti ČR*. *Revue pro právo a technologie.* 2013, č. 8, s. 72. ISSN: 1804-5383.

[3] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha : Policejní akademie ČR v Praze : Česká pobočka AFCEA, 2013, s. 57., cit. 2022-04-20, ISBN 978-80-7251- 397-0. Dostupné z: https ://www. govcert.cz/download/aktuality/container-nodeid- 548/slovnikv23 lnbuwebcolor.pdf

[4] NBÚ, *Národní strategie kybernetické bezpečnosti na období let 2015 až 2020* [online]. Národní bezpečnostní úřad – Národní centrum kybernetické bezpečnosti, 2015, s. 5., cit. 2022-04-20. Dostupné z: https://www.ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf

se nacházejí v kybernetickém prostoru, ale také informace v „nedigitální" formě. Jinak řečeno, zatímco předmětem kybernetické bezpečnosti je ochrana dostupnosti, integrity a důvěrnosti kybernetického prostoru, resp. jeho jednotlivých složek, kterými jsou mj. také informační systémy obsahující informace, předmětem ochrany informační bezpečnosti je ochrana dostupnosti, integrity a důvěrnosti samotných informací, bez ohledu na to, kde či v jaké podobě se nacházejí. V tomto smyslu je tedy možné konstatovat, že informační bezpečnost je pojmem širším než bezpečnost kybernetická. Naproti tomu pojem počítačová bezpečnost je v porovnání s kybernetickou bezpečností pojmem užším. Na rozdíl od kybernetické a informační bezpečnosti se navíc jedná o oblast v zásadě toliko technickou. Počítačovou bezpečnost lze definovat jako obor informatiky, který se zabývá zabezpečením informací v počítačích, přičemž zahrnuje zejména zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému, ochranu před neoprávněnou manipulací s daty, ochranu informací před krádeží (nelegální tvorba kopií dat) nebo poškozením, bezpečnou komunikaci a přenos dat (kryptografie), bezpečné uložení dat, dostupnost, celistvost a nepodvrhnutelnost dat.

Kyberbezpečnost je komplexní oblast, která zahrnuje celý soubor teoretických i praktických činností a preventivních aktivit – od právních a zákonných ukotvení přes regulaci, řešení incidentů a hrozeb, kryptografickou ochranu až po vzdělávání, osvětu, výzkum a vývoj atd.

2. KYBERNETICKÉ ÚTOKY

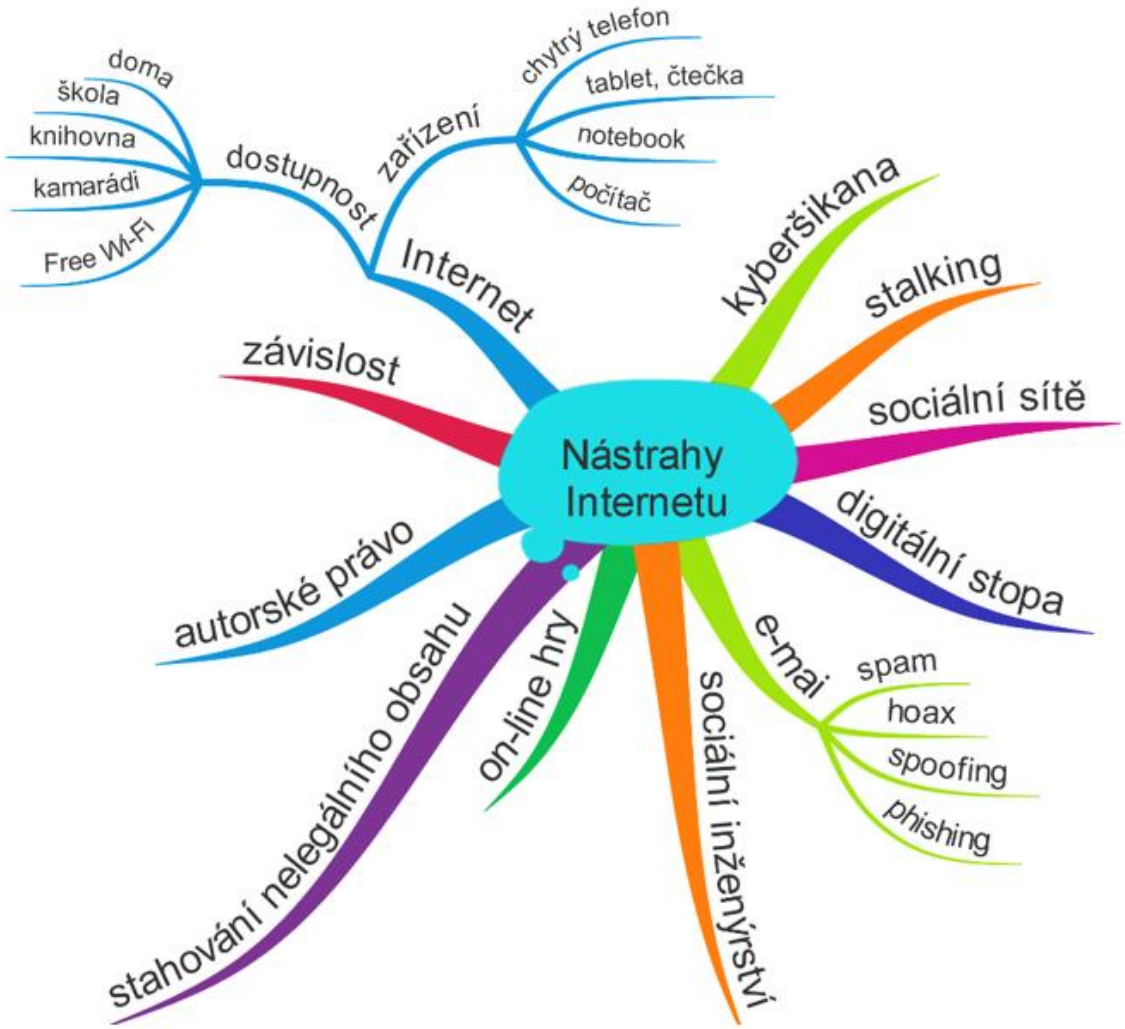
ICT jsou v dnešní době stále více využívány k páchání nejrůznějších podvodných praktik na internetu. Rozmach podvodného jednání na internetu je spojený se dvěma významnými zlomy v „počítačovém světě“. Prvním takovým zlomem byl nástup osobních počítačů a jejich rozšíření mezi veřejnost, druhým pak byl vznik globální sítě Internet, který umožnil vzdálený přístup k počítačům (Smejkal, 2015, s. 133-134). Díky výhodám, které s sebou Internet nese se, mimo jiné stal i útočištěm podvodníků. S výhodou možnosti skrytí identity je spjata minimalizace odhalení pachatele, neomezené množství potencionálních obětí nebo zánik nutnosti přímého kontaktu s obětí.[5]

Podvodníci vystavěli svoji činnost na faktu, že velká část uživatelů neoplývá dostatečným povědomým o tom, jak internet a komunikace na něm funguje a současně využili faktu, že uživatelé ICT slepě důvěřují výstupům a informacím ze svých zařízení. Tato bezmezná důvěra v moderní technologie a informace z internetu se stala živnou půdou pro nejrůznější podvodné praktiky. Mezi takovéto praktiky můžeme zařadit bankovní počítačové podvody zahrnující metody jako: phishing/spear phishing, pharming, skimming, vishing nebo smishing; samotný phishing, což je „podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití“[6]; falešné webové stránky; podvodné e-shopy; falešné inzeráty nebo podvody, které mají charakter sociálního inženýrství.

[5] KOŽÍŠEK, Martin; PÍSECKÝ, Václav. Bezpečně n@ internetu: průvodce chováním ve světě online. 1. Vyd. Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-247-5595-3

[6] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* [online]. 3. Vyd. Praha: Policejní akademie ČR v Praze, 2015, cit. 2022-04-05, 240 s. ISBN 978-80-7251-436-6.

Obr. 1: Nástrahy internetu



Zdroj: Gymnázium Jana Keplera[7]

2.1 Sociální inženýrství

Informační a komunikační technologie se, i přes jejich neustálý a rapidní rozvoj, neobejdou bez zásahu lidské bytosti. K jejich správnému fungování, zprovoznění a údržbě je stále třeba lidské síly. Lidé, v tomto případě uživatelé, vykazují obecně větší míru rizika chybovosti, protože na rozdíl od strojů vstupují do jejich procesu rozhodování lidské city, emoce, stres a další faktory ovlivňující tento proces. Útočníci jsou si těchto nedostatků lidských bytostí vědomi a patřičně jich k realizaci útoků zneužívají.

Sociální inženýrství je technika využívající lidské chybovosti a důvěřivosti s cílem vylákat z oběti citlivá data, přístupové údaje, přístupy k systémům a další podobné důvěrné informace. Důvěra v obětech je často vzbuzována za pomoci falešné identity útočníků, kteří se vydávají za spolupracovníky, administrátory, či pracovníky technické podpory. Samotné útoky sociálního inženýrství mohou být

[7] GYMNÁZIUM JANA KEPLERA, *Bezpečí na internetu*, 2016, cit. 20202-04-16, dostupné na https://gjk.cz/o-skole/skolni-psycholog/bezpeci-na-internetu/

doprovázeny dalšími podvodnými jevy, například donucení oběti k instalaci nebo rozšíření malware či jiného škodlivého kódu.

Stěžejním prvkem k realizaci úspěšného útoku pomocí sociálního inženýrství je komunikace mezi útočníkem a obětí. Na rozdíl od ostatních kybernetických útoků je sociální inženýrství možné realizovat v určitých částech, zejména ve fázi získávání důvěry a přístupových či jiných údajů, mimo kyberprostor. Útočníci tak místo komplikovanějších útoků na specifické prvky v kyberprostoru cílí na reálné osoby – uživatele, kteří jsou z hlediska kybernetické bezpečnosti nejzranitelnějším článkem celé soustavy informačních a komunikačních technologií.

V praxi lze dle autora rozlišovat dva druhy cíle útoku sociálního inženýrství. Prvním cílem je narušit integritu dat, systémů, databází či jejich funkčnosti. V těchto případech se útočníci zaměřují na napáchání co možná největšího množství škod právě narušením integrity zmíněných prvků. Druhým cílem je krádež, kdy útočníci získají přístup k datům, přístupovým údajům, systémům nebo databázím, a následně data, která jsou v těchto prvcích obsažena, odcizí.[8]

⇨⇨⇨ V prostředí vzdělávacích institucí je třeba mít na paměti, že sociální inženýrství může zneužít prakticky kdokoliv z vnitřní struktury. Útočníky mohou být pedagogové, ale také studenti. V některých případech se může jednat o hloupé žerty, nicméně i tyto útoky mohou být nebezpečné. Interní informace by měly zůstat interními. Vyzrazování, byť i pocitově nepodstatných informací mimo vzdělávací instituci může vést k jejich zneužití či uskutečnění jiného kybernetického útoku. Informace, které jsou pro vzdělávací instituci citlivé a kritické, by neměly být zbytečně šířeny mezi uživatele, kteří jejich znalost k výkonu povolání nepotřebují.

Jak poznat sociální inženýrství?

Existuje několik varovných signálů. Podezření by měla vyvolat přílišná naléhavost sdělení, která se snaží donutit příjemce jednat bez rozmyslu, nebo nestandardní žádost o citlivá data. Renomované společnosti nikdy nepožadují hesla ani osobní údaje prostřednictvím e-mailů nebo po telefonu. Se sociálním inženýrstvím se nejčastěji setkáváme v e-mailech.

Níže uvádíme nejčastější varovné signály, které ukazují na sociální inženýrství (zdroj: eset.com):

1. Špatná gramatika a pravopisné chyby.
2. Podezřelá adresa odesílatele.
3. Pocit naléhavosti a nátlaku.
4. Žádost o citlivé informace.
5. Pokud něco zní až příliš dobře na to, aby to byla pravda, pravděpodobně jde o podvod.

Řada dalších kybernetických útoků techniky sociálního inženýrství zneužívá, mezi nejznámější patří phishing a spam.

[8] SOCIAL ENGINEERING HANDBOOK: *How to Take the Right Action* [online]. Bratislava:ESET, c1992 – 2021, cit. 2022-04-20. Dostupné z: https://datasecurityguide.eset.com/storage/download-widget-files/ESET_Data%20Security%20Guide_Social%20Engineering%20Handbook_UK.pdf

2.2 Phishing

Název tohoto útoku je odvozen z anglického fishing – rybaření. Cílem phishingu je získání důvěry oběti, která je následně zneužita k získání citlivých dat, finančních prostředků či přístupových údajů. Formy phishingu jsou různorodé, nejběžněji však mívají povahu e-mailu zaslaného oběti, ve kterém je dále schován odkaz na podvodnou webovou stránku. Tyto podvodné webové stránky pak kopírují, často naprosto přesně, vzhled oficiální webové stránky. Rozpoznat tak podvrh od legitimního e-mailu nebo webové stránky může být pro běžné uživatele často obtížné. Phishingové útoky se často na první pohled tváří jako naprosto legitimní požadavky, například od bankovních institucí, IT oddělení či dalších poskytovatelů služeb, ke kterým je vyžadován přístup pomocí přihlašovacích nebo jiných ověřovacích údajů.[9] Phishing je v dnešní době jedním z nejběžněji používaných kybernetických útoků.

Zamezit situacím, kdy se uživatelé stávají obětí phishingu, lze zejména dostatečnou obezřetností a opatrností. Uživatelé by nikdy neměli otevírat hypertextové odkazy, u kterých neznají původ nebo cíl tohoto odkazu. Odhalit phishingový útok lze často i z pouhého oslovení uvedeného v e-mailové zprávě. Ty často začínají obecnými frázemi, například *„Vážený uživateli“* nebo *„Vážený kliente“*. Problém vyvstává tehdy, kdy je phishingový útok za pomoci sociálního inženýrství upraven přesně pro konkrétní osobu (*tzv. spear-phishing*). Zde již nelze aplikovat obecné pravidlo oslovení z důvodu útočníkovy možné znalosti jména oběti. Vyjma oslovení správným jménem mohou zprávy obsahovat řadu jiných pravdivých informací, které se útočníkovi podařilo získat, například konkrétní jména pracovníků instituce, pracovní pozice, odkazy na legitimní webové stránky instituce a další podobné údaje, které dokáží v oběti vzbudit důvěru. Uživatelé by nikdy neměli otevírat podezřelé odkazy nebo stahovat a otevírat podezřelé soubory, které se v těchto zprávách nacházejí. Vždy, když si uživatel není jist legitimitou, měl by obsah konzultovat s odesílající osobou prostřednictvím jiného komunikačního kanálu pro ověření, zda daná osoba zprávu opravdu odeslala. Pokud není uživatel schopen žádným dostupným způsobem ověřit legitimitu sdělení, je vhodné jej konzultovat s osobou pověřenou řešením kybernetických hrozeb v dané instituci.[10]

[9] What Is Phishing?. *Phishing.org*. Clearwater, Florida, USA: KnowBe4 [cit. 18.12.2021]. Dostupné z: https://www.phishing.org/what-is-phishing
[10] AVAST*, Phishing*. Praha: AVAST, c1988-2022 [cit. 20.4.2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

2.3 Spam

Dalším z řady kybernetických útoků, se kterými se lze v prostředí vzdělávacích institucí setkat, je spam. Toto označení je užíváno pro zprávy, které jsou uživateli zasílány bez jeho souhlasu, obecně se pak označují jako nevyžádaná elektronická pošta. Spam ve své surové podobě nepředstavuje zvýšené bezpečnostní riziko, nebezpečný začíná být ve chvíli, kdy je jeho součástí podezřelá příloha, odkazy vedoucí na neznámé, podvodné a nelegální stránky nebo jiný druh škodlivého kódu. Charakteristické pro spam je pak opakované zasílání stejného sdělení.[11]

V praxi jsou dnes již naprosto běžné filtry spamu, které jsou schopné rozpoznat, zda se jedná o hromadné nevyžádané sdělení a přesunout ho následně do příslušné složky, obvykle označované poskytovateli e-mailových schránek jako *nevyžádaná pošta* nebo *spam.* Tyto filtry však nejsou neomylné a existuje tak šance, že filtr zprávu nedokáže rozpoznat a neprovede její filtraci. Zpráva se pak ocitne mezi doručenou poštou, k čemuž rozesílatelé spamu využívají řadu technik. Mezi ty nejběžnější pak patří využití proxy serverů, které spam rozesílají na základě požadavků a skrývají tak reálnou identitu odesílatele. Spam filtry spam odhalují na základě řady kritérií, mezi které mimo jiné patří IP adresa odesílatele a doména. V případě domény vzdělávací instituce poskytovatelé služeb elektronické pošty často filtrují i příchozí zprávy z jiných domén, často však pouze zobrazením upozornění, že odesílatel zprávu odeslal z účtu mimo doménu.[12]

⇨⇨⇨ Pro vzdělávací instituce může spam i v čistě surové podobě představovat určitou míru nebezpečí, minimálně je pak nutné zhodnotit časové hledisko, kdy velké množství spamu dokáže pracovníky značně zdržovat a obtěžovat při běžné pracovní činnosti. Největší riziko autor pak spatřuje v momentu, kdy je množství spamu neúměrně vysoké, zejména v situacích, kdy je odesílatel spamu schopen zprávy odesílat se shodným obsahem pole příjemce a odesílatele. Uživateli se zpráva zobrazí, jako kdyby ji zaslal sám sobě, a často je tímto způsobem ošálen filtr spamu. Za neméně nebezpečné lze považovat taková nevyžádaná sdělení, která obsahují neznámé odkazy a přílohy. Obsah sdělení, u kterého uživatel nemá znalost původu, je podezřelý či neobvyklý, by neměl být otevírán a zpráva by měla být oznámena osobě odpovědné za řešení podobných incidentů. Na místě je pak všem zaměstnancům ohlásit možný výskyt podobného sdělení a připomenout správné chování v této situaci. Pro instituci je spam vysokým rizikem především proto, že e-mailové adresy většiny vzdělávacích institucí jsou veřejně dostupné. Pro útočníka je tak přípravná fáze – získávání adresátů, značně zjednodušena a může útok cílit plošně na řadu e-mailových schránek. Při nesprávném nastavení nebo nefunkčnosti filtru spamu mohou nastat i situace, kdy dojde k zahlcení schránek.

[11] NIC.CZ, *Buď pánem svého prostoru: Jak chránit sebe a své věci, když jste online* [online]. Praha: CZ.NIC, 2013. [cit. 20.04.2022]. ISBN 978-80-904248-6-9. Dostupné z: https://knihy.nic.cz/files/edice/bud_panem_sveho_prostoru.pdf

[12] SPAMMER-X, POSLUNS, Jeffrey, ed. *Inside the SPAM Cartel: Trade Secrets From The Dark Side*. Rockland, MA: Syngress, c2004. ISBN 1-932266-86-0.

2.3 Hoax

Tzv. hoax je nepravdivá (případně pouze částečně pravdivá) poplašná zpráva, jejímž úkolem je většinou ovlivnit názor či chování ovlivňované osoby.1 Může přitom jít nejen o textovou zprávu, ale i o článek, video, obrázek, řetězovou e-mailovou zprávu. V posledních měsících se hoaxy začaly šířit také formou přeposílaných hlasových zpráv. Hoax má za cíl se co nejvíce rozšířit, proto často apeluje na rozeslání či sdílení. Nejčastějšími tématy hoaxu jsou hrozba před nebezpečím, uniklé „tajné“ informace, zprávy slibující štěstí odměnou za rozeslání, pochybné nabídky práce a další. Některé hoaxy mohou být i neškodné, zábavné. Základem je kriticky přemýšlet o obsahu, který konzumujeme. Zamyslet se obecně nad tím, zda daná informace dává smysl. Hoaxy mají také často některé společné znaky.
Typický hoax:

- Nabádá k dalšímu masivnímu šíření (řetězové přeposílání, sdílení od člověka k člověku).
- Působí na emoce čtenáře (např. strach, vztek).
- Obsahuje překvapivou či odhalující zprávu (nebezpečí, šok).
- Obsahuje gramatické chyby či překlepy.
- Někdy je krkolomně přeložen z jiného jazyka do češtiny (špatný syntax).
- Často je psán CAPS LOCKEM.
- Obsahuje spoustu vykřičníků.

Obr. 2: Ukázka Hoaxu

Zdroj: MÁCA R.[13]

[13] Fake news & 5G na českém internetu, cit. 2022-04-20, dostupné: https://www.politikaspolecnost.cz/wp-content/uploads/2019/11/Fake-news-5G-na-%C4%8Desk%C3%A9m-internetu-IPPS.pdf

Hoaxy mohou být někdy zábavné – často se jedná o vtipy, legrační „řetězovky“, obrázky anebo satirická vyjádření. Mnohem častěji ale bývají hoaxy nebezpečné – často se v nich vyskytují různé nebezpečné rady, zejména v ohledu na zdravotnické informace. V současné době se šíří například hoaxy o prevenci či léčbě Covid-19, které nejsou pravdivé a následováním těchto rad si může uživatel velmi ublížit. Už před výskytem pandemie se také šířilo mnoho hoaxů o domácím, alternativním „léčení“ rakovinových onemocnění. Hoaxy obsahující nebezpečné rady mohou souviset i s jinými tématy, nejen zdravotnickými. Některé z nich nabádají například ke stažení určitých (škodlivých) souborů nebo naopak ke smazání některých souborů (často antivirových) z vlastního počítače.

Dalším typem je falešná prosba o pomoc – může se jednat například o žádost o příspěvek na nemocné děti či zvířata nebo jiné charitativní podpory. Peníze ale ve skutečnosti skončí v kapsách podvodníků. Hoaxy také mohou obsahovat falešné výzvy k placení různých účtů či lživé zpoplatnění používaných aplikací. I v tomto případě může proto dojít i k finanční škodě.6 Hoaxy také někdy obsahují odkazy, pod kterými se může skrývat zavirovaný soubor či podvodná webová stránka.

Dojít tak může k tzv. phishingu (viz výše), kdy uživatel například prozradí falešné webové stránce své přihlašovací údaje nebo dokonce údaje k bankovnímu účtu. Při samotném přeposílání hrozí další rizika. Přeposíláním hoaxů může uživatel prozradit své osobní údaje, které poté mohou být prodávány třetí straně nebo jinak zneužity. Pokud je hoax například posílán jako řetězový e-mail, zpravidla obsahuje v kopii mnoho dalších e-mailů. Pokud se tyto e-maily dostanou třetí straně, může je začít využívat například k marketingovým účelům.

Doporučený postup při obdržení hoaxu

Pokud identifikujeme podezřelou zprávu, je vhodné podstoupit tyto kroky:

- Kriticky se zamyslet nad obsahem zprávy. Nejednat v afektu či bez přemýšlení.
- Ověřit si, zda jsou uvedené informace pravdivé. Na aktuální hoaxy pravidelně upozorňuje například web www.stopfake.org/cz/ či www.fakticke.info. Databáze hoaxů kolujících na internetu od roku 2000 se nachází na webu www.hoax.cz.
- Pokud podezřelá zpráva obsahuje jakýkoliv odkaz, v žádném případě na něj neklikat. Stejně tak nestahovat či neotvírat žádné přiložené soubory.
- Nepřeposílat hoaxy dál.
- V případě neznámého odesílatele kontakt nahlásit či zablokovat.
- V případě veřejného sdílení (například na facebookové timeline, na kanálu YouTube apod.) nahlásit nevhodný obsah.
- Upozornit odesílatele, že se jedná o lživou zprávu.
- Pokud vám pravidelně tyto typy zpráv posílají blízcí či přátelé, je vhodné si s nimi o problematice promluvit a požádat je, aby do budoucna již podobné podvody nerozesílali.

Fakenews:

Termínem fakenews označujeme lživé a nepravdivé zprávy (hoaxy, dezinformace), někdy se termínem fakenews označuje také samotná žurnalistika, která je založena právě na úmyslném šíření těchto nepravdivých informací prostřednictvím masmédií – v posledních letech především sociálních médií (sociálních sítí). Fakenews se „tváří“ jako zprávy pravdivé, jejich cílem je ovlivnit a zmanipulovat příjemce. Někde se rozdíly mezi termínem hoax a fakenews stírají.

2.4 DoS

Název DoS je zkratkou anglického Denial of Service. Volně lze toto spojení přeložit jako odepření služby. Cílem DoS útoků je paralyzovat určitý prvek sítě informačních a komunikačních technologií nebo celou síť. Způsob, kterým je stavu odepření služby docíleno, je zahlcení cíle mnoha požadavky. Cíl, kterým může být například konkrétní server, jeho konkrétní služba, síť nebo její prvky, není schopen tento velký počet požadavků zpracovávat. Důsledkem je pak nedostupnost cíle legitimním uživatelům. V praxi se lze setkat se zkratkou DDoS – Distributed Denial of Service, tedy distribuované odepření služby. Běžně je tento útok veden z řady výpočetních strojů, proto je odhalení a potlačení útoku často velmi složité, až nemožné.[14]

⇨⇨⇨ V případě vzdělávacích institucí lze za potenciální cíl vzít v potaz webové stránky, informační vzdělávací systémy, počítačové sítě v odborných učebnách nebo WiFi sítě, přesněji aktivní prvky sítí. Nutné je však vzít v potaz i DoS útoky vedené uvnitř sítě, kdy infikovaný stroj připojený do lokální sítě infikuje škodlivým kódem ostatní stroje, které následně vedou útok na dostupné služby či servery. Řada vzdělávacích institucí začíná upouštět od běžné evidence v papírové podobě. Například evidence docházky či zápisy hodin se již nezanášejí do papírových třídních knih, nýbrž do elektronických systémů a databází. Tyto databáze jsou běžně provozovány na serveru a jsou zpřístupněny dle kompetencí daným uživatelům vzdělávací instituce. Kompetence se pak liší v závislosti na tom, zda je uživatelem administrátor, pedagog nebo třídní učitel. Náhradou papírových třídních knih se často celý proces evidence značně zjednodušil, urychlil a zpřehlednil, nicméně vyvstala nová rizika plynoucí z digitální povahy těchto evidencí. Servery hostující služby vzdělávacích informačních systémů jsou pak nedílnou součástí běžného provozu instituce a jejich nedostupnost může způsobit značný chaos a řadu nepříjemností spojených s následným doplňováním evidencí. Každý DoS útok je specifický a nelze učinit taková opatření, která by spolehlivě zabránila všem útokům. Nutno také zmínit, že sofistikovaná řešení na ochranu před DoS útoky jsou velmi nákladná a pro vzdělávací instituce finančně často nedostupná.

2.5 Podvodný přístupový bod

Podvodný přístupový bod (z anglického rogue access point) je aktivní prvek, ve formě přístupového bodu nebo routeru, umístěný do sítě bez vědomí vlastníka či správce sítě. Takto umístěný přístupový bod může být potenciálním rizikem pro uživatele, který se k němu připojí a využívá jej pro komunikaci s internetem a zbytkem sítě. V prostředí vzdělávací instituce se lze běžně setkat s přístupovými body, které do sítě bez vědomí administrátora umístí některý ze zaměstnanců, aniž by měl podvodné úmysly. Často tak řeší například slabý signál bezdrátové sítě legitimního přístupového bodu nebo nedostatek portů pro připojení zařízení pomocí kabelu.[15]

Nebezpečí podvodných přístupových bodů spočívá zejména v možné krádeži dat přenášených skrze tento bod. Útočník, který bod do sítě umístil, je schopen data odcizit, sledovat nebo pozměnit. V praxi tento útok využívá dvě metody zachycování dat, aktivní a pasivní. Při pasivním zachycování dat útočník

[14] What is a denial of service attack (DoS)?. Palo Alto Networks [online]. Kalifornie, USA: Palo Alto Networks, c2022, cit. 2022-04-22. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

[15] Rogue access point. *PCMag* [online]. New York, NY: PCMag, c1996-2022, cit. 2022-04-22, dostupné z: https://www.pcmag.com/encyclopedia/term/rogue-access-point

stojí v komunikaci v jejím středu, odposlouchává ji a přenesená data může shromažďovat. Při aktivním zachycování útočník data od odesílatele přijme, pozmění a pak odešle dále v podvržené podobě.

Doplnění:

Kybernetické útoky jsou často prováděny a koncipovány tak, aby zasáhly konkrétní cíl, nicméně je třeba vzít v potaz možnost, že útok napáchá i vedlejší škody nebo zamýšlený cíl mine, tedy situace, kdy se škodlivé účinky útoku projeví mimo původně stanovený cíl. Tento pojem je spjat zejména s využitím kybernetických útoků ve spojitosti s dosahováním národních, mezinárodních a válečných cílů, kdy je diskutována obzvláště morální stránka a poměr mezi výhodou plynoucí z dosažení cíle a způsobenými vedlejšími škodami. V dnešní době je naprosto běžné, že jsou pracovní prostředí mnoha odvětví propojena takovým způsobem, aby bylo možné vyvíjet činnost i mimo lokální síť v zaměstnání. To umožňuje pracovní proces v určitých poměrech zjednodušit, zrychlit, ale také učinit méně bezpečným.

Příkladem vedlejších škod může být malware určený pro kompromitaci a zašifrování databáze či systému vzdělávací instituce, šířený prostřednictvím škodlivého kódu umístěného do odkazu či souboru v e-mailu. Ten je následně zaslán na adresu některého ze zaměstnanců instituce. Šiřitel škodlivého kódu se domnívá, popřípadě spoléhá na to, že adresát škodlivý kód otevře uvnitř lokální sítě instituce nebo na zařízení, jehož součástí je i cílený systém nebo databáze. Může však nastat situace, kdy adresát tento kód z e-mailu spustí mimo lokální síť instituce, například na počítači, který má v místě bydliště a běžně jej mimo osobního využívá také jako pracovní. Škodlivý kód tak může způsobit škody pouze na tomto stroji, který není součástí lokální sítě. Zašifrovaná či kompromitovaná databáze pouze na jediném, v tomto případě osobním stroji je *„zanedbatelná“* škoda oproti situaci, kdy se malware začne šířit uvnitř celé lokální sítě instituce. Za vedlejší škody lze považovat také situace, kdy se škodlivý kód z lokální sítě začne šířit mimo ni.

Až 95 % případů, kdy nastane nějaký „kybernetický problém“ je totiž způsobeno vlastním chováním uživatelů – lidskou chybou.

Nejzávažnější kybernetické hrozby v EU

Kybernetické hrozby v Evropské unii ovlivňují celou řadu odvětví – mnoho z nich navíc platí za životně důležité sektory pro fungování společnosti. Mezi pět sektorů, které jsou postižené nejvíce, patří podle pozorování Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) mezi dubnem 2020 a červencem 2021 veřejná správa/vládní instituce (198 hlášených incidentů), poskytovatelé digitálních služeb (152 incidentů), široká veřejnost (151 incidentů), zdravotnictví/lékařství (143 incidentů) a finance/bankovnictví (97 incidentů).

- **Ransomware**

Druh úmyslného útoku, při kterém pachatelé kybernetické kriminality zašifrují data určité organizace a za obnovení přístupu k nim požadují platbu. Průměrná částka požadovaného výkupného se zdvojnásobila.

- **Malware**

Výraz malware je složeninou anglických slov „malicious“ a „software“ a v překladu znamená škodlivý kód. Malwarem souhrnně označujeme veškeré počítačové viry, červy, trojské koně, botnety, keyloggery, spyware, adware, scareware, ransomware, sniffing a byl vytvořen k tomu, aby poškodil počítačový systém nebo jeho data či „odposlechl“ veškerou online aktivitu poškozeného včetně získání přístupu ke všem heslům. Škodlivý software, jehož účelem je poškodit určité zařízení, narušit jeho fungování nebo k němu získat neoprávněný přístup. Malwarové útoky v EU se snížily o 43 %.

- **Nelegální těžba kryptoměn**

Neoprávněné použití počítačů, chytrých telefonů a tabletů jiných osob ke generování kryptoměn. Kryptoměny jsou i nadále nejčastější platební metodou pachatelů kybernetické kriminality.

- **E-mailové útoky**

Pokusy o podvodné získání hesel nebo údajů z kreditních karet pomocí různých technik, jako je phishing, smishing a spam. Mezi návnadami používanými v hromadných e-mailových útocích dominují i nadále témata související s covidem-19.

- **Narušení ochrany údajů a úniky dat**

Uvolnění citlivých, důvěrných nebo chráněných dat do nedůvěryhodného prostředí. Došlo k nárůstu počtu případů narušení ochrany zdravotních údajů.

- **Útoky distribuovaným odmítnutím služby (DDoS)**

Útoky, které brání uživatelům sítě nebo systému v přístupu k příslušným informacím, službám a dalším zdrojům. Bylo zaznamenáno více než 10 milionů útoků DDoS souvisejících s pandemií covidu-19.

- **Dezinformace**

Úmyslný útok, který spočívá ve vytvoření nebo sdílení nepravdivých nebo zavádějících informací s cílem manipulovat s veřejným míněním.Jedním z hlavních témat dezinformačních útoků je covid-19.

- **Neúmyslné hrozby**

Většinou vyplývají z lidské chyby, mohou být rovněž důsledkem fyzických katastrof spojených s poškozením IT infrastruktury.

- **Hrozby pro dodavatelské řetězce**

Strategie útoku cíleného na určitou organizaci prostřednictvím zranitelných míst v jejím dodavatelském řetězci s potenciálem vyvolat lavinový efekt. 58 % útoků na dodavatelské řetězce má za cíl získat přístup k datům.[16]

[16] Zpráva agentury ENISA o typech ohrožení za rok 2021 (údaje od dubna 2020 do července 2021), cit. 20.04.2022, dostupné na: https://www.consilium.europa.eu/cs/infographics/cyber-threats-eu/

3. JAKOU HROZBU JE POTŘEBA NEOPOMENOUT

3.1 Mobilní nebezpečí

Mobilní zařízení, především ta „chytrá“ jsou v dnešní době digitálních technologií přirozenou součástí života většiny lidí. Výrobci přicházejí na trh se stále promyšlenějšími a technologicky propracovanějšími zařízeními, ať už se jedná o chytré Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy patří mezi nejvyužívanější služby mobilních telefonů posílání SMS zpráv (79,82 %), telefonování (77,21 %), přehrávání hudby (58,04 %), fotoaparát (57,34 %), herní aplikace (56,29 %), videokamera (43,75 %) a webové prohlížení (9,74 %). Za poslední dva roky došlo ke změně preferencí jednotlivých služeb využívaných prostřednictvím mobilních zařízení. Vycházet z tohoto výzkumu můžeme především z pohledu rizik, která jsou s využíváním mobilních zařízení pojená. Jen málo dětí a mladistvých si uvědomuje, že mobilní zařízení všeho druhu jsou poměrně efektivním prostředkem pro páchání kyberkriminality. Jako rizikové můžeme označit využívání Bluetooth technologie, neopatrné využívání Wi-Fi sítí, celkově špatné nebo chybějící zabezpečení mobilních zařízení nebo neopatrné využívání aplikací.

⇨⇨⇨ Možnými následky neopatrného zacházení s mobilními zařízeními mohou být některé výše jmenované sociálně patologické jevy nebo ztráta osobních údajů.

Netolismus: Závislost na digitálním zařízení (telefon, počítač…) nebo na prostředí (internet, soc. sítě).

Vznik netolismu (stejně jako jiných závislostí) je nevědomým procesem a mnoho lidí si vůbec neuvědomuje, že jim v důsledku nadměrného užívání digitálních technologií hrozí nějaké riziko. Při brouzdání či sebeprezentaci na sociálních sítích nemyslí dotyčný člověk v uvedený okamžik na věci, které ho trápí a sužují. Nicméně po ukončení takových aktivit „přesycení“, dochází k poklesu uvolnění a vystřízlivění. Pak se člověk cítí ještě mnohem hůře a osaměleji, než kdyby takovouto aktivitu vůbec nekonal. Žádná návyková látka totiž skutečný problém nevyřeší, jen ho oddaluje a dlouhodobě tak více škodí, než pomáhá. Jedná se o takový závislostní „bludný kruh.“

3.2 Sociální sítě

Přelom 21. století byl pro lidstvo důležitým společenským mezníkem hned z několika pohledů. Jako nejzásadnější pro tuto práci se ukazuje vznik a rozvoj sociálních médií, z nichž nejužívanější jsou sociální sítě. Sociální média změnily podobu společnosti z pohledu sociálních interakcí a komunikace jako

dosud žádný jiný fenomén dnešní doby. V současné době komunikuje prostřednictvím služeb sociálních médií (sociální sítě Facebook, Twitter a LinkedIn) více než jedna miliarda populace. Sociální sítě se staly prostředkem komunikace, seberealizace a sebevyjádření, centrem zábavy, nástrojem pro navazování a udržování nových vztahů, a zvláště pro děti a mladistvé prostředím, kde tráví většinu svého volného času.

Výhody a nevýhody sociálních sítí

VÝHODY

- Možnost propojit se s lidmi z celého světa.
- Jednoduchý a okamžitý způsob komunikace.
- Zdroj zpravodajství.
- Informace jsou přenášeny v reálném čase.
- Sociální sítě jsou zdrojem zábavy.
- Pro žáky a studenty mohou sloužit jako zdroj informací i komunikace, a tím zlepšovat průběh jejich studia.
- Pomáhají lidem, kteří se bojí komunikovat s ostatními na fyzické úrovni nebo jsou jinak izolovaní či znevýhodnění.
- Starším lidem mohou pomáhat zůstat v kontaktu se společností a aktuálním děním.

NEVÝHODY

- Vedou nás ke sdílení nadměrného množství informací.
- Někteří lidé mohou nahrazovat online vztahy za skutečné.
- Mohou působit rušivě a v nejzazších případech negativně narušovat pohodlí našeho života.
- Nadměrné užívání sociálních sítí může narušovat spánek.
- Mohou být prostředím, kde vznikají a rychle se šíří různé nepravdivé a manipulativní zprávy.
- Vytváří více možností, jak neproduktivně trávit volný čas.
- Nijak nebrání vytváření falešných profilů / identit.
- Jsou často prostředím, kde může docházet k různým rizikovým jevům či nevhodnému chování (kyberšikana, kyberstalking apod.).

Na první pohled si můžeme říct, že nástup sociálních sítí přinesl společnosti jen samá pozitiva. Když se však na sociální sítě podíváme z pohledu bezpečnosti, velmi rychle zjistíme, že s velkou spoustou výhod, které sociální sítě bezpochyby mají, se pojí i nezanedbatelné množství rizik a hrozeb, které mohou náš pohyb v tomto téměř idylickém prostředí znepříjemnit. V posledních letech se stále častěji setkáváme s případy trestné činnosti páchané právě prostřednictvím sociálních sítí. Důvodem je především

samotná povaha sociálních sítí, která vychází z otevřenosti tohoto sociálního prostředí a nepřeberného množství možností, které prostřednictvím svých služeb sociální sítě nabízí.

Sociální sítě jsou internetové služby, které registrovaným uživatelům umožňují vytvářet a spravovat soukromé, veřejné, profesní nebo firemní účty, umožňují sdílet obrazový materiál (jako jsou fotografie a videa) a další aktivity uživatele, ale co je asi nejpodstatnější, sociální sítě se staly shromaždištěm a distributorem informací všeho druhu. Kromě A právě možnost šíření a získávání informací prostřednictvím sociálních sítí je jedním z rizik, která jsou v dnešní době nejnebezpečnější, především proto, že se na první pohled jeví jako neškodné nebo dokonce užitečné. O to větší dopad však na náš život mohou mít a je tedy třeba s těmito riziky seznámit zejména ty nejzranitelnější – děti, mladistvé a seniory.

⇨⇨⇨ Mezi nejčastější rizika spojená se sociálními sítěmi patří bezpochyby právě šíření nebezpečného a nevhodného obsahu jako je zakázaná pornografie, extremisticky zaměřené stránky, stránky nabádající k sebepoškozování nebo stránky určené k zesměšňování. Kromě nebezpečného a nevhodného obsahu se můžeme na sociálních sítích setkat i s výše uvedeným závadným chováním (podvody, ovlivnění mravní výchovy mládeže, kyberšikana, sexting, aj.), které můžeme opět rozdělit na nebezpečné a nevhodné, přičemž hranice těchto činů se odvíjí od jejich skutkové podstaty. Mezi další rizika spojená s užíváním sociálních sítí bezpochyby patří zneužití osobních údajů a obsahu (fotografie, videa), krádež identity, trestná činnost spojená s podvody, manipulace, ale i na první pohled neškodná činnost jako je hraní her.[17]

Sociální bubliny a sociální sítě

Sociální (nebo filtrová, názorová, informační) **bublina** popisuje vznik politických, sociálních nebo kulturních rozdílů, které vytváří bariéry mezi různými skupinami společnosti. Často brání přenosu informací z jedné skupiny (bubliny) do druhé. Členové dané bubliny pak mohou mít dojem, že názor jejich bubliny je názorem celé společnosti. Sociální bubliny jsou přirozenou součástí lidských společností a jsou přítomny od nepaměti. Člověk se přirozeně obklopuje lidmi, s nimiž si rozumí – sdílí s nimi názory, hodnoty a postoje. Nástupem internetu a sociálních sítí se však dostala výlučnost sociálních bublin na mnohem vyšší úroveň. Sociální i informační bubliny jsou v současném digitalizovaném světě velmi ovlivněny především tzv. **personalizovaným vyhledáváním**. To funguje tak, že vyhledávací **algoritmy** zobrazují uživateli informace „které chce vidět“ (ty, jenž korespondují s jeho názory). Tyto algoritmy vychází z uživatelova předchozího chování na internetu a mohou ovlivňovat vše – od zpráv, které bude mít zobrazeny na sociálních sítích, přes nabízené reklamy až po to, jací přátelé mu budou na sociálních sítích doporučováni. Podobné techniky jsou využívány řadou sociálních sítí nebo i vyhledávačem Google. Pro člověka je jednodušší hledat si potvrzení svých názorů a začlenění se do stejné skupiny. Internet tento jev jen umocňuje.

Dobrým příkladem, jak se tvoří sociální bubliny, **může být Facebook a jeho „zed‘“** (News feed). Ta slouží k odebírání novinek a příspěvků od přátel, z odebíraných/sledovaných skupin a stránek. Při výběru informací, které se uživateli zobrazí, „zed‘“ vychází mimo jiné z toho, co v minulosti uživatel označil tlačítkem „to se mi líbí“ (like). Podobný obsah potom v budoucnu dostává přednost před jiným zobrazovaným obsahem. Původní snahou je nabídnout uživateli takový obsah, který chce vidět. V

[17] JEDLIČKOVA P., Problematika kybernetické bezpečnosti ve výuce, Diplomová práce, Masarykova univerzita, 2016

konečném důsledku pak ale může docházet k situacím, kdy sociální síť může dávat přednost zobrazení například zábavných videí před upřednostněním důležitých (politických) zpráv. Lidé v sociálních bublinách také používají celou řadu metod, k tomu, aby v bublině nedocházelo k prezentaci odlišných názorů – ať už selekcí diskutujících, jejich napadáním, hromadným odmítáním protinázorů v diskuzích apod. – což vede k dalšímu posilování skupinou sdíleného názoru [18]

Používání internetu a mobilních telefonů je v dnešní době téměř samozřejmostí každého jedince. S nadměrným užíváním zmíněných technologií mohou souviset i určitá rizika. Online prostředí neboli virtuální svět má své neodmyslitelná pozitiva, ale na druhou stranu se zde skrývají nebezpečí, která by neměla být ignorována. Nejčastější rizika, se kterými se můžeme my, resp. naše děti ve virtuálním světě setkat:

- **Kyberšikana.**
- **Zveřejňování osobních údajů na sociálních sítích.**
- **Komunikace s cizím člověkem.**
- **Osobní schůzka s cizím člověkem (domluvený přes sociální sítě)**
- **Fake news**

4. KYBERŠIKANA ZAMĚŘENÁ NA UČITELE: CELOSVĚTOVÝ PROBLÉM

Kyberšikana je specifickým druhem klasické šikany, která je realizována v rámci služeb internetu nebo GDM sítí (mobilní telefony). Mezi nejznámější a nejvíce využívané definice kyberšikany patří definice amerických výzkumníků Hinduji a Patchina, kteří kyberšikanu definují jako záměrnou, opakovanou a zraňující činnost využívající počítač, mobilní telefon a jiné elektronické přístroje. Pod samotnou kyberšikanou se může skrývat řada různorodých projevů, které mohou probíhat samostatně nebo v kombinaci.

Tab. 1: Kyberšikana – kombinace třísložkového komplexu

Použité formy psychické šikany	Formy šikanujícího obsahu	Nástroje pro šíření kyberšikany
• Dehonestování (ponižování, nadávání). • Pomlouvání. • Provokování. • Vyhrožování a zastrašování. • Vydírání. • Obtěžování.	• Text. • Videozáznam. • Audiozáznam. • Grafický záznam (fotografie, karikatura). • Volání, prozvánění. • Krádež identity.	• Veřejné chaty (textové, videochaty), emaily, messengery, ankety, sociální sítě, virtuální vzdělávací prostředí, online hry, SMS, MMS, cloud, webové stránky atd.

Zdroj: SZOTKOWSKI R., KOPECKÝ K., *Kyberšikana a další druhy online agrese zaměřené na učitele*, 2018, Olomouc, cit. 2022-04-10, dostupné na https://www.e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/103-kybersikana-a-dalsi-druhy-online-agrese-zamerene-na-ucitele/file

[18] MARTINEK P., KOSOVA L., *Bezpečně v kyber*, cit.25.4.2022, dostupné na www: https://www.pppuk.cz/soubory/ppp_teplice/bezpecne_v_kyber.pdf

V posledních letech se stále více objevují případy, ve kterých se terčem fyzických či verbálních útoků stávají učitelé všech typů škol. S příchodem nových technologií se agresivní chování zaměřené na pedagogy začalo objevovat také v online prostředí a na tradiční formy šikanování plynule navázaly formy kybernetické – především kyberšikana a další formy online agrese. Oproti tradičním formám šikany, která probíhá „tváří v tvář“, má kyberšikana ze své podstaty mnohem větší dosah, který zhoršuje prožívání oběti. Pokud je oběť (žák, učitel) šikanována ve třídě, svědky pomluv, nadávek, posmívání a ztrapňování je maximálně několik desítek lidí. V prostředí internetu je svědkem (ale i útočníkem) klidně i několik desítek tisíc lidí. Tuto situaci lze demonstrovat např. na videonahrávkách zachycujících učitele ve vyhrocených, emočně vypjatých situacích probíhajících v prostředí školy – žáci tajně či veřejně zachytí jednání učitele prostřednictvím mobilního telefonu a umístí výslednou nahrávku na internet, např. na server YouTube.

Kyberšikana jako taková může probíhat bez přestávek – oběť může být šikanována 24 hodin denně, 7 dní v týdnu. Samotný útok na oběť lze provést v podstatě kdykoli – jak v době školní výuky, tak o přestávkách, mimo školní vyučování, o víkendu, v libovolnou denní či noční dobu. Limitována není ani samotná příprava kyberšikany, pachatel má k dispozici libovolné množství času a může si svůj útok promyslet (např. vytvořit z fotografie dehonestující, urážlivou koláž, kterou bude dále rozšiřovat mezi online uživatele). Protože kyberšikana probíhá zejména v prostředí internetu, útok se šíří daleko rychleji než u běžné šikany.

Mezi nejčastější projevy kyberšikany patří:

- Poškození pověsti učitelé – verbální útoky (ztrapňování, urážení, nadávání, zesměšňování, ponižování…).
- Kyberobtěžování: zastrašování, vyhrožování, vydírání...
- Průnik na účet.
- Krádež identity (zveřejňování ponižujících, intimních fotografií / videí).

Velmi nepříjemnou formu kyberšikany představují útoky s cílem **poškodit pověst učitele** zveřejněním nepravdivých informací, které jsou však natolik citlivé, že mohou vážným způsobem poškodit profesní či soukromý život učitele. Provokování, jehož cílem je vyprovokovat oběť k překvapivé reakci, která je nahrána prostřednictvím mobilního telefonu a sdílena v prostředí internetu, se označuje termínem kyberbaiting (cyberbaiting). Velké množství ponižujících záznamů vzniká přímo v prostředí školy – v době vyučování či o přestávkách. Oběťmi natáčení se nestávají pouze žáci, ale také samotní učitelé.

Kyberobtěžování (cyberharassment) - nejčastěji se jedná o obtěžování pomocí urážlivých nebo výhružných zpráv, doručovaných oběti prostřednictvím SMS, e-mailů, chatu, sociálních sítí a dalších online komunikačních služeb. Cílem obtěžování je především vyvést oběť z rovnováhy a znepříjemňovat jí život. Obtěžování může přerůst až v trestný čin nebezpečné pronásledování (stalking, kyberstalking).

Krádež identity učitele patří k velmi častým formám kybernetických útoků, které využívají jak děti, tak dospělí. Cílem tohoto typu útoku je především proniknout na cizí elektronický účet (emailový účet, účet na sociální síti), převzít identitu původního majitele účtu a zneužít ji k útokům na ostatní uživatele.

Mezi základní možnosti zneužití profilu patří:

1. Jménem majitele útočník publikuje nepravdivé, urážlivé, pomlouvačné informace.
2. Krádeže informací z profilu – např. stáhnutí fotogalerií, kontaktních seznamů apod.
3. Mazání informací z profilu – např. smazání adresáře kontaktů.

4. Zveřejnění soukromých informací, zveřejnění soukromé komunikace.
5. Rozesílání zpráv s nevhodným obsahem jménem majitele účtu – např. zpráv s xenofobním či rasistickým obsahem, zpráv obsahujících dětskou pornografii apod.
6. Zneužití osobních a kontaktních informací z profilu (např. k přihlašování do různých online služeb – seznamek, portálů s pornografickým obsahem, internetových obchodů, aukčních serverů apod.).

Mezi základní způsoby, jak útočník na online profil pronikne, patří:

1. Průnik prostřednictvím slabého hesla (oběť využívá slabé heslo, které je složeno z jednoduché sekvence čísel – např. 12345, nebo obsahuje slova z běžné slovní zásoby – tzv. slovníkové výrazy).
2. Průnik prostřednictvím chybně zvolené kontrolní otázky (oběť má sice silné heslo, ale slabou kontrolní otázku pro vstup na účet, kterou lze snadno zjistit – např. jméno matky za svobodna).
3. Průnik skrz přihlášený účet – majitel účtu se zapomněl odhlásit (např. v rámci počítačové učebny).

Doplnění:

Hodnocení učitelů v online prostředí

Formou útoku, který je na hranici opodstatněné či neopodstatněné kritiky a zároveň kybernetické agrese či přímo kyberšikany, je tzv. hodnocení či známkování učitelů v online prostředí. To je realizováno prostřednictvím různých internetových stránek či serverů, jako jsou například www.oznamkujucitele.cz, www.hodnoceniskol.cz, www.znamkujapp.cz, www.primat.cz či známý anglický portál wwww.ratemyprofessor.com. Princip všech výše uvedených portálů je stejný – umožnit uživatelům (a to v podstatě komukoli) oznámkovat a slovně ohodnotit konkrétní učitele z konkrétních škol. Místo objektivního hodnocení pak v celé řadě případů učitelé zažívají silnou dávku online agrese jak ze strany svých žáků, tak i jejich rodičů. Ponechme teď stranou, zda hodnocení je či není opodstatněné a pravdivé, je minimálně etickým problémem, zda je v pořádku umožnit prostřednictvím nemoderovaných internetových stránek realizovat kyberšikanu zacílenou na konkrétní profesní skupinu a cíleně pak konkrétní osobu profesně poškodit. Proto – jak již bylo řešeno výše, narážíme na právo vyjádřit svobodně svůj názor (např. kritiku) na jedné straně a na pomlouvání a urážení na straně druhé.

Obr. 2: Strategie vyrovnávání se s kyberšikanou (stručný přehled s popisem)

1. **Technická řešení** – oběť využívá k řešení kyberšikany technologické prostředky a nástroje.

Aktivity: Blokace obsahu (blokační tlačítka, nahlášení problému administrátorovi služby), blokování agresora, změna přihlašovacích údajů k účtům (hesla, kontrolní otázky). Změna nastavení soukromí v rámci online profilu. Dočasné vypnutí či přímo smazání profilu. Změna online jména / přezdívky. Smazání či filtrování ubližujících zpráv.

2. **Vyhýbání se a ignorace** – oběť se snaží vyhnout agresorovi a zraňujícímu obsahu (např. jej odstraní), případně se snaží ignorovat situaci a soustředí se na jiné aktivity, omezí stávající aktivity.

Aktivity: Oběť přestane používat sociální sítě, messengery. Oběť situaci ignoruje a neřeší ji. Oběť smaže své internetové stránky a profily. Oběť se vyhýbá agresorovi a omezí či dočasně přeruší využívání mobilního telefonu.

3. **Disociace** – u disociace oběť odděluje „reálný" a „virtuální" svět – virtuální svět vnímá jako něco, co není skutečné. Věří, že se lidé na internetu prostě chovají jinak, než je tomu ve skutečnosti.

Aktivity: Oběť sama sebe přesvědčí, že to, co se děje na internetu v podstatě není reálné, že agresor by se tak ve skutečném světě nezachoval, že to není doopravdy. Oběť bagatelizuje internetovou agresi.

4. **Odplata / konfrontace s agresorem** – při odplatě se uplatňují nejrůznější formy online i offline agrese, dochází k přepínání rolí. Konfrontace s agresorem zahrnuje aktivity, při kterých oběť ve snaze vyřešit kyberšikanu komunikuje s agresorem či agresory – ať již online či offline, ať již veřejně či v soukromí.

Aktivity: Odplata zahrnuje dehonestováni, vydírání a vyhrožování, urážení, sdílení ponižujících materiálů. Dále pak aktivity spojené s převzetím identity pachatele / nově oběti apod. Při konfrontaci oběť se snaží vyjasnit si a vysvětlit situaci s agresorem.

5. **Přerámování** – při přerámování dojde ke změně úhlu pohledu na agresora či samotnou situaci.

Aktivity: Oběť znevažuje či znehodnocuje agresora („nestojí mi za to, je to ubožák, nemá cenu za kvůli němu trápit"). Oběť přesvědčí sebe sama, že situace není tak vážná, jak se jeví.

6. **Vyhledávání podpory** – zahrnuje aktivity, ve kterých oběť do řešení zapojuje další osoby či instituce (např. přátelé, rodiče, kolegy, poradenské linky, policii).

Aktivity: Oběť se svěří s problémem kolegovi učiteli, či řediteli. Nebo anonymně kontaktuje online poradu a jsou i případy, kdy oběť kontaktuje Policii ČR.[19]

4.1 Bezpečná online výuka[20]

Nastavte si jasná pravidla a dbejte na jejich dodržování:

- Pro online výuku zvolte jednotné vzdělávací prostředí (platformu).

[19] SZOTKOWSKI R., KOPECKÝ K., *Kyberšikana a další druhy online agrese zaměřené na učitele*, 2018, Olomouc, cit. 2022-04-10, dostupné na https://www.e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/103-kybersikana-a-dalsi-druhy-online-agrese-zamerene-na-ucitele/file

[20] MARTINEK P., KOSOVA L., *Bezpečně v kyber*, cit.25.4.2022, dostupné na www: https://www.pppuk.cz/soubory/ppp_teplice/bezpecne_v_kyber.pdf

- S žáky komunikujte pravidelně, dejte jim vymezený prostor pro komunikaci, poskytujte jim zpětnou vazbu.
- Nastavte správná oprávnění – oddělte uživatelské role žáků a role pedagogů.
- Do přihlašovacích údajů nepatří jméno a příjmení žáků.
- Používejte bezpečná hesla (12 znaků, speciální znaky, frázová hesla atd.).
- Využívejte funkce předsálí.
- Videohovory lze uzamknout a zamezit tím přístupu nežádoucích osob.
- Chraňte osobní údaje žáků i pedagogů – nesdílejte veřejně záznamy z výuk.
- Využívejte pro zálohování cloud.
- Pozor na citlivé údaje! Na to, kde, jak a s kým je sdílíte!
- Dodržujte základní pravidla bezpečného pohybu na internetu a doporučení MŠMT.

V případně online výuky je velmi užitečné využívat cloudových řešení, která umožňují např. pravidelně zálohovat data spojená s výukou a zajistit jejich obnovu v případě bezpečnostního incidentu (v souvislosti malwarem, ransomwarem apod.). Pozor – do komerčních cloudových řešení NEPATŘÍ citlivé údaje spojené s žáky, např. zprávy z pedagogicko-psychologických poraden či další podobné materiály o dítěti (zdravotní dokumentace, vyšetření apod.).

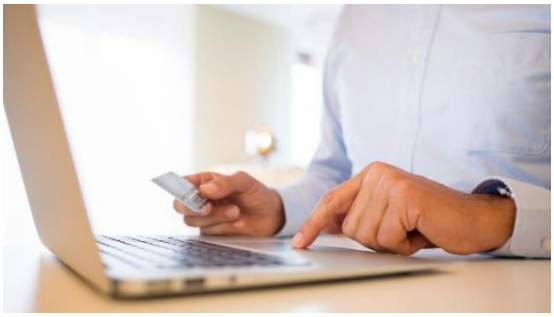
Ochraňte svou výuku

Abyste předešli nabourání online výuky, dodržujte následující pravidla:

- Nesdílejte s žáky přihlašovací údaje do online hodin (např. kód dané hodiny a vstupní heslo), ale žáky přímo do hodiny připojte pomocí jejich uživatelských účtů. Využívejte uzavřené systémy (jednotná vzdělávací prostředí), ve kterých lze snadno spravovat uživatelská oprávnění. Např. definovat, že po přihlášení do hodiny budou mít všichni žáci vypnuté mikrofony, nebudou moci lekci nahrávat, nebudou moci aktivně sdílet obrazovku apod.
- Využívejte funkce předsálí.
- Zamykejte probíhající výuku. Při virtuálním uzavření videochatu učitelem se totiž do hodiny nedostanou další uživatelé, pokud jim to sám učitel nedovolí.
- Používejte rozmazání pozadí (či virtuální pozadí). Minimalizujeme tak riziko, že někdo získá citlivé údaje o domácnosti (pedagogů, žáků, rodičů).

4.2 Osobní údaje a osobnost na internetu

Osobní údaj je jakákoliv informace týkající se fyzické osoby, lze-li ji tak přímo či nepřímo identifikovat (rodné číslo, podoba, e-mailová adresa…). Citlivý údaj je osobní údaj vypovídající např. o národnostním, rasovém nebo etnickém původu, náboženství, zdravotním stavu, sexuálním životě apod. V rámci ochrany osobnosti je chráněna mimo jiné důstojnost člověka, právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.



Základní pravidla pro práci s osobními údaji[21]

Při registracích:

- Přemýšlejte a prověřujte, komu dáváte své údaje k dispozici.
- Zadávejte jen nutné minimum údajů.
- Vytvořte si samostatnou e-mailovou adresu pro registrace do internetových služeb. Vyhnete se tak záplavě reklamních nabídek v e-mailu, který používáte pro běžnou komunikaci.
- Zvažte, zda opravdu chcete dostávat od každého e-shopu jeho reklamní nabídky. Ačkoliv se máte rozhodovat sami, obchodníci vám často tuto volbu „usnadní“ a souhlas zaškrtnou za vás. Nebojte se zaškrtnutí odstranit, pokud informační zprávy dostávat nechcete. Poměrně často totiž zároveň s tímto souhlasem poskytujete obchodníkovi svolení k předání vaší e-mailové adresy dalším osobám.
- Nepoužívejte slabá nebo lehce odhadnutelná hesla. Silné heslo nemusí být nutně složité k zapamatování – například heslo ArelYnekAcha, které vzniklo ze jména Karel Hynek Mácha vynecháním prvních písmen a mezer. Nepoužívejte ani stejné heslo pro všechny služby. Důležité služby jako internetové bankovnictví by měly mít složitostí odpovídající heslo!

Na sociálních sítích:

- Nepřidávejte si mezi přátele neznámé kontakty. Je jednoduché vytvořit falešný profil mladé atraktivní ženy a získat přístup k neveřejným údajům lidí, kteří si takový kontakt přidají mezi své přátele.
- Přemýšlejte nad informacemi, které o sobě zveřejňujete, a nad tím, komu je sdělujete. Víte, kdo jsou přátelé vašich přátel? Co by z nich například vyčetl váš zaměstnavatel? Nezapomeňte na to, že není složité spojit si informace z více zdrojů.
- V žádném případě nezveřejňujte na sociálních sítích informace, jejichž případné zveřejnění by vám vadilo. Ani je nikomu neposílejte. Mějte na paměti, že žádné zabezpečení není dokonalé a k vašim datům se může dostat někdo jiný. Soukromé fotografie pak mohou být zneužity například ke kyberšikaně.

Při prohlížení Internetu:

- Stahování některého obsahu, především pornografie, nelegálních kopií filmů nebo softwaru, přináší riziko napadení vašeho počítače viry. Internetové stránky, které takový obsah nabízejí, jsou záměrně plné virů a jejich návštěvou mnohonásobně zvyšujete riziko napadení svého počítače. U zavirovaného počítače pak nelze žádná data považovat za bezpečná, speciálně vaše osobní.

Doplnění:

Anonymizace

Pokud přistupujete na Internet z počítače na veřejném místě, je využijte anonymních oken, která moderní internetové prohlížeče nabízejí. Všechny informace, které si prohlížeč z vašeho surfování pamatuje, budou totiž po zavření anonymního okna smazány. Nehrozí tak, že by další uživatel stejného

[21] ZACH R., *Ochrana osobních údajů*, 2022, cit. 2022-04-21, dostupné na https://www.jaknainternet.cz/page/1183/ochrana-osobnich-udaju/

počítače viděl historii vámi navštívených stránek, nebo dokonce měl přístup k vašemu e-mailu, když se zapomenete odhlásit.

⇨⇨⇨ **Cookies** neboli sušenky jsou krátké textové soubory vytvářené webovým serverem a ukládané v počítači prostřednictvím vašeho prohlížeče. Když se později vrátíte na stejný web, prohlížeč pošle uloženou cookie zpět a server tak získá všechny informace, které si u vás předtím uložil. Cookies tedy slouží ke sledování statistických dat (např. návštěvnost webu), zvýšení uživatelského komfortu (např. zapamatování vašeho nastavení jazyka nebo doručovací adresy) a personalizace obsahu (např. výsledky vyhledávání klíčových slov, ale také přesnější zacílení reklamy).

Zpracování osobních údajů návštěvníků webových stránek je v rámci Evropské unie upraveno směrnicí o soukromí a elektronických komunikacích, která vyžaduje, aby provozovatelé webových stránek získali od návštěvníků těchto stránek souhlas s využíváním cookies (tzv. princip opt-in). Výjimku představují pouze technické cookies, které jsou nezbytné pro správnou funkci webových stránek.

V českém zákoně však nebyl požadavek na souhlas zcela přesně formulován a provozovatelé webů i odborná veřejnost jej často vykládali jako princip opt-out, tedy „co výslovně neodmítnu, to dostávám“. Schválením novely zákona o elektronických komunikacích jsou s účinností k 1. lednu 2022 odstraněny jakékoli nejasnosti – správci webových stránek mohou shromažďovat osobní údaje návštěvníků těchto stránek pouze na základě jejich prokazatelného souhlasu (princip opt-in).

Pokud navštívíte webovou stránku a žádá vás o přijetí cookies – není to vaše povinnost, webová stránka bude fungovat dál (max. s omezením některých služeb).

Digitální stopa: Každý necháváme v online prostředí svou digitální stopu. Příspěvky a komentáře na sociálních sítích, vlastní fotografie a videa, IP adresy, cookies… Vše, co jednou nahrajete na internet, už na něm navždy zůstane. Dobře si proto rozmyslete, co na něj umístíte, abyste se do budoucna vyhnuli:

- **ztrátě soukromí,**
- **krádeži identity,**
- **manipulaci,**
- **vydírání.**

Digitální stopy nelze smazat, jsou samozřejmou součástí našich kroků na internetu. Přesto je můžeme řídit a minimalizovat. Otázkou, jak na to, se zabývá řada organizací. Jednou z nich je již zmíněná Internet Society. Ta nabízí několik jednoduchých doporučení:

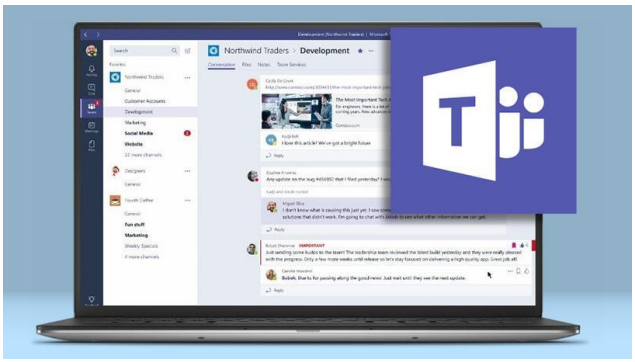
- **Uvědomte si, že každá informace sdílená na internetu představuje riziko pro vaše soukromí. Platí zde jednoduchá zásada: co jednou zveřejníte, už nikdy nevrátíte.**
- **Soukromí je otázka kontextu. Používejte různé účty pro různé účely (mail pro práci a osobní záležitosti, platební kartu pro online a offline platby atp.). Umožní vám to udržet oddělené různé části digitální stopy.**
- **Zkontrolujte si základní nastavení (elektronických zařízení, prohlížečů, aplikací). Ta jsou většinou nastavená veřejně než soukromě. Myslete také na nastavení souborů Cookies.**
- **Používejte rozšíření soukromí zejména pro internetové prohlížeče (např. Abine, TrackMeNot, Ghostery). Umožní nejen snížit vaši digitální stopu, ale také udržet pozornost o tom, kdo vás zrovna sleduje.**

Zajímavost:

Víte o tom, že aplikace Facebook Messenger, WhatsApp, Skype, Zoom či u žáků oblíbený Discord mají věkový limit pro jejich používání na 15 let věku? Bez souhlasu rodičů by je tak neměli žáci mladší 15 let ke komunikaci používat! Proto by se měly využívat zejména takové systémy, které opatření spojená s GDPR dodržují a které poskytují škole jednotné vzdělávací prostředí/platformu s jednotným přístupem ke vzdělávacímu obsahu a komunikaci. V tomto případě je pak vhodnou volbou například používání produktů Google GSuite/Workspace či Microsoft (Teams, Office365/Microsoft365).

Děti, které jsou v dlouhodobé izolaci v důsledku pandemie, jsou často pod velkým tlakem, což může vyústit v jejich frustraci. Tu mohou ventilovat tzv. digitálním zlobením, které není srovnatelné s dlouhodobými rizikovými jevy jako kyberšikana, která je opakovaná, intenzivní a má za cíl ublížit. "Digitální zlobení" je například vkládání různých videí pro pobavení ostatních, jeho cílem není ublížit.

Proto snažte se zlepšovat školní klima – zajímejte se o to, čím a jak žáci žijí a zda se necítí osamělí, podporujte týmovost a zdravý životní styl. Zasmějte se s žáky, oceňte jejich kreativitu a komunikujte pozitivně. Snažte se jejich „digitální zlobení" orientovat na jinou činnost, např. vytvořit logo třídy, nebo koláž z fotek spolužáků, když byli v mateřské škole.



Chraňte se před hackerům[22]

- WI-FI: vždy změňte výchozí hesla na routerech.
- Nainstalujte antivirovou ochranu na všechna zařízení připojená k internetu.
- Zkontrolujte oprávnění vašich aplikací a vymažte vše co nevyužíváte.
- Používejte silná a odlišná hesla k přihlášení do emailu a na sociální sítě.
- Pravidelně zálohujte svá data a provádějte aktualizace.
- Zabezpečte svá elektronická zařízená heslem, PINem, nebo pomocí biometrie.
- Zkontrolujte nastavení ochrany vašeho soukromí na sociálních sítích.
- Buďte pozorní a nikdy:
    - Neodpovídejte na podezřelé zprávy a volání.
    - Neotevírejte odkazy a přílohy z nevyžádaných emailů a textových zpráv.
    - Nesdílejte údaje k vaší platební kartě ani k internetovému bankovnictví.
    - Nesdílejte zprávy z neoficiálních zdrojů.
    - Nevkládejte své fotografie a video na neprověřené servery.
    - Nebuďte přehnaně důvěřiví.
    - Nesdělujte citlivé informace, které by mohly být zneužity (osobní údaje, fotografie, hesla k el. účtům…)
    - Seznamte se s pravidly služeb internetu a GSM sítí.

[22] NUKIB, 2021, cit. 05.04.2022, Dostupné na: https://www.nukib.cz/cs/infoservis/doporuceni/1512-ochrante-svuj-domov-proti-hackerum/

4.3 Mýty, které dělají ze škol snadné cíle

V oblasti zabezpečení IT však koluje řada mýtů, kterým lidé s rozhodovací pravomocí mnohdy věří. Je těžké jednoznačně určit, který bezpečnostní mýtus je nejhorší a způsobuje největší škody. Rozhodně se však nevyplácí spoléhat se na to, že firma je pro útočníky nezajímavý cíl. Stejně tak podceňovat zabezpečení zařízení, která nevnímáme jako napadnutelná přesto, že jsou zapojená do počítačových sítí.

Pro útočníky nejsme zajímavý cíl

Kdybychom sestavovali pomyslný žebříček nebezpečných mýtů v oblasti kybernetické bezpečnosti, jedno z předních míst by určitě obsadilo tvrzení „naše škola je na kyberútok moc malá“. Tahle domněnka je stejně tak rozšířená, jako mylná. Kyberútočníci se o velikost školy nestarají a často převládá vidina možného zisku informací. Pro kyberútočníky může být výhodné napadat školy, jejichž vedení si myslí, že jim za útok nestojí.

Bezpečnost ohlídá antivirový program

Řada organizací se spoléhá na silná hesla a antivirový software. Ačkoliv obojí má svou nepochybnou hodnotu, ani jedno neposkytuje absolutní záruku bezpečnosti. Silná hesla jsou dobrá věc. Při dostatečném úsilí, tedy dostatečném množství strojového času, je ale možné téměř každé heslo prolomit. Obranou je hesla obměňovat, a hlavně používat dvoufaktorovou autentizaci. Znamená to, že se učitel hlásí do vnitřní sítě školy (intranet) ještě pomocí vícefázového ověření.

Zabezpečit je třeba hlavně počítače

Do sítě školy je připojena řada zařízení, která nejsou vnímána jako nebezpečná, a přesto přes ně protékají důležitá data, zajímavá pro útočníky. Typickým příkladem jsou tiskárny.

Bezpečnostní hrozby přichází zvenku

Poslední z rozšířených pověr je představa, že bezpečnostní hrozby přichází odněkud zvenku. Velmi často to tak není. Podstatnou část úniků dat mají na svědomí zaměstnanci. Ať už jde o úmyslnou činnost odcházejícího nespokojeného zaměstnance nebo se jedná o incident způsobený nepozorností, nejzranitelnější článek bezpečnostního řetězce vždycky byl a bude člověk. Vnitřní hrozby je proto potřeba monitorovat stejně jako vnější.[23]

[23] VŠE O PRŮMYSLU, *Kybernetická bezpečnost: mýty, které dělají z obětí snadné cíle*, 2/2022, cit 2022-04-22, Dostupné na: https://www.vseoprumyslu.cz/digitalizace/kyberneticka-bezpecnost/kyberneticka-bezpecnost-myty-ktere-delaji-z-firem-snadne-cile.html

5. SHRNUTÍ: DESATERO, JAK UCHRÁNIT SVŮJ POČÍTAČ

V podstatě neexistuje ucelený návod, jak uchránit svůj počítač (soukromý nebo firemní) od jakékoli infiltrace přicházející z Internetu. Vezmeme-li však v úvahu omezené možnosti šíření počítačových virů, vyvodil jsem několik jednoduchých kroků, jak se těmto a mnohým podobným infiltracím zcela vyhnout.

1. Neotvírat přílohy e-mailů s neočekávaným nebo neznámým typem přiložených souborů, jejichž obsah není přesně znám. Škodlivé programy se často šíří prostřednictvím nevyžádané pošty. Pokud nevíte, od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy.
2. Pozor je nutné si dávat na e-maily, v nichž odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a aktualizovali informace o vašem účtu. Pokud je to možné, tak takovou aktualizaci raději neprovádějte.
3. Nespouštět odkazy na neznámé nebo podezřelé stránky a ani se po těchto webech raději nepohybovat.
4. Při zadávání přístupových hesel na internetových stránkách je nutné vždy zkontrolovat, zda je web zabezpečený. To poznáte například podle ikonky zámečku na liště internetového prohlížeče, nebo tak, že adresa webové stránky začíná zkratkou https, kde „s“ znamená bezpečná.
5. Používat antivirový a ideálně i antispywarový software, který je schopen nejen zastavit již probíhající infekci, ale v případě správné funkčnosti a nastavení rovněž předejít nakažení počítače.
6. Používejte firewall. Ten pomáhá lépe chránit operační systém. Méně zkušení uživatelé by jej rozhodně neměli vypínat. Při nedostatečných znalostech je vhodné jej nechat pracovat v automatickém režimu.
7. Používat vždy nejaktuálnější verzi operačního systému vždy s instalovanými opravnými balíčky. Důležité jsou pravidelné aktualizace celého počítače. Ty je nutné stahovat pro operační systém, bezpečnostní bránu (firewall), antivirus i další programy.
8. V internetových kavárnách a na cizích počítačích se nikdy nepřihlašujte do internetového bankovnictví. V počítači mohou být nainstalován keylogger (jedná se o software, který snímá stisky jednotlivých kláves).
9. Ostražitost je nutná při připojení k nezašifrovaným bezdrátovým sítím (WiFi a GSM). Ty totiž může kdokoliv odposlouchávat a získat tak přístup ke všem datům v cizím počítači.
10. Pravidelně provádějte zálohy svých dat a bezpečně je ukládejte.

⇨⇨⇨ Samostatnou kapitolou jsou **hesla**. Vzhledem ke zvyšujícímu se počtu uživatelských účtů, roste i počet hesel, které tyto účty mají aspoň částečně chránit. Pro uživatele je stále složitější si všechna tato hesla zapamatovat. To je také důvodem, proč si uživatelé hesla píší na lístečky, vkládají si papírky s hesly do peněženek a k dokladům. Přitom prolomení hesla je jednou z nejjednodušších hackerských úloh. Programy, které to umějí, jsou totiž volně ke stažení na Internetu.

Mezi nejhorší hesla v ČR za rok 2021 patří:

1. 123456
2. 12345
3. 123456789
4. Password
5. Qwerty
6. martin
7. heslo
8. 111111
9. 12345678
10. 654321
11. 123223
12. maminka

13. 1234
14. 1234567
15. Machal
16. Milacek
17. Monika
18. Sparta
19. Veronika
20. Slunicko

Zdroj: Klozová M.[24]

Pozn. Prvních 11 hesel se dá prolomit za méně než 1 sekundu.

Tab. 2: Počet všech kombinací hesla a čas na jeho prolomení

Hesla složený ze všech existujících znaků		
Počet znaků	**Počet kombinací**	**Potřebný čas na prolomení**
4	268 435 456	4 minuty
8	72 057 594 037 927 900	91 let
12	19 342 813 113 834 100 100 000 000	24,5 miliardy let

Zdroj: Novinky.cz[25]

Jak je z tabulky patrné, delší hesla složená ze znaků v kombinaci s číslicemi a různými znaky se prolamují pochopitelně hůře. V dobrém hesle by neměly být použité jen běžné znaky. Čím větší množinu znaků v hesle použijete, tím je složitější heslo prolomit. K dispozici máte 10 číslic, 26 základních písmen abecedy (a-z), které můžete zdvojnásobit použitím velkých a malých písmen a nakonec i interpunkční znaménka (. , : ; - ? ! ...) a spoustu speciálních znaků (@ # & $ ^ _ * ...). Dohromady tedy máte k dispozici přes 80 znaků relativně snadno použitelných na běžné klávesnici. Nezapomínejte však, že na internetu některé servery nepodporují použití určitých speciálních znaků (např. $, &, \, /, ', <, >, ", , ˇ) z bezpečnostních důvodů.

Desatero bezpečnosti u hesel[26]:

1. Nikomu nesvěřovat své přístupové údaje (hesla).
2. Používat silná a různá hesla pro různé typy služeb, po kompromitaci nebo jednou za čas je měnit, používat správce hesel.
3. Odhlašovat se ze svého účtu po každém použití veřejného počítače.
4. Odhlašovat se z účtů na webových službách (i na mobilních zařízeních).
5. Zabezpečovat soukromí na osobních účtech u webových služeb (sociální sítě).
6. Vypnout automatické přihlašování a vyplňování osobních údajů ve webovém prohlížeči.
7. Dávat si pozor na podezřelé zprávy a e-maily (zejména pokud vyžadují mou interakci - např. zaslání peněz, a to i od kamaráda!).
8. Ověřovat si informace u jejich poskytovatelů přímo (podívat se na web, zavolat do banky apod.).
9. Používat kvalitní antivirový program (i na mobilních zařízeních).
10. Pravidelně aktualizovat antivirový program a operační systém zařízení.

A PŘEDEVŠÍM: POUŽÍVAT ZDRAVÝ SELSKÝ ROZUM

[24] KLOZOVÁ M., *Internetem bezpečně*, 2022, cit. 2022-04-19, dostupné na https://www.internetembezpecne.cz/nejhorsi-hesla-roku-2021/

[25] NOVINKY.CZ, Nejhloupější hesla, která lidé používají na internetu. [online] [cit. 2012-04-20]. Dostupné z WWW: http://www.novinky.cz/internet-apc/250913-nejhloupejsi-hesla-ktera-lide-pouzivaji-na-internetu.html

[26] KRAJE PRO BEZPEČNÝ INTERNET, *Bezpečnost na internetu (pro pedagogy)*, 2022, cit 2022-04-20, dostupné: https://elearning.ecrime.cz/mod/scorm/player.php?a=53&currentorg=CourseID-org&scoid=108&sesskey=xB7cxCEyBL&display=popup&mode=normal

6. SLOVNÍČEK: ZÁKLADNÍ TERMINOLOGIE KYBER. BEZPEČNOSTI[27]

- **Adware (Advertising Supported Software)** – jedná se o softwarový produkt znepříjemňující práci s počítačem vnucenou nevyžádanou reklamou. Cílem je předání reklamního sdělení většinou proti vůli uživatele systému. Typickým příznakem jsou vyskakující reklamní okna během surfování na Internetu. Většinou není přímo pro uživatele nebezpečný.
- **Aktivní hrozba (Active Threat)** - jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti dat. Následkem toho může dojít k modifikaci zpráv, vložení falešných zpráv, odmítnutí služby nebo vydávání se za někoho jiného.
- **Analýza hrozeb (Threat Analysis)** - zkoumá činnosti a události, které by mohly negativně ovlivnit kvalitu služby informačních technologií nebo samotná data.
- **Analýza zranitelnosti (Vulnerability Analysis)** - systematické analyzování systému a provozovaných služeb vzhledem k bezpečnostním slabinám systému. Analyzují se také bezpečnostní opatření.
- **Analýza počítačového viru (Virus Analysis)** – jedná se o soubor činností zahrnující ucelený rozbor chování počítačového viru (šíření, skrývání, způsobené škody), zkoumání kódu viru a jeho následné odstranění.
- **Antivirový program (Antivirus Program)** - program pro vyhledávání počítačových virů, léčení napadených souborů, zálohování a obnovu systémových oblastí na disku, ukládání kontrolních informací o souborech na disku.
- **Bezpečnost informací (Information Security)** - zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností informací (např. autentičnosti, odpovědnosti, nepopíratelnosti a spolehlivosti). Uplatnění obecných bezpečnostních opatření a postupů k ochraně informací před jejich ztrátou nebo kompromitací.
- **Bezpečnostní manažer (Security Manager)** – zaměstnanec organizace nebo firmy odpovědný za bezpečnost systému. Má jasně definované odpovědnosti a pravomoce.
- **Bot** – jedná se o parazitní program, který je bez vědomí uživatele nainstalován na jeho počítači. Umožňuje neautorizovanému uživateli (hackerovi) vzdáleně tento počítač ovládat a využívat ho pro plnění různých příkazů.
- **Brána (Gateway)** – je název pro místo vstupu do informačního systému, které je většinou vybaveno zvláštními bezpečnostními prvky (např. firewallem, autentizací přístupu, šifrováním vstupů a výstupů).
- **CCD COE (Cooperative Cyber Defence Centre of Excellence)** – NATO, středisko pro spolupráci v kybernetické obraně (sídlo: Tallinn, Estonsko, http://www.ccdcoe.org).
- **CERT (Computer Emergency Response Team)** – představuje tým bezpečnostních specialistů pro okamžitou reakci na počítačové incidenty. Tato střediska již existují ve většině vyspělých států světa.
- **Certifikace (Certification)** - proces ověřování způsobilosti informačního systému k nakládání s utajovanými informacemi, schválení této způsobilosti a vydání certifikátu. Celý proces provádí třetí strana.
- **CIRC (Computer Incident Response Capability)** – schopnost rychlé a efektivní reakce na rizika, zranitelnosti v systémech a na počítačové incidenty.

[27] Ing. Petr HRŮZA, Ph.D., *Kybernetická bezpečnost*, Brno, 2021

- **CSIRT (Computer Security Incident Response Team)** – odborný tým osob zabývající se prevencí a řešením bezpečnostních incidentů vzniklých v informačních systémech a počítačových sítích.
- **Cyberstalking** – jedná se o nejrůznější druhy stopování a obtěžování s využitím elektronického média (zejména prostřednictvím elektronické pošty), jejichž cílem je například vzbudit v oběti pocit strachu. Informace o oběti pachatel nejčastěji získává z webových stránek, fór nebo chatovacích místností („chat" je způsob on-line komunikace více osob prostřednictvím Internetu).
- **Červ (Worm)** - jedná se o samostatný program schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů či sítí. Zde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží k vyhledávání bezpečnostních skulin v systémech nebo v poštovních programech.
- **DDoS Distribuované odmítnutí služby (Distributed Denial of Service)** – jedná se o druh útoku na internetové služby nebo stránky, při němž dochází k přehlcení požadavků a pádu nebo minimálně nefunkčnosti a nedostupnosti služby pro ostatní uživatele. Útok je veden z několika počítačů najednou (v jednom časovém intervalu).
- **Důvěrnost (Confidentiality)** – jedná se o stav, kdy informace není dostupná neoprávněným uživatelům nebo není odhalena neautorizovaným přístupem.
- **Hacking** – neoprávněný průnik do informačního systému, provedený zvnějšku (zpravidla ze vzdáleného počítače). Samotný průnik je podmínkou pro další neautorizovanou činnost v rámci cílového systému. Pachatel se zpravidla nepřipojuje k objektu útoku (počítači) přímo, ale přes jeden či více internetových serverů v různých částech světa. Cílem takového postupu je podstatné snížení možnosti identifikace skutečného umístění počítače, ze kterého byl útok primárně veden.
- **Integrita (Integrity)** - zajištění správnosti, celistvosti a úplnosti informací.
- **Kybernetická bezpečnost (Cyber Security)** – souhrn právních, organizačních, technických a fyzických opatření, která umožňují odolávat úmyslně i neúmyslně vyvolaným kybernetickým útokům a zmírňovat či napravovat jejich následky. Nejčastěji se dává do souvislosti s finančně, politicky či vojensky motivovanými útoky. Důležitým aspektem kybernetické bezpečnosti je ochrana před krádeží identity.
- **Kybernetický prostor (Cyber Space)** – lze ho vnímat jako digitální prostředí tvořené informačními a komunikačními technologiemi, ve kterých informace vznikají, jsou zpracovávány a dochází k jejich výměně. Kybernetický prostor lze také chápat jako metaforu vyjádření virtuálního (nefyzického) prostředí vytvořeného propojením počítačových systémů v síti. V kybernetickém prostoru probíhá vzájemné působení mezi subjekty stejně jako v reálném světě, ovšem bez nutnosti fyzické aktivity.
- **Kybernetický terorismus (Cyber Terrorist)** – nezákonný útok proti počítačům, počítačovým sítím a v nich uloženým informacím, při kterém je záměrem útočníka získat informace, negativně je ovlivnit nebo převzít kontrolu nad prvky infrastruktury systému
- **Management rizik (Risk Management)** – chápeme jako činnost sloužící k řízení a kontrole organizace s ohledem na rizika. Je nedílnou součástí systematického řízení organizace. Jeho cílem je analyzovat současná i budoucí rizika a vhodnými opatřeními zmenšovat pravděpodobnost výskytu a závažnost jejich možných nežádoucích následků
- **Malware (Škodlivý software)** – tímto pojmem se označuje jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány nebo mohou reagovat na konkrétní naprogramovanou spouštěcí událost (např. na okamžik, kdy oprávněný uživatel otevře zprávu v rámci elektronické pošty).
- **Narušení (Breach)** – situace, kdy došlo k narušení nebo spíše k prolomení důvěrnosti, integrity nebo dostupnosti informačního systému v důsledku překonání bezpečnostních opatření.

- **Nevyžádaná pošta (Spam)** - masové šíření nevyžádaného sdělení. V nejčastějším případě se jedná o reklamu nejrůznějšího charakteru. Není-li systém dostatečně zabezpečen, může nevyžádaná pošta tvořit značnou část elektronické korespondence.
- **Ohrožení (Exposure)** – dá se vysvětlit jako skutečnost existence zranitelnosti, která může být zneužita hrozbou.
- **Opatření / Protiopatření (Countermeasure)** – činnost na úrovni fyzické, logické nebo administrativní bezpečnosti, která snižuje zranitelnost a chrání systém před danou hrozbou.
- **Phishing** – metoda usilující o zcizení digitální identity uživatele (například jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů) za účelem jejího následného zneužití. Jedná se většinou o vytvoření podvodné zprávy, šířené elektronickou poštou. V této zprávě se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce limitovaly důvěryhodného odesílatele (například banku).
- **Riziko (Risk)** – jedná se o pravděpodobnost, že hrozba zneužije zranitelnost systému a způsobí narušení jeho důvěrnosti, integrity nebo dostupnosti.
- **Spyware** – je program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele. Skrytě monitoruje chování oprávněného uživatele počítače nebo systému. Zjištěné informace průběžně zasílá určenému uživateli, který tyto informace dále zpracovává. Spyware představuje z hlediska bezpečnosti dat velkou hrozbu, protože odesílá různé informace z počítače bez vědomí uživatele.
- **Trojský kůň (Trojan Horse)** - jedná se o program implantovaný do informačního systému bez vědomí oprávněného uživatele, který monitoruje specifické činnosti, o které projevuje útočník zájem. Jedná se například o znaky, které oprávněný uživatel stiskl na klávesnici (zejména hesla) nebo stránky, které navštívil. Tyto údaje předává útočníkovi k dalšímu zpracování. Ten tak může získat přístupové informace k navštíveným webovým stránkám, bankovním účtům nebo kontům elektronické pošty.
- **Útok (Attack)** - je pokus o zničení, vystavení hrozbě, změně, vyřazení z činnosti, zcizení nebo získání neautorizovaného přístupu do počítače nebo počítačových sítí.
- **Vir (Virus)** - parazitující škodlivý kód, který se připojí k určitým programům nebo systémovým oblastem a pozmění je. Může se nekontrolovatelně rozšiřovat nebo po svém spuštění zahájit destrukční procesy (poškození, změnu či zničení dat, degradaci funkce operačního systému, stahování dalšího malware atd.)
- **Warez** – výroba a rozšiřování pirátského software.
- **Zadní vrátka (Backdoors)** – jsou to skryté kódy, které po instalaci na cílový počítač umožňují jeho vzdálené řízení.
- **Zranitelnost (Vulnerability)** - vlastnost nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou.

CVIČNÝ TEST[28]

1) Co je kyberšikana?
a) Jakékoliv agresivní chování v kyberprostoru
b) Narušování online výuky
c) Vzájemná vulgární internetová komunikace mezi žáky
d) Dlouhodobé, opakované ubližující jednání s negativním dopadem na oběť

2) S jakým typem kybernetické agrese se učitelé nejčastěji setkávají?
a) Založení falešného profilu na sociálních sítích
b) Šíření ponižující či ztrapňující zvukové nahrávky
c) Verbální útoky (ponižování, urážení apod.) po internetu
d) Vydírání prostřednictvím internetu či telefonu

3) Které z následujících projevů netolismu můžeme zařadit mezi tzv. psychologické projevy?
a) Zvyšování nadváhy
b) Snižování fyzické aktivity
c) Narušení vztahů s rodinou a přáteli
d) Stres, úzkostné stavy a deprese

4) Co označuje pojem nomofobie?
a) Strach ze ztráty mobilního zařízení nebo některé z jeho funkcí (signál, vybití baterie apod.)
b) Virtuální měna, kterou může hráč získat za strašení ostatních hráčů v online hře
c) Strach z nedostatku přístupu k novým informacím
d) Úzkostné stavy při zmínce o pornografii

5) Kdo je nejčastějším pachatelem (kyber)stalkingu?
a) Spolužák nebo spolužačka
b) Bývalý partner nebo bývalá partnerka
c) Online známost
d) Kolega nebo kolegyně z práce

6) „Kyberbaiting" znamená:
a) Vyhrožování a zastrašování učitele
b) Krádež identity učitele
c) Vytváření falešných profilů učitele
d) Vyprovokování učitele a natočení jeho reakce

7) Vyberte pravdivé tvrzení o netolismu (závislostech):
a) Člověk může být závislý pouze na počítačových hrách
b) Člověk může být závislí pouze na virtuálním prostředí ale ne na zřízení jako takovém

[28] MARTINEK P., KOSOVA L., *Bezpečně v kyber*, cit.25.4.2022, dostupné na www: https://www.pppuk.cz/soubory/ppp_teplice/bezpecne_v_kyber.pdf

c) Člověk může být závislý jak na virtuálním prostředí, tak na zařízení jako takovém

8) Co označuje výraz „Ana“?
a) Nástroj pro online výuku
b) Populární online hru
c) Výraz pro využívání anonymity na internetu
d) Zkrácený výraz pro mentální anorexii

9) Co označuje zkratka MMORPG?
a) Hru na hrdiny pro velký počet hráčů
b) Hru vyžadující po hráči pravidelné měsíční poplatky
c) Zkratku pro jednu z poruch příjmu potravy
d) Jakoukoliv online hru

10) Jaká je nejpopulárnější sociální síť na světě?
a) Instagram
b) Twitter
c) Facebook
d) TikTok

Správné odpovědi:
1 – d; 2 – c; 3 – d; 4 – a; 5 – b; 6 – d; 7 – c; 8 – d; 9 – a; 10 – c

POUŽITÉ ZDROJE

- AVAST, *Phishing*. Praha: AVAST, c1988-2022 [cit. 20.4.2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing
- ESET, SOCIAL ENGINEERING HANDBOOK: *How to Take the Right Action* [online]. Bratislava: ESET, c1992 – 2021, cit. 2022-04-20. Dostupné z: https://datasecurityguide.eset.com/storage/download-widget-files/ESET_Data%20Security%20Guide_Social%20Engineering%20Handbook_UK.pdf
- GEERS, Kenneth. *Strategie Cyber Security* [online]. Tallinn: CCD COE Publication, 2011, s. 9. [cit. 23. 12. 2018]. ISBN 978-9949-9040-7-5 (pdf). Dostupné z: http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF
- GYMNÁZIUM JANA KEPLERA, *Bezpečí na internetu*, 2016, cit. 20202-04-16, dostupné na https://gjk.cz/o-skole/skolni-psycholog/bezpeci-na-internetu/
- HARASTA, Jakub. *Právní aspekty kybernetické bezpečnosti ČR*. *Revue pro právo a technologie.* 2013, č. 8, s. 72. ISSN: 1804-5383.
- HRŮZA, P., *Kybernetická bezpečnost*, Brno, 2021, Univerzita obrany, 2012, 90 s. ISBN 978-80-7231-914-5

- JEDLIČKOVA P., *Problematika kybernetické bezpečnosti ve výuce*, Diplomová práce, Masarykova univerzita, 2016
- JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Policejní akademie ČR v Praze : Česká pobočka AFCEA, 2013, s. 57., cit. 2022-04-20, ISBN 978-80-7251-397-0. Dostupné z: https ://www. govcert.cz/download/aktuality/container-nodeid- 548/slovnikv23 lnbuwebcolor.pdf
- JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* [online]. 3. Vyd. Praha: Policejní akademie ČR v Praze, 2015, cit. 2022-04-05, 240 s. ISBN 978-80-7251-436-6.
- KOŽÍŠEK, Martin; PÍSECKÝ, Václav. Bezpečně n@ internetu: průvodce chováním ve světě online. 1. Vyd. Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-247-5595-3
- MARTINEK P., KOSOVA L., *Bezpečně v kyber*, cit.25.4.2022, dostupné na www: https://www.pppuk.cz/soubory/ppp_teplice/bezpecne_v_kyber.pdf
- NIC.CZ, *Buď pánem svého prostoru: Jak chránit sebe a své věci, když jste online* [online]. Praha: CZ.NIC, 2013. [cit. 20.04.2022]. ISBN 978-80-904248-6-9. Dostupné z: https://knihy.nic.cz/files/edice/bud_panem_sveho_prostoru.pdf
- NBÚ, *Národní strategie kybernetické bezpečnosti na období let 2015 až 2020* [online]. Národní bezpečnostní úřad – Národní centrum kybernetické bezpečnosti, 2015, s. 5., cit. 2022-04-20. Dostupné z: https://www.ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf
- NUKIB, 2021, cit. 05.04.2022, Dostupné na: https://www.nukib.cz/cs/infoservis/doporuceni/1512-ochrante-svuj-domov-proti-hackerum/
- Rogue access point. *PCMag* [online]. New York, NY: PCMag, c1996-2022, cit. 2022-04-22, dostupné z: https://www.pcmag.com/encyclopedia/term/rogue-access-point
- SPAMMER-X, POSLUNS, Jeffrey, ed. *Inside the SPAM Cartel: Trade Secrets From The Dark Side*. Rockland, MA: Syngress, c2004. ISBN 1-932266-86-0
- SZOTKOWSKI R., KOPECKÝ K., *Kyberšikana a další druhy online agrese zaměřené na učitele*, 2018, Olomouc, cit. 2022-04-10, dostupné na https://www.e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/103-kybersikana-a-dalsi-druhy-online-agrese-zamerene-na-ucitele/file
- VŠE O PRŮMYSLU, *Kybernetická bezpečnost: mýty, které dělají z obětí snadné cíle*, 2/2022, cit 2022-04-22, Dostupné na: https://www.vseoprumyslu.cz/digitalizace/kyberneticka-bezpecnost/kyberneticka-bezpecnost-myty-ktere-delaji-z-firem-snadne-cile.html
- What Is Phishing?. *Phishing.org*. Clearwater, Florida, USA: KnowBe4 [cit. 18.12.2021]. Dostupné z: https://www.phishing.org/what-is-phishing
- What is a denial of service attack (DoS)?. Palo Alto Networks [online]. Kalifornie, USA: Palo Alto Networks, c2022, cit. 2022-04-22. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
- ZACH R., *Ochrana osobních údajů*, 2022, cit. 2022-04-21, dostupné na https://www.jaknainternet.cz/page/1183/ochrana-osobnich-udaju/