VNÍMÁNÍ VZDĚLÁVÁNÍ V TÉMATU SOCIÁLNÍHO INŽENÝRSTVÍ VE SPOLEČNOSTI AVAST

Bc. Šarlota Balážová; balazova.sar@gmail.com; (Fakulta informatiky a statistiky, Vysoká škola ekonomická v Praze)

Článek vychází z bakalářské práce s názvem Vnímání vzdělávání v tématu sociálního inženýrství ve společnosti Avast, jejíž cílem je popsat a základně analyzovat problematiku sociálního inženýrství a postoj k ní ve společnosti Avast, v souvislosti s edukací veřejnosti. Článek se věnuje sociálnímu inženýrství a častým podvodným praktikám, jakožto i jeho vývoji v souvislosti s pandemií Covid-19. Zaměřuje se pak na význam edukace veřejnosti v oblasti sociálního inženýrství a podrobněji rozebírá ohrožené věkové skupiny a edukaci na toto téma ve školství. Z případové studie společnosti Avast Software se zabývá jejím postojem ke vzdělávání veřejnosti v oblasti sociálního inženýrství a rozebírá její jednotlivé iniciativy v tomto směru, tedy internetové blogy, interaktivní webovou hru Avast Phishing Game a zejména pak největší vzdělávací projekt Nadace Avast – Buď safe online. Volně dostupné informace a data k případové studii jsou doplněné dvěma rozhovory se zaměstnanci společnosti Avast, kteří mají vzdělávací projekty na starost.

http://doi.org/10.52036/1335793X.2022.1-2.39-50

Sociální inženýrství je v dnešním digitálním světě stále se rozvíjející téma. Metody sociálních inženýrů jsou čím dál sofistikovanější a je čím dál náročnější je rozpoznat, zejména pro zranitelné skupiny uživatelů internetu jako jsou děti nebo senioři. Je tedy zásadní snažit se o osvětu a vzdělávání nejen těchto skupin, ale i celé společnosti tak, aby se počet úspěšných útoků a peněžních ztrát z nich plynoucích dařilo minimalizovat.

Přesvědčovací metody, které sociální inženýři využívají pro konstrukci svých podvodů se dají různě kombinovat a jednotlivé podvody optimalizovat tak, aby byl jejich výnos pro sociální inženýry co největší. Z jejich snah pak vychází série nejčastěji využívaných podvodných praktik, jejichž základní principy fungují již dlouhodobě a sociální inženýři je postupně pouze upravují dle svých aktuálních potřeb a inovují s příchodem nových technologií a společenských témat. Jedním z těchto témat, které nelze opomenout je pandemie Covid-19, která také dala vzniknout novým obměnám známých podvodných praktik.

Tato pandemie nejen nabídla sociálním inženýrům nové náměty pro podvody, ale významně zrychlila posun dnešní společnosti do digitálního světa a jen zdůraznila potřebu plošného vzdělávání lidí na téma nejen sociálního inženýrství, ale především i bezpečnosti na internetu obecně. Svůj podíl na této vzdělávací činnosti v ČR i ve světě má i antivirová společnost Avast Software, na kterou se tento článek blíže zaměřuje.

Článek se nejprve rámcově zabývá charakteristikou sociálního inženýrství a jeho běžnými podvodnými praktikami, a pak i sociálním inženýrstvím v souvislosti s Covid-19, významem edukace veřejnosti ohledně technik sociálního inženýrství a věkovým složením jeho obětí. Nakonec rozebírá blíže postoj společnosti Avast k tématu sociálního inženýrství a její techniky edukace veřejnosti.

Pro detailnější nahlédnutí do aktivit společnosti Avast na poli vzdělávání v tématu sociálního inženýrství a bezpečnosti na internetu jsou jedněmi ze zdrojů článku také rozhovory vedené se dvěma zaměstnanci společnosti, kteří se v jejím rámci zabývají vzdělávacími projekty.

POJEM SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství nebo také sociotechnika bere způsoby, jakými lidé dělají svá rozhodnutí a využívá jejich zranitelnosti. Je to jakákoliv aktivita, která ovlivňuje člověka, aby udělal něco, co není v jeho zájmu a cílem sociálního inženýra je, abyste se rozhodli bez přemýšlení (Hadnagy, 2018, s. 4 – 7).

Jakobsson (2016, s. 29) v rámci zkoumání důvodů, proč se lidé nechávají zmanipulovat sociální inženýrství definuje jako umění využívat sociální dovednosti a přesvědčovací techniky za účelem zisku informací, ke kterým nemáme autorizovaný přístup.

Sociální inženýrství je tedy nástrojem k páchání zločinů nejen v kyberprostoru, ale i ve fyzickém světě. Často

se tak můžeme setkat i s útoky, které využívají kombinaci obou. Hlavním nástrojem pro ochranu před útoky sociálních inženýrů je přitom informovanost široké veřejnosti o různých technikách podvodů a na co si dávat při běžném životě a pohybu na internetu pozor.

BĚŽNÉ PODVODNÉ PRAKTIKY

Sociální inženýrství dnes funguje především online, a to ve většině případů prostřednictvím emailové komunikace. Nevyžádané emaily dělíme na tři kategorie: spam (nevyžádané obchodní nabídky), Trojský kůň (email obsahuje škodlivý software) a emailové podvody, tedy scam (cílem emailu je krádež) (Jakobssen, 2016, s. 52). V rámci emailových podvodů se nemusí vždy jednat přímo o krádež peněz nebo majetku, často jde o krádež citlivých dat, která pak útočník dále využívá pro svůj prospěch.

Mezi emailovými podvody pak vynikají různá schémata, která útočníci využívají nejčastěji, protože mají vysokou úspěšnost. Dnes se jedná především o Business Email Compromise, advanced fee scam (podvod dopřednou platbou), tech support fraud (podvod s technickou podporou) a honeytrap. Všechny tyto podvody využívají techniky sociálního inženýrství, často právě jejich kombinace a můžeme se setkat i s kombinací fyzických a virtuálních technik, ale v celkovém objemu podvodů je to zanedbatelné množství.

SOCIÁLNÍ INŽENÝRSTVÍ A COVID-19

Americké IC3 evidovalo za rok 2020 více než 28,5 tis. nahlášených internetových podvodů souvisejících s Covid-19 (IC3, 2021). Útočníci využívali zranitelnost jednotlivců a drobných podnikatelů v souvislosti s protipandemickými opatřeními a vládními kompenzacemi finančních ztrát. Většinou se jednalo o podvody s půjčkami a granty, ale velkou část tvořily také phishingové útoky, jejichž cílem byl zisk citlivých osobních dat. Tyto pak útočníci použili pro neoprávněné žádosti o různé druhy státních finančních kompenzací.

S vývojem vakcíny proti Covid-19 se také objevilo množství podvodných schémat kdy pomocí emailů, SMS zpráv a příspěvků na sociálních sítích útočníci lákali z lidí peníze za přednostní přístup k vakcíně nebo její aplikaci bez čekání a/nebo registrace. Časté byly také útoky, kdy se útočník vydával za vládního zaměstnance a v souvislosti s vakcinací a opatřeními tak snadněji vylákal z obětí citlivá data.

Z průzkumu vnímání kyberzločinu ve Velké Británii v rámci spolupráce Avastu s britskou Neighbourhood Watch (projekt Cyberhood Watch) vyplynulo, že 32 % z více než 28 tisíc dotazovaných Britů vnímá od začátku pandemie Covid-19 internet jako nebezpečnější místo než dříve, a to právem.

Mimo tento projekt společnost Avast vydala analýzu internetové podvodné aktivity v roce 2020. Ta ukazuje, že celkový počet phishingových útoků se v ČR v prvních dvou vlnách pandemie zvedl téměř na dvojnásobky a také, že část z nich byla přímo související s Covid-19. Každopádně phishingové útoky přímo související s Covid-19 se vyskytovaly převážně během první vlny pandemie v březnu 2020 a tvoří méně než 1 % z celkového množství phishingových útoků na uživatele Avastu za celý rok (Avast, 2020). Projekt Cyberhood Watch se v návaznosti na tato zjištění začal zabývat edukací Britů na téma bezpečnosti na internetu.

VÝZNAM EDUKACE VEŘEJNOSTI V OBLASTI SOCIÁLNÍHO INŽENÝRSTVÍ

Edukace veřejnosti je jedním ze dvou hlavních nástrojů běžně využívaných pro boj s útoky sociálních inženýrů. Tím druhým jsou automatizované filtry, které pomocí nastavených pravidel vyhledávají podezřelé znaky např. v emailech a část útoků dokážou odvrátit. Toho docílí buď tím, že oběť upozorní na podezřelou aktivitu, nebo útok rovnou zablokuje odstraněním nebo odvrácením zprávy do spamové složky.

Edukací jako nástrojem pro boj se sociálním inženýrstvím se myslí, například online vzdělávací hry, vzdělávací publikace, kurzy a přednášky nebo články a zprávy, jejichž cílem je zlepšit povědomí uživatelů o nástrahách na internetu a útocích sociálních inženýrů. V ideálním případě se snažíme uživatele internetu vzdělávat tak, aby se zlepšilo nejen jejich povědomí o sociálním inženýrství, ale především jejich schopnost jednotlivé útoky rozeznat a bránit se jim.

Z celosvětových statistik IC3 je vidět, že v posledních letech pozorujeme čím dál tím prudší nárůst počtu nahlášených internetových podvodů stejně jako ztrát z nich plynoucích.

OBĚTI SOCIÁLNÍHO INŽENÝRSTVÍ

Z dat IC3 za rok 2021 vyplývá, že nejčastěji se stávají oběťmi sociálního inženýrství osoby starší 60 let. Relativně malý rozdíl je v počtu podvodů ve věkových kategoriích mezi 30 a 60 lety, kdy náchylnější jsou kategorie 30 – 39 a 40 – 49 let. To je nejspíše způsobeno vzrůstajícím objemem podvodů business email compromise, které se zaměřují spíše na skupinu lidí v plném pracovním vytížení s větší odpovědností.

Když si ale porovnáme množství podvodů s celkovou ztrátou tak zjistíme, že ztráta se s rostoucím věkem úměrně zvyšuje. Nejvyšší ztráta je tedy, stejně jako nejvyšší počet případů, u kategorie nad 60 let, ale dru-

Graf 1 – Uživatelé setkávající se s phishingovými útoky v Česku 2020. Zdroj: Avast, 2020.

há nejvyšší ztráta připadá na navazující kategorii 50 – 59 let, ačkoli ta má oproti jiným věkovým skupinám menší celkový počet podvodů. Vyplývá z toho tedy, že sice méně lidí ve věkové kategorii 50 – 59 let podlehne podvodu než v kategoriích 30 – 49 let, ale průměrně je jejich peněžní ztráta připadající na jeden podvod vyšší.

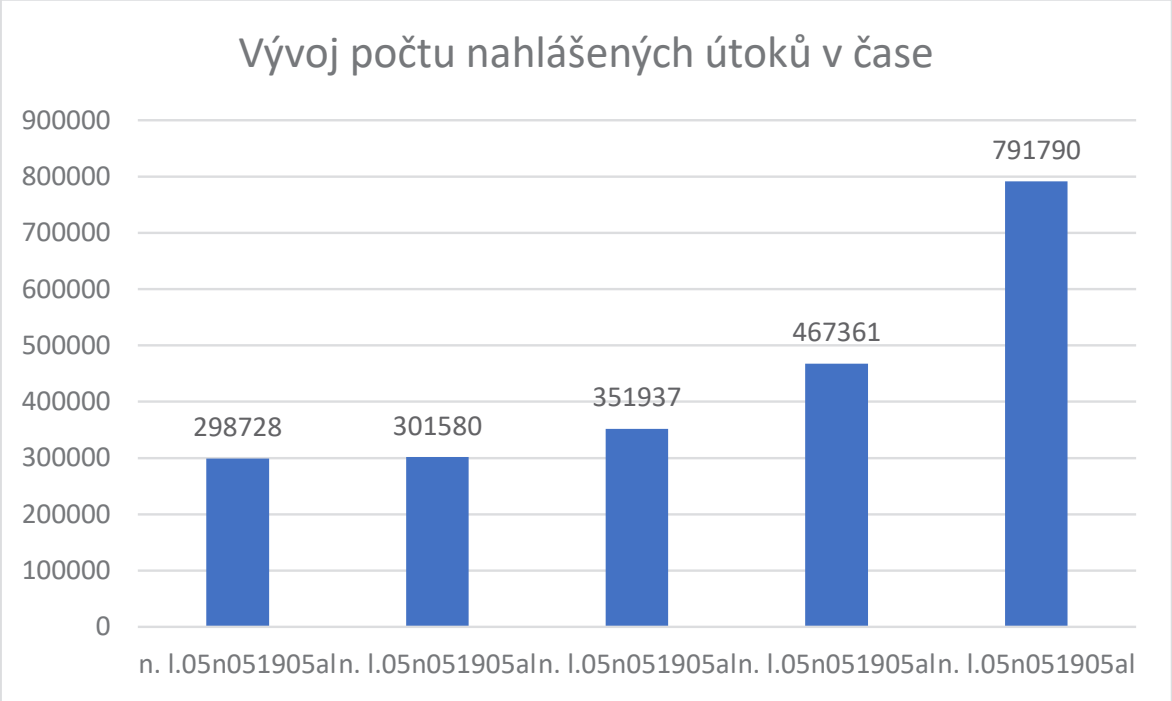
V rámci projektu E-Bezpečí Univerzity Palackého v Olomouci vznikla v roce 2018 výzkumná zpráva Starci na netu, zabývající se internetovou aktivitou osob starších 35 let. I v tomto výzkumu se ukázalo, že především senioři nad 65 let jsou skupinou vysoce náchylnou k emailovým podvodům. Zejména se jedná o phishingové útoky imitující bankovní instituce, u kterých až 45 % respondentů v této věkové skupině uvedlo, že na zprávy vyžadující pod záminkou přihlášení do bankovního účtu reagují. V některých konkrétních situacích toto číslo navíc bylo až dvakrát vyšší než u přechozí věkové skupiny 55 – 64 let (Kopecký et al., 2018, s. 18 – 19).

Ukazuje se na tom tedy opět, že náchylnost k podvodům sociálního inženýrství roste s věkem, a především senioři nad 60 let jsou velice ohroženou věkovou skupinou. Tito se často obětmi sociálního inženýrství stávají a mohou přitom být okradeni i o velké peněžní částky.

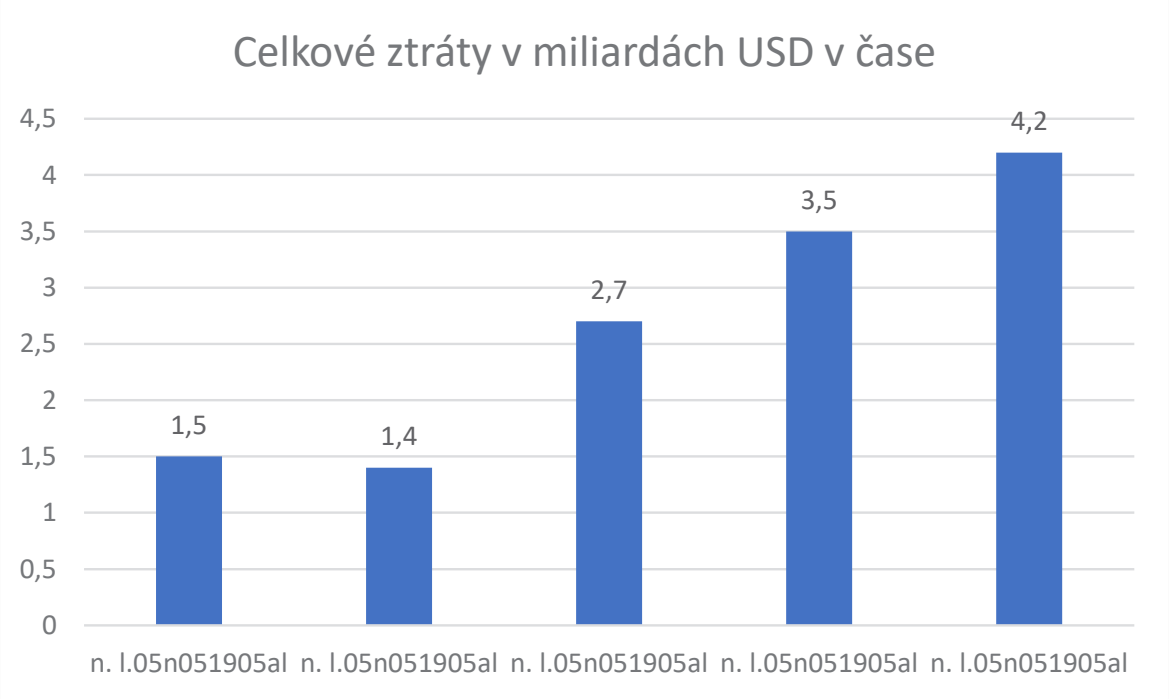
EDUKACE V TÉMATU SOCIÁLNÍHO INŽENÝRSTVÍ VE ŠKOLSTVÍ

Vzhledem k tomu, že k roku 2018 získávalo 76,4 % žáků na druhém stupni základních škol informace o kyberbezpečnosti od svých učitelů a 40 % z nich si přeje právě od nich tyto informace dostávat i nadále (Daňhelka, 2018, s. 12), je velice důležité vzdělávání o bezpečném chování na internetu na školách nezanedbávat.

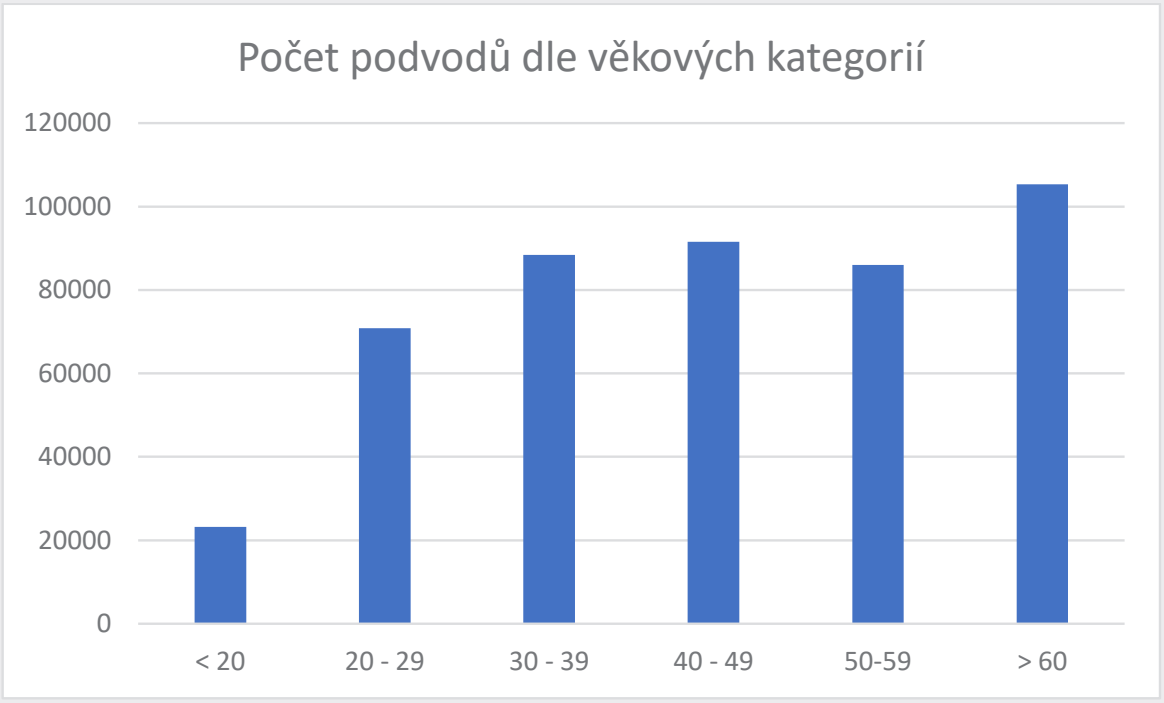
Zároveň ale aktuální úroveň, na které jsou žáci schopni rozeznávat bezpečné chování na internetu od nebezpečného není ideální a příliš mnoho dětí se v průzkumu v rámci projektu Kraje pro bezpečný internet přiznalo,



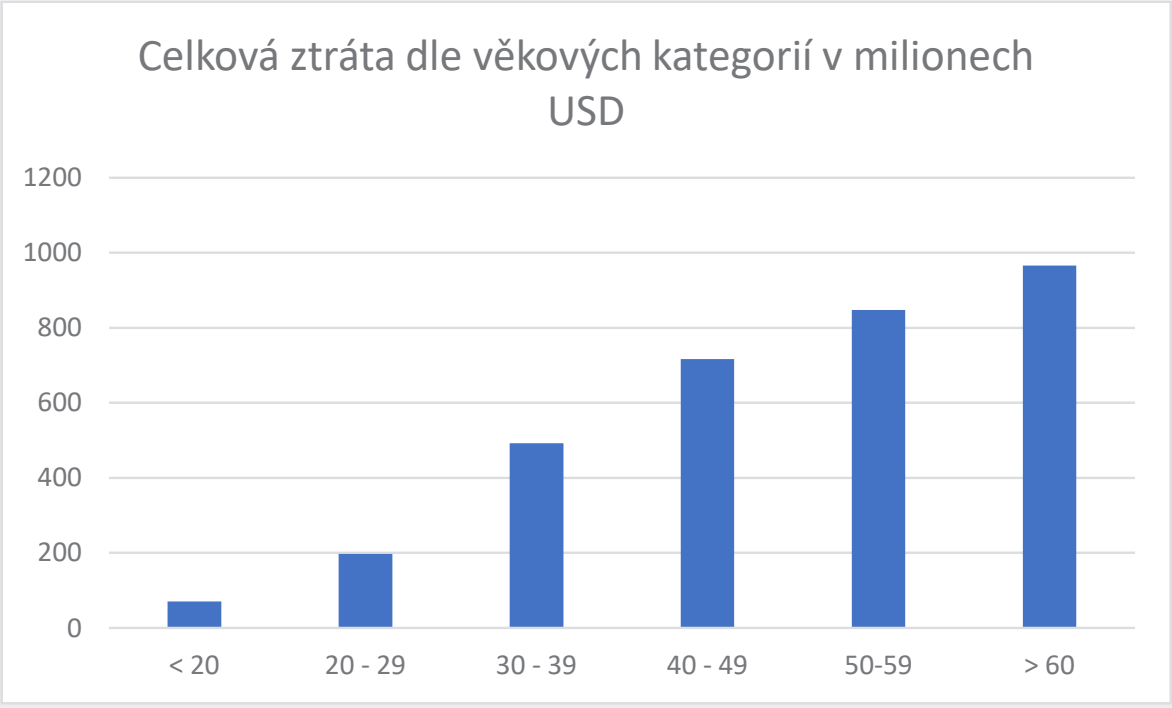
Graf 2 – Vývoj počtu nahlášených útoků v čase. Zdroj: IC3, 2021. Zpracování vlastní.



Graf 3 – Celkové ztráty v miliardách USD v čase. Zdroj: IC3, 2021. Zpracování vlastní.



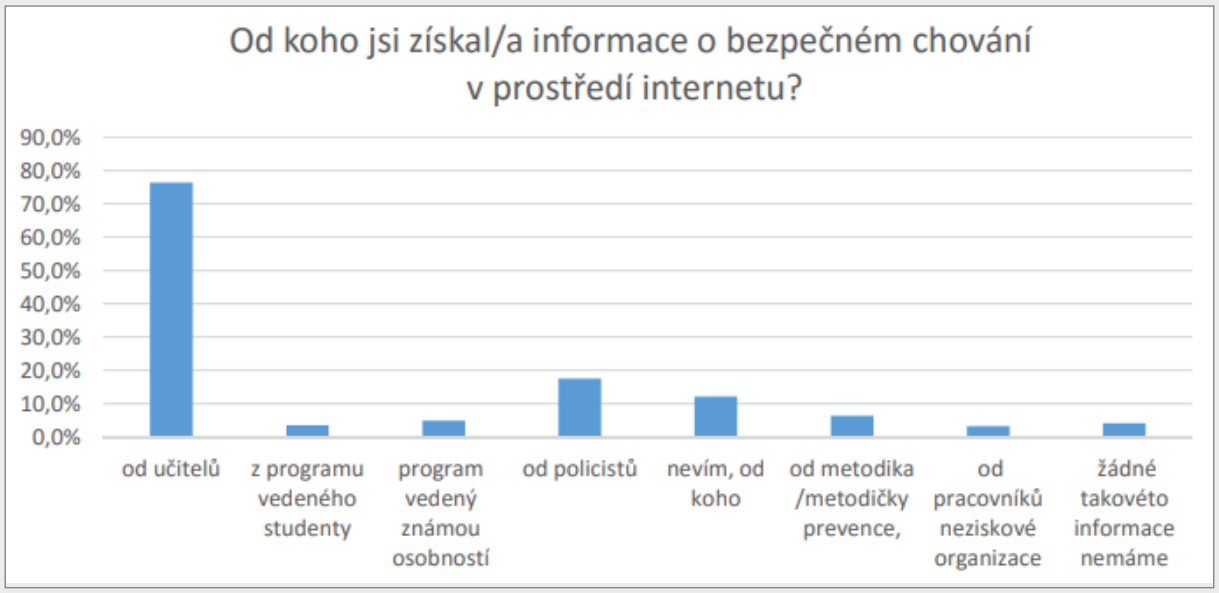
Graf 4 – Počet podvodů dle věkových kategorií. Zdroj: IC3, 2021. Zpracování vlastní.



Graf 5 – Celková ztráta dle věkových kategorií. Zdroj: IC3, 2021. Zpracování vlastní.

	Celek rel. četnost	35–44 let rel. četnost	45–54 let rel. četnost	55–64 let rel. četnost	65 let a více rel. četnost
Zpráva o tom, že je k dispozici nový výpis transakcí na účtu, který si můžete prohlédnout po přihlášení na váš účet.	39 %	34 %	40 %	39 %	45 %
Zpráva o tom, že je nutné změnit zabezpečení vašeho účtu a musíte si rychle změnit vaše heslo.	13 %	10 %	10 %	16 %	17 %
Zpráva o tom, že vám omylem připsala na účet větší množství peněz a vy musíte transakci potvrdit přihlášením se na účet.	1 %	1 %	0 %	1 %	2 %
Zpráva o tom, že se vám někdo pokusil dostat na váš účet a je nutné, abyste se co nejdříve přihlásili na váš účet a změnili si heslo.	4 %	4 %	2 %	2 %	9 %
Zpráva o tom, že jste přečerpali povolený limit účtu a je nutné, abyste se co nejdříve přihlásili na váš účet a provedli kontrolu zůstatku.	5 %	6 %	4 %	6 %	3 %
Zpráva o tom, že došlo ke změně nastavení internetového bankovnictví a je nutné, abyste změnu potvrdili přihlášením na váš účet.	7 %	4 %	6 %	6 %	15 %
Zpráva o tom, že na váš účet byla připsána platba ze zahraničí, kterou musíte do 48 hodin potvrdit přihlášením na váš účet.	2 %	1 %	2 %	2 %	2 %
Zpráva o tom, že je nutné uhradit vystavenou fakturu. Faktura je součástí přílohy emailu.	8 %	5 %	7 %	9 %	15 %
Jiné	33 %	43 %	37 %	28 %	18 %
N (celkem respondentů)	*534*	*163*	*126*	*128*	*117*

Tabulka 1 – Jak lidé nad 35 let reagují na příchozí e-maily. Zdroj: Kopecký et al., 2018, s.17 – 18.



Graf 6 – Od koho žáci dostávají informace o bezpečnosti na internetu. Zdroj: Daňhelka, 2018, s. 12.

Graf 7 – Osobní zkušenost školních dětí s kyberkriminalitou. Zdroj: Daňhelka, 2018, s. 17.

že sami nelegální a nebezpečné aktivity na internetu provádějí nebo prováděly, a to v nezanedbatelném množství. Dá se také předpokládat, že ne všichni se k nelegálním aktivitám přiznali, a tedy jsou čísla reálně ještě vyšší. Například, uvést nepravdivé údaje při registraci na sociální sítě muselo zákonitě víc dětí, než se k tomu přiznalo. Vyplývá to z počtu dětí, které dle stejného průzkumu sociální sítě s věkovými omezeními používají.
Z tohoto průzkumu tedy vyplývá, že aktuální úroveň edukace na téma bezpečnosti na internetu a kyberkriminality ve školství je nedostatečná a je na místě upravit školní vzdělávací plány a vzdělání pedagogů tak, aby děti získávaly dostatečné znalosti na místě a od lidí kterým samy věří, tedy ve škole od svých učitelů (Daňhelka, 2018, s. 12, 18 –19).

METODIKA VÝZKUMU

Práce, ze které tento článek vychází je koncipovaná jako kompilační, s případovou studií společnosti Avast. Tato společnost byla zvolena proto, že autorka je již třetím rokem jejím zaměstnancem a s jejím zájmem o edukaci veřejnosti v oblasti sociálního inženýrství tedy byla už seznámena.
V první fázi případové studie byly zjišťovány informace o společnosti Avast v souvislosti s tématem práce z volně dostupných zdrojů a zároveň formulovány otázky pro předem zvolené respondenty. Otázky navazují na dostupné informace o vzdělávacích snahách společnosti Avast na poli internetové bezpečnosti a rozšiřují je, jejich cílem bylo získání dalších informací a dat k tématu práce, která nejsou volně dostupná.
Jako respondenty autorka z vlastního průzkumu napříč společností zvolila Edera Jair Tejada Ortigozu, který v rámci své bakalářské práce v roce 2019 vyvíjel Avast Phishing Game a Terezu Kofroňovou, hlavní manažerku vzdělávacího projektu Nadace Avast Buď Safe Online. Tito dva zaměstnanci Avastu se v tématu vzdělávání veřejnosti na téma sociálního inženýrství orientují v rámci Avastu nejlépe a byli tak nejpřínosnějšími respondenty.

VZDĚLÁVACÍ INICIATIVY SPOLEČNOSTI AVAST

Edukace veřejnosti o bezpečnosti na internetu je součástí firemní společenské odpovědnosti (corporate social responsibility – CSR), která může být motivovaná dvěma způsoby: strachem nebo nadějí. Strachem z následků, které by pro společnost nebo její stakeholdery mohlo přehlížení CSR mít anebo, jako je to v případě společnosti Avast, nadějí na vytvoření lepšího světa, zlepšení vzdělání lidstva a také postavení společnosti na trhu (Machado a Davim, 2018).
Avast se dlouhodobě různými způsoby zabývá edukací veřejnosti v oblasti sociálního inženýrství. Nejznámějším a nejvýznamnějším je projekt Buď safe online, který se zaměřuje na vzdělávání školních dětí o bezpečnosti na internetu, včetně témat sociálního inženýrství, ale Avast je také mimo jiné jedním z partnerů projektu E-Bezpečí Pedagogické fakulty Univerzity Palackého v Olomouci, který se zabývá především podporou výuky o kyberbezpečnosti na školách a hlavním sponzorem vzdělávacího dokumentu V Síti.
I Buď safe online, i E-Bezpečí se ale také věnují vzděláváním rodičů školních dětí o bezpečnosti dětí na internetu. To je v dnešní době důležité především kvůli rozvoji internetu za poslední dvě dekády, který je tak prudký, že rodiče školních dětí nestíhají všechny nové technologie, sociální sítě a zařízení ani sledovat, natož se sami dostatečně vzdělávat ohledně jejich nástrah. Avast plánuje projekt Buď safe online v budoucnu rozšířit na další cílové skupiny, jako jsou žáci na středních školách nebo právě rodiče a učitele (Kofroňová, 2022). Aktuálně dle Kofroňové (2022) vzniká i konverzace mezi Nadací Avast, Národním pedagogickým institutem ČR a DigiKoalicí o možnosti proniknutí projektu Buď safe online do výuky informatiky na základních školách. Zároveň v rozhovoru souhlasila, že by si zasloužila větší pozornost v ohledu vzdělávání o bezpečnosti na internetu i věková skupina nad 60 let, která je nejvíce ohrožená sociálním inženýrstvím, ale uvedla, že Nadace Avast se v současné chvíli neplánuje soustředit na rozšiřování svých vzdělávacích aktivit tímto směrem.
Na širokou veřejnost jsou pak zaměřené aktivity Avastu na internetových blozích, které se zabývají mimo jiné rozebíráním a popisováním jednotlivých podvodů, jsou jimi Avast Blog, Akademie Avast a Avast Decoded a dále pak tiskové zprávy a informační články o sociálním inženýrství na webových stránkách Avastu.
Z průzkumu vnímání kyberzločinu ve Velké Británii v rámci spolupráce Avastu s britskou Neighbourhood Watch vyplynulo, že dvě pětiny dotazovaných se obávají kyberzločinu více, než komunitních zločinů a 36 % těch, co se stali oběťmi kyberzločinů přišlo v jejich důsledku o peníze (Avast, 2021). V rámci této spolupráce v návaznosti na tato zjištění vznikl projekt Cyberhood Watch, který informuje Brity o statistikách kyberzločinu ve Velké Británii, o nástrahách sociálního inženýrství a dalších internetových hrozeb a o důležitosti vzdělávání pro boj s nimi. Na webu projektu je i interaktivní kvíz, který detailně informuje o různých aspektech kyberbezpečnosti, radí, jak se chránit a na konci každého úseku obsahuje kontrolní otázky. Značná část tohoto kvízu se sice zabývá phishingem, ale jiné meto-

dy sociálního inženýrství jsou zde úplně opomenuty. Místo nich se zbytek kurzu ale věnuje neméně důležitým tématům jako jsou bezpečná hesla, malware a další.

AVAST PHISHING GAME

V roce 2019 vytvořil student Katedry softwarového inženýrství ČVUT a zaměstnanec Avastu Eder Jair Tejada Ortigoza v rámci své bakalářské práce gamifikovanou webovou aplikaci, jejíž účelem bylo vzdělávání lidí k identifikaci phishingových webů, zvýšení povědomí o tomto tématu a použití na mezinárodních akcích sponzorovaných společností Avast nebo jiných externích kanálech jako jsou blogy a sociální média (Tejada Ortigoza, 2019, s. vii).

Hra vznikala jako nová verze již existující hry, vytvořené zaměstnancem Avastu Martinem Hronem. Motivací pro přetvoření hry byla pro Tejada Ortigozu skutečnost, že původní verze nebyla vhodná pro mobilní zařízení, a tedy se nedala dobře použít na konferencích ani sdílet s veřejností. Také bylo potřeba její obsah upravit tak, aby ukázky phishingu byly aktuálnější.

Poprvé byla otestována v Science Museum, London v rámci výstavy Top Secret sponzorované Avastem, a poté na veletrhu Women in Business, který se konal také v Londýně. V rámci tohoto veletrhu byla hra poprvé sdílena i s širokou veřejností pomocí sociální sítě Twitter, kde Avast vyzval veřejnost pomocí příspěvku k vyzkoušení hry.

Ve své práci také Tejada Ortigoza provedl sběr a analýzu dat z aplikace měsíc po jejím spuštění pro veřejnost, kdy zjistil, že okolo 30 – 40 % uživatelů po celém světě nebylo ve hře schopno úspěšně identifikovat phishingové weby (Tejada Ortigoza, 2019, s. 31). V rozhovoru pak Ortigoza (2022) tvrdí, že výsledky pro něj samotného byly překvapením, očekával totiž, že nejlepšího hodnocení dosáhne více než 85 % hráčů.

Kvůli několika zrušeným konvencím z důvodu pandemie Covid-19 nebyla bohužel hra dále využita, po výměně marketingového týmu byl celý projekt upozaděn a hra aktuálně není veřejnosti dostupná (Ortigoza, 2022).

PROJEKT BUĎ SAFE ONLINE

Nadace Avast společně s influencerem Jiřím Králem (který vystupuje pod uměleckým pseudonymem Jirka Král) spustili v březnu 2018 projekt Buď safe online.

Projekt běží pod záštitou MŠMT a je primárně určený pro edukaci dětí na základních školách ohledně správného chování na internetu. Ambasadorka projektu Tereza Kofroňová (2022) zdůraznila v rozhovoru vliv Jiřího Krále na vznik projektu a jeho klíčovou pozici, bez něj by totiž projekt nemohl efektivně zasáhnout svou cílovou skupinu ani zdaleka v takové míře. Vznik projektu popisuje takto:

„S nápadem založit projekt, který bude dětem pomáhat být „safe online" přišel v roce 2017 Jirka Král. Toho hojně oslovovali s prosbou o pomoc jeho fanoušci na Instagramu. Došlo tak ke spojení experta na bezpečnost (Avastu) a populárního influencera, který na projektu od začátku spolupracuje bez nároku na jakýkoliv honorář."

První vlnou byla v roce 2018 série živých přednášek na školách, kdy původní ambasadorka projektu Julie Szymanská s Jiřím Králem jezdili přednášet na vybrané základní školy o bezpečnosti na internetu. Těmito přednáškami proškolili během dvou let 3 000 dětí a měly velkou úspěšnost (Kofroňová, 2022).

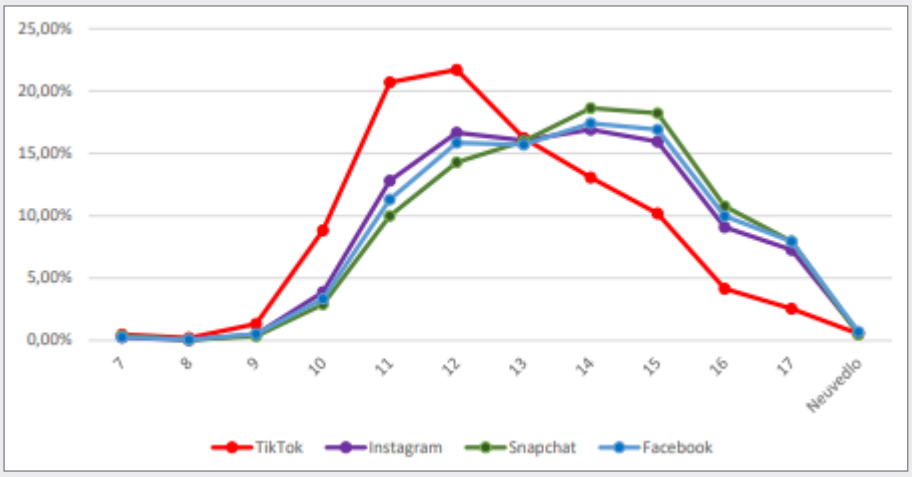
Od roku 2020 byl pak spuštěn na internetu volně dostupný interaktivní on-line kurz, který si může kdokoliv projít sám, ale je určený i pro využívání učiteli na základních školách k výuce. Jednou ze součástí kurzu je i edukace dětí ohledně podvodů na internetu a jak jim nepodlehnout. Tento kurz je aktuálně propagovaný už i dalšími influencery a oslovil díky tomu za dva roky od spuštění více než 70 000 dětí (Kofroňová, 2022). Projekt získal již řadu ocenění včetně Cen SDGs 2019, Effie Awards 2019 a 2020 a WebTop100 (Avast, 1988 – 2022).

Ukázky v jednotlivých kapitolách online kurzu využívají příspěvky z prostředí Instagramu, což je mezi dětmi na druhém stupni základních škol nejpoužívanější sociální síť, používá ji přes 70 % žáků (Daňhelka, 2018, s. 11) a i samotná simulovaná konverzace mezi kamarády má vzhled konverzace na Instagramu.

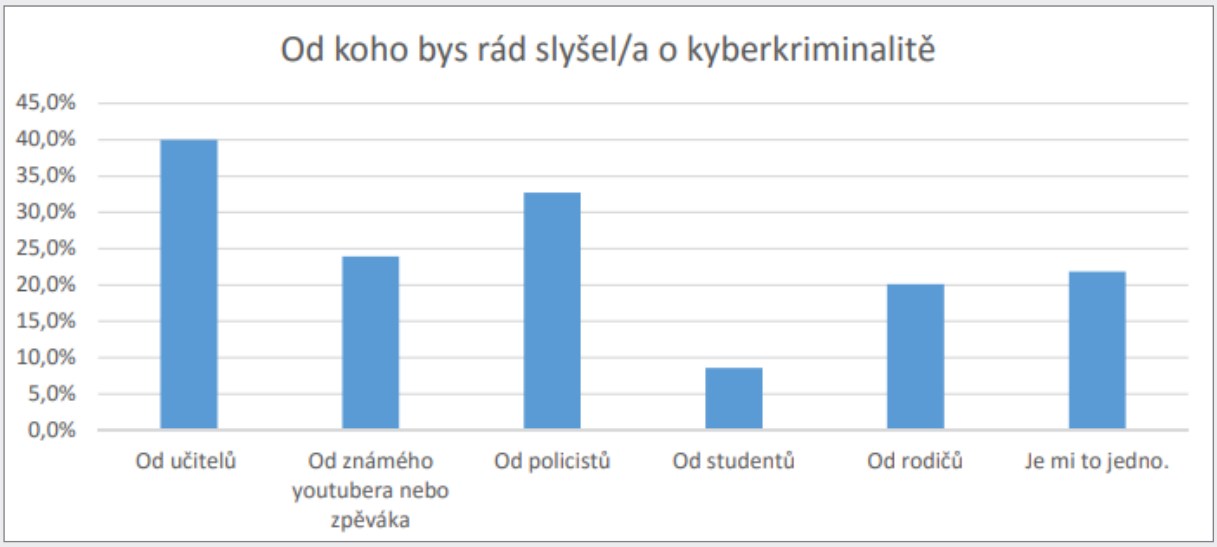
Na konci každé kapitoly kurzu je pak kvízová otázka, za kterou lze získat až 3 hvězdičky podle úrovně správnosti odpovědi. Otázka sama o sobě už shrnuje dítěti, jak by se v dané situaci mělo zachovat, ale po jejím vyhodnocení se ještě zobrazí v rámci „Opáčka" tipy, jak konkrétně může postupovat.

V rámci projektu je na stejném webu jako kurz i Buď safe online blog, kde mohou děti najít články o bezpečnosti na internetu napsané takovou formou, aby to pro ně bylo zajímavé a jednoduše pochopitelné. Blog má několik částí, od rychlých základních tipů až po články rozdělené dle jednotlivých témat bezpečnosti na internetu.

Mimo svého webu s kurzem a blogem má projekt i vlastní účty na sociálních sítích, kde je velice aktivní. Příspěvky Buď safe online jsou různého charakteru, ale jejich společné znaky jsou využívání mezi dětmi populárních obrázků, smajlíků a slangu. Snaží se děti zaujmout i jinak než vzdělávacími příspěvky a vybudo-



Graf 8 – Věkové rozložení dětských uživatelů dominantních sociálních sítí. Zdroj: Kopecký a Szotkowski, 2019, s. 10.



Graf 9 – Od koho by žáci rádi slyšeli o kyberkriminalitě. Zdroj: Daňhelka, 2018, s.12.

vat jim k projektu kladný vztah. Často různé problémy demonstrují na jejich oblíbených hrách nebo celebritách nenásilně, ale příspěvky prokládají informacemi, návody a tipy pro větší bezpečnost na internetu. Příspěvky jsou pro publikum často interaktivní, snaží se vyvolat se sledujícími diskuzi tak, že se dětí se ptají na různé otázky k tématu nebo je vyzývají k jednoduchému hlasování. Děti pak mohou odpovídat i v komentářích.
Profil na Instagramu funguje i jako forma helpdesku, kdy děti mohou do soukromých zpráv informovat o hrozbách, podvodech a jiných problémech, se kterými se na internetu setkaly a tyto zprávy pak bezpečnostní experti Avastu prověřují a reagují na ně (Kofroňová, 2022).

Na TikToku Buď safe online jsou pak příspěvky zaměřené spíše na mladší část školních dětí, jsou uvolněnější a mají zábavnější a jednodušší formu předávání informací. Oproti ostatním dominantním sociálním sítím je totiž dětské publikum na TikToku asi o dva roky mladší (Kopecký a Szotkowski, 2019, s. 10).

V jednotlivých videích kurzu, na všech účtech Buď safe online na sociálních sítích (Instagram, TikTok, YouTube) a v článcích na blogu se pak objevují i další dětem známé osobnosti z virtuálního světa. Děti k influencerům často vzhlíží a berou je jako své vzory, idealizují si je, a proto je právě Jiří Král a jeho vliv skvělým způsobem, jak děti edukovat v oblasti bezpečnosti na internetu. V průzkumu Vnímání kyberkriminality mezi dětmi v rámci projektu Kraje pro bezpečný internet (Daňhelka, 2018) se ukázalo, že děti na základních školách nejčastěji získávají informace o bezpečnosti na internetu od svých učitelů (> 75 %), případně od policistů (17,5 %), pouze necelých 5 % z nich má tyto informace z programu vedeného známou osobností jako je Jiří Král. Ze stejného průzkumu přitom vyplývá, že by si více než 20 % dětí tyto informace přálo dostávat právě od nich.

Avast proto začal po obrovském úspěchu projektu, který by bez Jiřího Krále nebyl možný (Kofroňová, 2022) oslovovat i jiné relevantní influencery, kteří projekt rozšířili mezi další masu dětí a pomohly mu dosáhnout takového úspěchu na sociálních sítích.
Aktuálně se projekt začíná rozšiřovat ale i na další cílové skupiny, jako například rodiče pomocí podcastu Máma a táta na síti a v plánu je zaměřit se i na žáky středních škol a pedagogy (Kofroňová, 2022).

ZÁVĚR

Sociální inženýrství je pouze jednou z mnoha nástrah, kterých je internet plný. Je proto velice důležité nezanedbávat edukaci veřejnosti o těchto nástrahách, a to hlavně v dnešní době, kdy se každodenní život čím dál víc přesouvá do digitálního světa. Ohrožené jsou především školní děti a senioři nad 60 let věku, kteří jsou náchylnější naletět na různé podvodné praktiky.

Ač z výzkumů vycházejí senioři jako nejzranitelnější, nejčastěji se vzdělávací projekty zabývají edukací dětí na úrovni základních škol. Děti je samozřejmě třeba vzdělávat především, a to proto, že na nich závisí úroveň vzdělanosti budoucích generací v tomto tématu. V ideálním případě by měly v dospělosti mít díky nynějším vzdělávacím snahám dostatečně vštípené vědomosti o tom, jak se v digitálním světě chovat tak, aby byl bezpečný pro všechny. Seniory je pak ale potřeba vzdělávat o bezpečnosti na internetu a zejména o sociálním inženýrství proto, že jsou kvůli velice rychlému vývoji technologií málo znalí a tím pádem náchylní naletět na podvodné praktiky, protože je neumí rozeznat. Na sklonku života pak kvůli tomu mohou přijít o úspory nebo se dokonce ještě zadlužit, většina peněz ztracených v rámci podvodů sociálního inženýrství jsou totiž právě peníze lidí starších 60 let.

Společnost Avast se zabývá edukační činností v různých zemích a pro různé cílové skupiny, ale největší důraz klade na vzdělávací projekt o bezpečnosti na internetu Buď safe online, určený zatím primárně pro děti na úrovni základních škol. Projekt začal sérií přednášek a aktuálně pokračuje formou volně dostupného online kurzu, blogu, vzdělávací aktivitou na Instagramu, TikToku a YouTube a formou podcastu. Na Facebooku také působí, ale tam spíše sdílí výše zmíněné aktivity, protože ten dnes už není mezi dětmi tak rozšířený.
Přiblížit se dětem a předat jim důležité informace se projektu daří z několika důvodů. Je to především zapojení mezi dětmi oblíbených influencerů do edukační činnosti, využívání jim blízkého jazyka a propojování témat bezpečnosti s jejich běžnými tématy. Počet dětí, které si za relativně krátkou dobu od jeho spuštění kurzem prošly je důkazem toho, že tento přístup funguje. Do budoucna je sice škoda, že se Avast neplánuje blíže věnovat vzdělávání lidí nad 60 let na téma nástrah sociálního inženýrství a bezpečnosti na internetu obecně, ale věnovat se místo toho rozšiřování projektu Buď safe online na žáky středních škol, rodiče a učitele je neméně důležité poslání. Velice užitečné by mohlo být i prostoupení projektu do výuky na školách, tyto snahy jsou sice teprve na úrovni diskuze, ale je dobrým znamením, že jsou podporované ze strany státu a dalších významných vzdělávacích institucí.

Použitá literatura

Avast Software s.r.o. [online]. Praha: Avast Software. © 1988 – 2022. Dostupné z: https://www.avast.com/

BALÁŽOVÁ, Šarlota, 2022. Vnímání vzdělávání v tématu sociálního inženýrství ve společnosti Avast. Bakalářská práce. Vysoká škola ekonomická v Praze. Fakulta informatiky a statistiky. Vedoucí práce doc. PhDr. Richard Papík, Ph. D.

Buď safe online. 2022. Instagram [online]. [cit. 2022-04-23]. Dostupné z: https://www.instagram.com/bud.safe.online/?hl=en

Buď safe online. 2022. TikTok [online]. [cit. 2022-04-23]. Dostupné z: https://www.tiktok.com/@bud.safe.online?lang=en

Buď safe online. 2022. YouTube [online]. [cit. 2022-04-23]. Dostupné z: https://www.youtube.com/c/budsafeonline/videos

Business Email Compromise Report. 2021. Greathorn.com [online]. Cybersecurity Insiders. [cit. 2022-03-06]. Dostupné z: https://info.greathorn.com/hubfs/Reports/2021-Business-Email-Compromise-Report-GreatHorn.pdf

Cyberhood Watch Insights Report. 2021. Avast.com [online]. Avast Software s.r.o. [cit. 2022-03-07]. Dostupné z: https://static3.avast.com/20001244/web/o/mkt/cyberhood/Cyberhood_Watch_UK_Insights_Report.pdf?_ga=2.265949455.1891201309.1646856208-794072161.1628834332

DAŇHELKA, Tomáš, 2018. Vnímání kyberkriminality mezi dětmi. Kpbi.cz [online]. Kraje pro bezpečný internet. [cit. 2022-03-06]. Dostupné z: https://www.kpbi.cz/prilohy/157_vyzkum_final.pdf

Elder Fraud Report 2020. 2021. Ic3.gov [online]. IC3 – FBI. [cit. 2022-03-06]. Dostupné z: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

FBI NATIONAL PRESS OFFICE, 2020. FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic. fbi.gov [online]. Washington, D.C.: FBI [cit. 2022-03-06]. Dostupné z: https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic

Hadnagy, C 2018. Social Engineering: The Science of Human Hacking. John Wiley & Sons, Incorporated. Newark. Dostupné z: ProQuest Ebook Central. [6 February 2022].

Internet Crime Complaint Center. 2022. Ic3.gov [online]. IC3 – FBI. [cit. 2022-03-06]. Dostupné z: https://www.ic3.gov

Internet Crime Report 2020. 2021. Ic3.gov [online]. IC3 – FBI. [cit. 2022-03-06]. Dostupné z: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

KOFROŇOVÁ, Tereza, 2022. E-mailový rozhovor o projektu Be safe online. Praha, 1.4.2022.

KOFROŇOVÁ, Tereza, 2020. Marketingová komunikace projektu Buď safe online. Diplomová práce. ČZU v Praze. Provozně ekonomická fakulta. Vedoucí práce Ing. Ladislav Pilař, MBA, Ph.D. Dostupné z: https://is.czu.cz/lide/clovek.pl?id=167028;zalozka=7;zp=274759;studium=235423

KOPECKÝ, Kamil a René SZOTKOWSKI, 2019. České děti v kybersvětě. E-bezpeci.cz [online]. O2 Czech Republic & Univerzita Palackého v Olomouci. [cit. 2022-03-06]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/117-ceske-deti-v-kybersvete/file

KOPECKÝ, Kamil, René SZOTKOWSKI, Martin KOŽÍŠEK a Jana KASÁČKOVÁ, 2018. Starci na netu. E-bezpeci.cz [online]. Univerzita Palackého v Olomouci. [cit. 2022-03-06]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/102-starci-na-netu-2017-2018/file

Machado, C, & Davim, JP (eds) 2018. Corporate Social Responsibility in Management and Engineering. River Publishers. Aalborg. Dostupné z: ProQuest Ebook Central. [6 March 2022].

Podcast Máma a táta na síti. 2021. Spotify [online]. Dostupné z: https://open.spotify.com/show/0inDp0lcM1FqA3MwB3U7Zf

TEJADA ORTIGOZA, Eder Jair, 2019. Avast Cybersecurity Phishing Game. Bachelor thesis. Czech Technical University in Prague. Faculty of Information Technology. Vedoucí práce Barry Richard. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/86231/F8-BP-2019-Tejada%20Ortigoza-Eder%20Jair-thesis.pdf?sequence=-1&isAllowed=y

TEJADA ORTIGOZA, Eder Jair, 2022. E-mailový rozhovor o pojektu Avast phishing game. Praha, 9. 3. 2022.