ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

SADA VZDĚLÁVACÍCH PLAKÁTŮ NA TÉMA POČÍTAČOVÁ BEZPEČNOST PRO SENIORY

BAKALÁŘSKÁ PRÁCE

Tobiáš Vaverka

Informatika se zaměřením na vzdělávání, obor Informatika se zaměřením na vzdělávání (maior) + Technická výchova se zaměřením na vzdělávání (minor)

Vedoucí práce: Mgr. Lenka Benediktová Ph.D.

Plzeň 2024

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 26. dubna 2024

.....

vlastnoruční podpis

Poděkování

Děkuji vedoucí práce Mgr. Lence Benediktové Ph.D. za ochotu cenné rady a připomínky k vypracování této bakalářské práce.

Děkuji MgA. Petru Filipovi za grafické ztvárnění ilustrací pro vzdělávací plakáty.

OBSAH

ÚVOD

Důležitost kybernetické bezpečnosti se stále zvyšuje v digitálním věku, kdy více lidí všech věkových kategorií využívá internet a digitální technologie. Senioři, kteří se stávají aktivnějšími uživateli těchto technologií, nejsou výjimkou. v důsledku toho se i potenciálními oběťmi kybernetických útoků a hrozeb. Většina vzdělávacích materiálů a kampaní zaměřených na počítačovou bezpečnost je však často náročná na pochopení, technická, a ne příliš přístupná pro seniory. Proto je nezbytné vytvořit specifické vzdělávací materiály, které budou uzpůsobeny potřebám a preferencím seniorů, v tomto případě v podobě sady vzdělávacích plakátů.

Tato bakalářská práce se zaměřuje na tvorbu sady vzdělávacích plakátů, které budou specificky navrženy tak, aby byly srozumitelné, atraktivní a efektivní pro seniory. Cílem je poskytnout seniorům znalosti, které jim pomohou chránit své osobní a finanční údaje před různými formami kybernetických hrozeb, jako jsou phishing, malware a sociální inženýrství.

Bakalářská práce se bude zabývat návrhem a tvorbou vzdělávacích plakátů, které budou obsahovat klíčové informace o počítačové bezpečnosti, důležité rady a tipy, a budou vizuálně atraktivní.

Kromě tvorby plakátů bude tato práce také zkoumat účinnost těchto materiálů prostřednictvím testování a hodnocení reakcí seniorů. Získané poznatky budou sloužit jako základ pro zlepšení a další rozvoj těchto vzdělávacích plakátů, aby byly co nejúčinnější v procesu osvěty a vzdělávání seniorů v oblasti počítačové bezpečnosti. Tímto způsobem tato bakalářská práce přispěje k ochraně seniorů před kybernetickými hrozbami, a zvýší jejich digitální dovednosti, čímž jim umožní bezpečnější a sebejistější využívání moderních technologií.

1 TEORETICKÝ ÚVOD

1.1 INTERNET A JEHO ZÁKLADNÍ POJMY

Internet je systém celosvětového rozsahu, který propojuje jednotlivé menší počítačové sítě. Počítače zde komunikují pomocí rodiny protokolů TCP/IP. Název je odvozen od anglického slovního spojení interconnected network. [1]

1.1.1 HISTORIE A VÝVOJ INTERNETU

Internet má své kořeny v ARPANET, což byl projekt financovaný agenturou Ministerstva obrany USA DARPA (Defense Advanced Research Projects Agency). Cílem bylo vytvořit síť, která by umožňovala udržet komunikaci v případě jaderného útoku. v roce 1969 byly připojeny první čtyři univerzity: UCLA, Stanford Research Institute, University of California-Santa Barbara a University of Utah. Toto připojení umožňovalo sdílení zdrojů a komunikaci mezi výzkumníky. [2]

V roce 1970 byl zaveden síťový řídicí protokol (NCP), který byl prvním standardem pro komunikaci v síti. Ray Tomlinson v roce 1971 vytvořil první e-mailový program. v roce 1974 Vinton Cerf a Bob Kahn publikovali koncept Transmission Control Protocol (TCP), který byl později doplněn o Internet Protocol (IP). [3]

ARPANET přešel na TCP/IP 1. ledna 1983, což je často považováno za "narození" moderního internetu. v roce 1984 byl uveden systém doménových jmen (DNS), což umožnilo snazší navigaci po internetu. v polovině 80. let NSF (National Science Foundation) vytvořila NSFNET, což byla další klíčová síť, která propojovala akademické a výzkumné instituce v USA. Tim Berners-Lee v roce 1989 v CERNu vytvořil World Wide Web, což zpřístupnilo internet široké veřejnosti prostřednictvím prohlížečů. v 90. letech došlo k deregulaci a komercializaci internetu, což umožnilo jeho masové rozšíření. [4]

Internet zažil exponenciální růst ve využívání a obsahu. Sociální média, e-commerce, cloud computing a mobilní internet dramaticky změnily způsob, jakým lidé používají internet. Rozvoj technologií jako jsou IoT (Internet věcí), umělá inteligence, a kvantové výpočty slibuje další transformaci internetu, ale současně přináší výzvy v oblasti bezpečnosti a soukromí. [5]

1.1.2 ZÁKLADNÍ PRINCIPY A FUNKCE INTERNETU

Internet je obrovská globální síť, která spojuje miliony menších sítí. Je často popisován jako "síť sítí", což znamená, že je to komplexní systém propojených počítačových sítí. [6]

Internet funguje na principu přenosu dat pomocí metody zvané paketové přeposílání. Data jsou rozdělena do menších kusů, nazývaných pakety, které jsou posílány nezávisle na sobě přes různé cesty v síti, a nakonec jsou znovu sestaveny v cílovém zařízení. [6]

Každé zařízení připojené k internetu má svou vlastní unikátní IP adresu (Internet Protocol Address), která slouží jako jeho identifikátor na internetu. [6]

Základem internetu je sada protokolů známá jako TCP/IP (Transmission Control Protocol/Internet Protocol). TCP zajišťuje správné doručení dat tím, že rozděluje informace na pakety, a IP určuje, jak se pakety dostanou na své cílové místo. [6]

Existují i další důležité protokoly, jako je HTTP (HyperText Transfer Protocol) pro webové stránky, SMTP (Simple Mail Transfer Protocol) pro e-mail, a FTP (File Transfer Protocol) pro přenos souborů. [6]

Routery a switche jsou klíčové komponenty, které řídí a směrují internetový provoz. Routery propojují různé sítě a rozhodují, jakým způsobem se pakety dostanou k jejich cíli. Internetová data jsou přenášena různými způsoby, včetně optických kabelů, které přenášejí data ve formě světelných impulsů, a bezdrátových technologií, jako je Wi-Fi. [6]

DNS slouží jako telefonní seznam internetu, překládá snadno zapamatovatelná doménová jména (např. google.com) na IP adresy, které počítače používají pro identifikaci a přístup k sobě. [6]

Internet funguje na end-to-end principu, což znamená, že síť sama o sobě není odpovědná za obsah přenášených dat. To umožňuje vysokou úroveň svobody a inovací, ale také přináší výzvy v oblasti bezpečnosti a regulace. [6]

Internet je navržen tak, aby byl škálovatelný, což znamená, že může růst a přizpůsobovat se bez potřeby zásadních změn v jeho základní struktuře. Otevřenost a standardizace protokolů umožňují snadnou integraci nových technologií a sítí.

Internet je tedy masivní, dynamický systém, který se neustále rozvíjí a mění. Jeho schopnost propojovat lidi, stroje a informace na celém světě má zásadní dopad na společnost, ekonomiku a kulturu. [6]

1.1.3 ZÁKLADNÍ TECHNOLOGIE A PROTOKOLY

Transmission Control Protocol (TCP) a **Internet Protocol** (IP) jsou dva klíčové protokoly, které stojí v jádru fungování internetu. Společně jsou známy jako TCP/IP a tvoří základní pravidla pro výměnu dat mezi různými zařízeními v síti. Přestože oba protokoly plní rozdílné, ale doplňující se funkce, jsou nezbytné pro efektivní a spolehlivou komunikaci na internetu. [6]

IP je zodpovědný za adresování a směrování paketů dat mezi zařízeními v síti. Každé zařízení připojené k internetu má přiřazenou unikátní IP adresu, která slouží k jeho identifikaci. IP adresy jsou číselné štítky přidělené každému zařízení, které umožňují jejich rozpoznání a lokalizaci v síti. Existují dva hlavní typy IP adres - IPv4 a IPv6. IP se stará o doručení datových paketů z jednoho místa na druhé, ale nezaručuje jejich spolehlivost, pořadí doručení, nebo integritu. [6]

TCP pracuje na vrcholu IP a zajišťuje, aby byla data doručena spolehlivě a v pořadí, v jakém byla odeslána. Řeší problémy, jako jsou ztráty paketů, chyby v datech a řazení. TCP umožňuje navázání "virtuálního připojení" mezi odesílatelem a příjemcem, což zajišťuje, že obě strany jsou připraveny na přenos dat. TCP reguluje množství dat odesílaných do sítě, aby se zabránilo jejímu přetížení, a zajišťuje správné doručení dat i v přetížené síti. [6]

TCP/IP je základem většiny internetových aplikací. IP se stará o adresování a doručování paketů, zatímco TCP se stará o kontrolu a správnost tohoto přenosu. TCP/IP je univerzální sada protokolů, což znamená, že umožňuje různým typům sítí a zařízení komunikovat mezi sebou. Díky tomu je internet skutečně globální a otevřený systém. Tato protokolová sada umožňuje snadné přidávání nových technologií a služeb, což je klíčem k neustálému rozvoji a inovacím na internetu. [6]

Takže, zatímco IP adresuje a směruje jednotlivé pakety, TCP zajišťuje, že celý přenos dat je proveden spolehlivě a efektivně. Společně tvoří základní infrastrukturu pro prakticky všechny formy digitální komunikace na internetu. [6]

Hypertext Transfer Protocol (HTTP) a jeho zabezpečená verze, HTTPS (Hypertext Transfer Protocol Secure), jsou základními protokoly používanými pro přenos dat na World Wide Web, tedy na internetu. Zatímco HTTP byl standardem pro mnoho let, HTTPS se stává stále více preferovanou volbou kvůli svým vylepšením v oblasti bezpečnosti. [6]

HTTP je protokol používaný pro přenos hypertextových dokumentů, jako jsou webové stránky. Když uživatel vyžádá webovou stránku (např. zadáním URL do prohlížeče), HTTP zajišťuje přenos souborů (jako jsou HTML, CSS, a obrázky) ze serveru na klienta (prohlížeč). HTTP je bezstavový protokol, což znamená, že každý požadavek od klienta na server je považován za zcela nový a nezávislý na předchozích interakcích. Komunikace probíhá formou požadavků (requests) a odpovědí (responses). Klient posílá požadavek na server a server odpovídá s relevantními daty nebo chybovým hlášením. [6]

Hlavní rozdíl mezi HTTP a HTTPS je ve šifrování. HTTPS používá šifrování, konkrétně protokoly SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security), aby zajistil, že všechny informace přenášené mezi webovým serverem a prohlížečem zůstanou soukromé a nedotčené. Díky šifrování je HTTPS mnohem bezpečnější než HTTP, což je nezbytné pro ochranu citlivých transakcí, jako je online bankovnictví, nákupy a přihlašovací údaje. HTTPS také poskytuje ověření webového serveru, což pomáhá ujistit uživatele, že komunikují s oprávněným serverem. [6]

HTTPS chrání před různými typy útoků, jako je "man-in-the-middle" (MITM), kde útočník může odposlouchávat nebo manipulovat s komunikací mezi klientem a serverem. Webové stránky používající HTTPS jsou často považovány za důvěryhodnější. Navíc, vyhledávače jako Google upřednostňují HTTPS ve svých výsledcích vyhledávání, což má vliv na SEO (optimalizace pro vyhledávače). [6]

Domain Name Systém (DNS), je klíčovou součástí internetu. Funguje jako telefonní seznam internetu, překládá lidsky čitelná doménová jména (například www.google.com) na IP adresy (například 172.217.16.195), které počítače používají pro nalezení a komunikaci s jinými počítači a servery na internetu. Zde je popis, jak tento proces funguje:

Když zadáte doménové jméno do webového prohlížeče, váš počítač nejprve zkontroluje, zda má pro toto doménové jméno uloženou IP adresu ve své cache paměti. Pokud váš počítač nemá požadovanou IP adresu uloženou, pošle dotaz na lokální DNS server, který je

obvykle poskytován vaším poskytovatelem internetových služeb (ISP). Pokud lokální DNS server nemá uloženou IP adresu, začne proces překladu: Dotaz je nejprve poslán na jeden z globálních kořenových DNS serverů. Tyto servery neprovádějí překlad samy, ale ukazují na TLD (top-level domain) servery, například .com, .net, atd. Dotaz je poté poslán na TLD server pro příslušnou doménu (např. server pro .com pro doménu google.com). Tento server ukáže na autoritativní DNS server pro dotazovanou doménu. Nakonec je dotaz poslán na autoritativní DNS server domény, který má přesné informace o IP adrese pro danou doménu. Autoritativní DNS server odpoví IP adresou pro doménové jméno zpět k lokálnímu DNS serveru, který následně pošle tuto informaci vašemu počítači. Váš počítač uloží tuto IP adresu do své cache paměti pro budoucí použití a použije ji k vytvoření připojení k cílovému serveru. [6]

Tento proces se odehrává během několika milisekund a umožňuje, aby byl internet snadno použitelný a efektivní. DNS je neustále aktualizován a udržován, aby reflektoval změny v IP adresách a doménových jménech. [6]

E-mailová komunikace na internetu využívá několik standardních protokolů, především SMTP, IMAP a POP3. Každý z těchto protokolů má svou specifickou roli v procesu odesílání, přijímání a ukládání e-mailů. [6]

SMTP se používá pro odesílání e-mailů z e-mailového klienta na server nebo mezi emailovými servery. Když odesíláte e-mail, váš e-mailový klient (např. Outlook, Thunderbird) použije SMTP k připojení na váš výchozí SMTP server. Tento server poté ověří vaše přihlašovací údaje a předá e-mail cílovému SMTP serveru, který je přidružen k doméně příjemce. Standardní porty pro SMTP jsou 25, 587 a 465. [6]

IMAP se používá k přístupu k e-mailům uloženým na serveru. Umožňuje uživatelům číst, organizovat a spravovat e-maily přímo na e-mailovém serveru, což je užitečné pro přístup z různých zařízení. Když se připojíte k e-mailovému serveru pomocí IMAP, váš e-mailový klient načte seznam e-mailů, ale stáhne jejich obsah až ve chvíli, kdy si je otevřete. To umožňuje synchronizaci stavu e-mailů (např. nepřečtené, označené) mezi různými zařízeními. Standardní porty pro IMAP jsou 143 a 993. [6]

POP3 se používá ke stahování e-mailů ze serveru na lokální zařízení. Po stažení jsou e-maily často odstraněny ze serveru. Když se připojíte k e-mailovému serveru pomocí POP3,

všechny nové e-maily jsou staženy do vašeho zařízení a často jsou následně ze serveru odstraněny. To znamená, že přístup k e-mailům je možný pouze z tohoto zařízení, což může být nevýhodné při používání více zařízení. Standardní porty pro POP3 jsou 110 a 995. [6]

1.1.4 INFRASTRUKTURA INTERNETU

Síťová infrastruktura je fyzickým a logickým základem internetu. Skládá se z řady propojených zařízení a médií, které umožňují přenos dat mezi různými počítačovými systémy a síťovými zařízeními po celém světě. Zde je přehled klíčových komponent a jejich role v síťové infrastruktuře:

Zahrnuje optické vlákno (pro vysokorychlostní přenos dat na dlouhé vzdálenosti), koaxiální kabely (používané kabelovými internetovými poskytovateli) a kroucené dvojlinky (pro lokální síťové připojení, například Ethernet). Zahrnuje Wi-Fi (pro lokální bezdrátové připojení) a mobilní síťové technologie jako 4G a 5G (pro internetové připojení prostřednictvím mobilních sítí). [7]

Routery jsou zařízení, která směrují datové pakety mezi různými sítěmi. Například router ve vašem domě směruje internetový provoz mezi vašimi lokálními zařízeními a širším internetem. Routery na vyšších úrovních (například u poskytovatelů internetových služeb) směrují provoz na internetové páteřní síti. [8]

Switche jsou zařízení používaná v lokálních sítích (LAN). Jejich úkolem je připojovat různá zařízení v rámci jedné sítě a efektivně předávat data mezi nimi. Na rozdíl od routerů, které směrují data mezi různými sítěmi, switche se zaměřují na provoz uvnitř jedné sítě. [8]

Modem je zařízení, které moduluje a demoduluje signály pro přenos dat přes telefonní linky, kabelové systémy nebo satelitní spojení. v domácích sítích přeměňuje digitální signály od vašeho poskytovatele internetových služeb na signály, které může zpracovat váš router nebo počítač, a naopak. [8]

Páteřní síť internetu je tvořena sítí vysokorychlostních datových cest, které spojují různé části internetu. Tyto cesty obvykle využívají vysokokapacitní optické kabely a jsou spravovány hlavními telekomunikačními společnostmi a poskytovateli internetových služeb. [8]

Datacentra jsou velká zařízení, která hostí servery a další síťová zařízení. Servery jsou počítače navržené pro zpracování žádostí a dodávání dat ostatním počítačům přes síť.

Internetové služby, jako jsou webové stránky, cloudové úložiště a aplikace, jsou hostovány na serverech v těchto datacentrech. [7]

Pro globální připojení se používají satelitní spojení a podmořské kabely. Podmořské kabely, převážně optické, spojují kontinenty a přenášejí většinu mezikontinentálního internetového provozu. Satelity se používají pro připojení v odlehlých oblastech, kde není možné položit kabely. [9]

Celkově tvoří tyto komponenty složitou, ale dobře koordinovanou síť, která umožňuje přenos dat mezi počítači a servery po celém světě, čímž vytváří základ internetu.

1.1.5 POSKYTOVATELÉ INTERNETOVÝCH SLUŽEB (ISP)

Poskytovatelé internetových služeb (ISP) jsou organizace, které nabízejí služby připojení k internetu. Mohou to být velké telekomunikační společnosti, lokální poskytovatelé, nebo specializované firmy zaměřující se na internetové služby. [10]

ISP zajišťují fyzické a síťové připojení k internetové infrastruktuře, což umožňuje uživatelům přístup k internetu. Zajišťují přenos dat mezi uživatelským zařízením a internetovými servery. Přidělují IP adresy, které jsou nezbytné pro identifikaci zařízení na internetu. Poskytují ochranu proti kybernetickým útokům a zajišťují údržbu a aktualizace své sítě. Nabízí různé typy připojení jako jsou DSL, kabelové, optické, satelitní a mobilní internet. [10]

1.1.6 CLOUDOVÉ SLUŽBY A DATACENTRA

Cloud computing umožňuje organizacím snadno škálovat své IT zdroje podle aktuálních potřeb. Poskytuje vzdálený přístup k aplikacím a datům z jakéhokoliv zařízení připojeného k internetu. Redukuje potřebu pro investice do vlastní IT infrastruktury. [11]

Datacentra poskytují velkou kapacitu pro ukládání dat firem i jednotlivců. Nabízí výpočetní zdroje pro zpracování a analýzu dat. Umožňují provozování webových aplikací a služeb. [11]

Typy Cloudových Služeb:

- **IaaS (Infrastructure as a Service):** Nabízí základní infrastrukturní služby jako jsou servery, úložiště a sítě.
- **PaaS (Platform as a Service):** Poskytuje platformu s nástroji pro vývoj a spouštění aplikací.

- **SaaS (Software as a Service):** Nabízí předplatné softwaru, který je hostován v cloudu a přístupný přes internet. [11]

1.1.7 WEBOVÉ PROHLÍŽEČE A VYHLEDÁVAČE

Webové prohlížeče interpretují kód (HTML, CSS, JavaScript) webových stránek a zobrazují jej ve vizuálně přístupné formě. Umožňují uživatelům procházet internet pomocí URL adres a hyperodkazů. Poskytují zabezpečení při procházení internetu, jako je šifrování a ochrana proti phishingu. [12]

Vyhledávače jako Google, Bing či DuckDuckGo procházejí internet, indexují obsah webových stránek a umožňují uživatelům vyhledávat informace. Používají složité algoritmy k určení nejrelevantnějších výsledků na základě vyhledávacích dotazů. [12]

1.1.8 E-MAIL A INSTANT MESSAGING

E-mail se vyvinul od jednoduchých textových zpráv k bohatě formátovaným zprávám s obrázky a HTML obsahem. E-maily nyní mohou obsahovat přílohy, integrace s kalendáři a jiné funkce. [13]

Okamžité zprávy umožňují uživatelům vyměňovat zprávy v reálném čase. Podporují přenos fotografií, videí, hlasových a video hovorů. [13]

1.1.9 SOCIÁLNÍ MÉDIA

Sociální média umožňují uživatelům sdílet obsah, komunikovat a udržovat sociální vztahy. Mají silný dopad na společnost, politiku a kulturu. Sdružují lidi s podobnými zájmy nebo cíli. Poskytují platformy pro diskuse, sdílení názorů a spolupráci. [14]

1.1.10 STREAMOVÁNÍ VIDEÍ A HUDBY, E-COMMERCE

Streamování videí a hudby umožňují uživatelům sledovat filmy, seriály a poslouchat hudbu kdykoliv a odkudkoliv. Nabízí doporučení založená na předchozích preferencích uživatelů. [15]

Online nakupování umožňuje uživatelům nakupovat produkty a služby přes internet. Nabízí široký sortiment zboží s možností snadného porovnání cen a produktů.

Všechny tyto služby spolu tvoří dynamický a neustále se vyvíjející ekosystém, který formuje způsob, jakým dnes komunikujeme, získáváme informace, nakupujeme a zabavíme se online. [16]

1.2 INTERNETOVÁ BEZPEČNOST

Kybernetická bezpečnost je oblast, která se zabývá ochranou počítačových systémů, sítí a dat před neoprávněným přístupem, změnou nebo zničením. Zahrnuje široké spektrum praktik, technologií a procesů zaměřených na ochranu online aktivit a informací. Zde jsou některé základní pojmy a praktiky pro zabezpečení online aktivit:

1.2.1 ZÁKLADNÍ POJMY

Malware (škodlivý software): Software vytvořený s cílem poškodit nebo získat neautorizovaný přístup k počítačovým systémům. [17]

Phishing: Typ online podvodu, kde útočníci využívají falešné e-maily nebo webové stránky k získání citlivých informací, jako jsou hesla nebo přístup ke kreditní kartě. [17]

Ransomware: Typ malware, který šifruje data oběti a vyžaduje výkupné za jejich obnovení. [17]

DOS a DDOS útoky (Denial of Service a Distributed Denial of Service): Útoky, které přetěžují síťové zdroje, aby znemožnily přístup uživatelů k službám. [17]

Zero-Day exploit: Bezpečnostní chyba v softwaru, která ještě nebyla opravena vývojářem, a útočníci ji využívají k provedení škodlivých aktivit. [17]

1.2.2 ZÁKLADNÍ OCHRANNÉ PRAKTIKY

Silná a unikátní hesla: Používat složitá a jedinečná hesla pro každý účet a pravidelně je měnit. [17]

Dvoufaktorová autentizace (2FA): Poskytuje dodatečnou vrstvu zabezpečení vyžadující druhý faktor (např. kód odeslaný na telefon) kromě hesla. [17]

Aktualizace softwaru: Pravidelné aktualizace operačního systému, aplikací a antivirového softwaru pro zajištění nejnovějších zabezpečovacích oprav. [17]

Zálohování dat: Pravidelné zálohování důležitých dat na externí disk nebo cloud, aby se předešlo ztrátě v případě útoku. [17]

Opatrné klikání: Být ostražitý při klikání na odkazy v e-mailech nebo na neznámých webových stránkách. [17]

1.2.3 MOŽNÉ HROZBY

Viry, malware a phishing jsou běžné hrozby v kyberprostoru, které mohou vážně ohrozit osobní i firemní data a systémy. Zde je přehled těchto hrozeb a tipy, jak se proti nim bránit:

Viry jsou druh malware, který se šíří kopírováním sebe sama do jiných programů, souborů nebo počítačových systémů. Jak se bránit? Používejte spolehlivý antivirový software a pravidelně ho aktualizujte. Buďte opatrní při otevírání e-mailových příloh, zejména pokud pochází od neznámých zdrojů. Udržujte operační systém a všechny aplikace aktualizované. [17]

Malware je obecný termín označující jakýkoliv škodlivý software, včetně virů, trojských koní, ransomware a spyware. Jak se bránit? Kromě antivirového softwaru používejte také antimalwarové programy. Vyvarujte se návštěvy podezřelých nebo nezabezpečených webových stránek. Firewall může pomoci blokovat škodlivý provoz. [17]

Phishing je technika, kdy útočníci vytvářejí falešné e-maily nebo webové stránky, aby získali citlivé informace, jako jsou hesla, údaje o kreditních kartách nebo přihlašovací údaje. Jak se Bránit? Buďte vždy ostražití při zadávání citlivých informací online, a buďte si vědomi běžných znaků phishingových útoků, jako jsou gramatické chyby nebo podezřelé e-mailové adresy. Neotvírejte odkazy ani přílohy v e-mailech, které se jeví jako podezřelé nebo nepocházejí od důvěryhodných zdrojů. Kde je to možné, aktivujte dvoufaktorovou autentizaci pro další vrstvu ochrany. [17]

1.2.4 BEZPEČNOSTNÍ PRAKTIKY

Obecné bezpečnostní praktiky

Pro zvýšení online bezpečnosti existuje řada bezpečnostních protokolů a praktik, které mohou jednotlivci i organizace implementovat. Tato opatření zahrnují kombinaci technických nástrojů, metod a nejlepších postupů:

1. HTTPS: Použití HTTPS na webových stránkách pro šifrování komunikace mezi klientem a serverem.
2. VPN (Virtuální Privátní Síť): Použití VPN pro šifrování internetového provozu a ochranu identity online.
3. Šifrování Dat: Používání šifrování pro ochranu citlivých dat uložených na zařízeních nebo přenášených přes internet.
4. Antivirový a Antimalwarový Software: Neustálé aktualizace a pravidelné skenování systému, aby se zabránilo nákaze malwarem.

5. Firewally: Instalace a konfigurace firewall pro blokování neautorizovaného přístupu k síťovým zdrojům.
6. Dvoufaktorová nebo vícefaktorová autentizace (2FA/MFA): Implementace 2FA/MFA pro zvýšení bezpečnosti přihlašovacích procesů.
7. Silná a bezpečná hesla: Používání dlouhých, složitých hesel a pravidelná jejich změna. Využití správce hesel pro správu a uložení bezpečných hesel.
8. Bezpečnostní školení a vědomí: Pravidelné školení zaměstnanců a uživatelů o bezpečnostních hrozbách a nejlepších praktikách. Podpora kultury bezpečnosti a povědomí o rizicích.
9. Aktualizace a záplatování softwaru: Pravidelné aktualizace operačních systémů, aplikací a softwarových nástrojů pro zajištění nejnovějších bezpečnostních oprav.
10. Pravidelné zálohování dat: Zálohování důležitých dat na bezpečných, oddělených médiích nebo v cloudu.
11. Incidentní reakce a obnova: Mít plán pro reakci na bezpečnostní incidenty a procesy pro obnovu po útocích nebo narušeních.
12. Bezpečnostní audity a hodnocení Rizik: Pravidelné provádění bezpečnostních auditů a hodnocení rizik pro identifikaci a řešení zranitelností.
13. Opatrnost při e-mailové komunikaci: Vědomí o taktikách phishingu a vyhýbání se otevírání podezřelých e-mailů nebo příloh. [5]

Pokročilé Bezpečnostní Techniky

- **Síťová segmentace a izolace:** Oddělení kritických systémů a dat od zbytku sítě pro lepší ochranu.
- **Detekce a prevence průniku (IDS/IPS):** Použití systémů pro detekci a prevenci průniku pro monitorování a reakci na podezřelé aktivity.
- **Bezpečnostní informační a event management (SIEM):** Použití SIEM nástrojů pro pokročilý monitoring, analýzu a reportování bezpečnostních událostí.

Žádný systém není zcela neprostupný a klíčem k účinné kybernetické obraně je kombinace různých vrstev zabezpečení a neustálé vzdělávání. Bezpečnost je proces, nikoli jednorázové řešení. [18]

1.3 SENIOŘI NA INTERNETU

V dnešní digitální éře, kdy internet a digitální technologie hrají stále důležitější roli v našem každodenním životě, se stává počítačová bezpečnost stále naléhavějším tématem pro všechny uživatele, bez ohledu na jejich věk. Senioři, kteří byli v mnoha případech tradičně vnímáni jako technicky nepřipravení, se stále více zapojují do digitálního světa, a tím se stávají zranitelnějšími vůči různým kybernetickým hrozbám. Tato kapitola se zaměří na vytyčení základních oblastí a konkrétních témat, na které se vzdělávací plakáty budou

zaměřovat. Vzhledem k počtu plakátů, které budou zpracovány v rámci této práce bylo vybráno pět oblastí, které jsou podle získaných informací klíčové pro bezpečné fungování v rámci digitálního prostoru. Také zde bude rozepsáno, jak by měl vypadat vzdělávací materiál pro seniory. [19]

1.4 POČÍTAČOVÁ BEZPEČNOST A SENIOŘI

U starší populace narážíme na problém, že internet, jak jej známe dnes nezažili v mládí. Senioři postupně přijímají moderní digitální technologie, jako jsou počítače, chytré telefony, tablety a internet, aby například zůstali v kontaktu s rodinou, zůstali mentálně aktivní nebo si zjednodušili život. Tito lidé si však ne vždy uvědomují rizika s používáním těchto technologií spojená, což nám tedy přináší i nové výzvy a hrozby v oblasti počítačové bezpečnosti. Toto ovlivňují například tyto faktory:

Technické dovednosti: Senioři mají často omezené technické dovednosti a povědomí o digitálních technologiích. Toto většinou nastává z důvodu toho, že čím jsme starší tím hůře přijímáme nové technologie. Většinou nám začnou takové novinky, jako je internet, připadat zbytečné nebo máme pocit, že nemá smysl se s nimi učit, protože nám připadá, že už jsme na to moc staří. Najdou se samozřejmě i výjimky, ale většinou se setkáme s případy, kdy starší lidé nové technologie používají, ale nejsou ochotni se o nich více učit. [20]

Povědomí o hrozbách: Mnoho seniorů nemusí být dostatečně informováno o různých kybernetických hrozbách, jako jsou phishing, malware, sociální inženýrství a jiné formy útoků. Nedostatek povědomí může znamenat, že senioři jsou náchylní k narušení bezpečnosti svých osobních a finančních informací. v rámci internetu je velmi jednoduché vytvořit si vlastní informační bublinu, kterou si navzájem ovlivňujeme s lidmi, se kterými se na internetu bavíme nebo i tím, co na internetu vyhledáváme. v takovéto informační bublině se pak stane, že nám algoritmy jednotlivých stánek a sociálních sítí doporučují informace, které zajímají nás a naše známé. To může vést k tomu, že se k nám dostávají pouze informace potvrzující naši subjektivní pravdu. Člověk, který se aktivně nezajímá o různé hrozby, které nám internet přináší nebo nemá ve svém okolí někoho takového, o těchto informacích vůbec neví. Algoritmy nám navíc mohou samy doporučovat například lživé reklamy na investiční příležitosti, což s vývojem umělé inteligence bývá stále těžší rozlišit. [21]

Důvěřivost: Senioři jsou častěji více důvěřiví a náchylní věřit různým podvodům nebo manipulacím. Toto můžeme vidět jak online, tak i mimo internet. Někteří senioři se často stávají cílem podvodů, protože většinou disponují větším množstvím majetku, který během života nashromáždili, čímž se z nich pro podvodníky stává lákavý cíl. Ve větší důvěřivosti seniorů hraje roli více faktorů. Senioři bývají závislejší na pomoci ostatních, čehož podvodníci využívají. Podvodníci jsou pak schopni zneužít své postavení a nic netušícího seniora podvést. Další faktor, který hraje roli je zvýšená míra sociální izolace a osamělosti u seniorů. Senioři, kteří nemají, na koho se obrátit s pomocí, pak může častěji vstupovat do kontaktu s cizími osobami. Také se často nechají obalamutit falešným přátelským chováním. Mají pocit, že jim daná osoba chce pomoct, jelikož se k nim chová mile. S věkem pak také přichází snížení kognitivních schopností a tím se u člověka snižuje schopnost podvody rozlišit. [22]

Zabezpečení hesel: Vytváření a správa silných a jedinečných hesel může být pro seniory náročné. To vede k používání jednodušších hesel, která jsou snadněji uhodnutelná útočníky. Senioři si často neuvědomují, že slabé heslo lze jednoduše prolomit nebo je ani nenapadne, že by se jej někdo mohl pokusit prolomit. Kromě toho, že je heslo slabé a lehce uhodnutelné všemožnými algoritmy, které jsou k tomu navržené stává se, že místo bezpečné služby pro zprávu hesel je mají napsaná na lístečku vedle počítače, což je ekvivalentem klíče pověšeného z venku vedle zamčených dveří.[20]

1.5 VZDĚLÁVACÍ MATERIÁLY PRO SENIORY

V posledních letech došlo k nárůstu zájmu o vzdělávání v oblasti počítačové bezpečnosti. s tím souvisí i tvorba různých vzdělávacích materiálů a programů, které mají za cíl zvýšit povědomí seniorů o kybernetických hrozbách a naučit je, jak se jim bránit. Tyto materiály mohou nabízet různé formy vzdělávání, včetně tradičních kurzů, online školení, brožur, prezentací a plakátů.[23]

Vzdělávací materiály by měly být strukturovány tak, aby byly snadno pochopitelné a dostupné. Obsah by měl zahrnovat základní pojmy v oblasti počítačové bezpečnosti, jako jsou hesla, phishing, malware. Zároveň by materiály měly obsahovat praktické tipy a rady, jak se před hrozbami chránit. Většina seniorů preferuje materiály, které jsou snadno dostupné a konzumovatelné. Online materiály by měly být přístupné i pro ty, kteří nejsou zkušení internetoví uživatelé. Zároveň by měly existovat tištěné materiály, které lze

distribuovat ve fyzické podobě. Jazyk použitý v materiálech by měl být srozumitelný a vhodný pro cílovou skupinu. Zbytečná technická slova a fráze by měly být minimalizovány. Důraz by měl být kladen na jasné a efektivní komunikační techniky. Také je vhodné, aby vzdělávací materiály byly interaktivní. To může zahrnovat cvičení, testy, praktické příklady a scénáře, které umožní seniorům prakticky vyzkoušet své znalosti a dovednosti. Nakonec je důležité zkoumat, jak jsou existující vzdělávací materiály efektivní v dosahování svých cílů. To zahrnuje hodnocení znalostí a chování seniorů po absolvování vzdělávacího programu.[23]

1.6 TÉMATA PLAKÁTŮ

Na základě předchozích zjištěných informací bylo vybráno, pět témat, která zasahují do jednotlivých oblastí a jsou elementární pro fungování v digitálním prostoru.

1. Digitální stopa

   Plakát bude vyobrazovat, že informace, které člověk píše a sdílí na internetu se na něj nesmazatelně otisknou.

2. Silné heslo

   Plakát se bude zabývat důležitostí nastavení silného hesla na našich účtech a poukazovat na nebezpečí, když má člověk nastavené slabé heslo.

3. Pravdivost informací

   Plakát má za cíl ukázat, jak je jednoduché dostat na internet nepravdivé informace a že by člověk neměl slepě věřit čemukoliv, co je na internetu zapsáno.

4. Identita

   Na plakátu bude vyobrazeno, jak je důležité dávat si pozor na identitu lidí na internetu, vzhledem k tomu, jak je snadné se vydávat za někoho jiného.

5. Bankovní podvody

   Plakát se bude zabývat bankovními podvody. Bude zde upozornění na konkrétní bankovní podvod, jaké je jeho nebezpečí a jak se mu vyhnout.

1.7 ZÁVĚR TEORETICKÉHO ÚVODU

Tato kapitola nám poskytla cenný přehled současného stavu výzkumu a znalostí v oblasti počítačové bezpečnosti pro seniory a vzdělávacích materiálů určených pro tuto cílovou skupinu. z analýzy bylo zřejmé, že seniorům hrozí různé kybernetické hrozby v důsledku jejich omezených technických dovedností, nedostatečného povědomí o hrozbách a nedostatečného zabezpečení svých zařízení a informací.

Existující vzdělávací materiály a programy pro seniory v oblasti počítačové bezpečnosti mají své přednosti, ale také potenciální nedostatky. Klíčovými aspekty jsou struktura materiálů, jejich forma a přístupnost, jazyk a komunikace, interaktivita a efektivita. Bylo zjištěno, že efektivní vzdělávací materiály pro seniory by měly být srozumitelné, snadno dostupné a obsahující praktické rady a vizuální prvky pro zvýšení účinnosti a zapamatovatelnosti.

2 METODOLOGIE

V této kapitole je popsán způsob, jakým se budou sbírat data pro zhodnocení účinnosti plakátů. Kapitola taktéž zahrnuje, čím se bude výzkum zabývat a výběr vzorku účastníků.

2.1 VÝZKUMNÁ OTÁZKA A CÍLE

Hlavní výzkumnou otázkou této práce je: "Jsou vytvořené vzdělávací plakáty srozumitelné?" Aby mohla být otázka zodpovězena, bude potřeba vybrat vzorek ze zamýšlené skupiny, tedy seniorů. Na základě dat z dotazníku bude vyhodnoceno nakolik plakáty plní svoji zamýšlenou funkci, v jakém směru je možné plakáty vylepšit. Cílem je tedy nejenom zhodnotit účinnost a efektivitu vytvořených plakátů, ale i pokud to bude možné upravit je na základě zpětné vazby.

2.2 VÝBĚR VZORKU

Pro účely výzkumu bude vybrán vzorek seniorů, kteří budou hodnotit srozumitelnost jednotlivých plakátů před a po vysvětlení jejich obsahu. Dotazník je zaměřen na věkovou skupinu padesát let a více. Vzorek se skládá ze tří skupin. První a největší skupinou jsou účastníci Univerzity třetího věku. Druhou skupinou jsou učitelé dvou středních škol, a to konkrétně Střední průmyslové školy elektrotechnické a Střední průmyslové školy dopravní v Plzni. Poslední, třetí, skupinou, která čítá nejméně respondentů jsou oslovení jednotlivci, rodina, známí a podobně.

2.3 DOTAZNÍKOVÉ ŠETŘENÍ

Běžnou metodou sběru dat v pedagogickém výzkumu je dotazník. Dotazník lze definovat jako metodu kladení písemných otázek a získávání písemných odpovědí. Položené otázky se mohou týkat buď vnějších nebo vnitřních jevů. Jako příklad vnějšího jevu můžeme uvést názory učitelů na implementovaná organizační opatření a jako příklad vnitřního jevu postoje, motivy, emoční stavy atd. Samotný dotazník je systém připravených a důkladně formulovaných otázek, které jsou cíleně uspořádány. Na otázky odpovídá respondent písemně. Metoda dotazníku je často právem kritizována, protože neodhaluje, kdo respondenti opravdu jsou, ale pouze to, jak se sami vidí nebo jak chtějí být viděni. Vysoká frekvence používání dotazníků v pedagogickém výzkumu je pravděpodobně způsobena jejich zdánlivě jednoduchou strukturou. Data získaná z dotazníku mají vždy jen podmíněnou platnost a vyžadují velmi opatrnou interpretaci, aby bylo možné odlišit

objektivní zjištění od subjektivních úsudků. Na druhou stranu je nespornou výhodou dotazníku, že umožňuje relativně rychlý a nákladově efektivní sběr dat od velkého počtu respondentů. [24]

2.3.1 DRUHY POLOŽEK DOTAZNÍKU

Místo pojmu položka se běžně používá pojem „otázka“. Označení položka je vhodnější, jelikož některé prvky dotazníku nemusí být v podobě otázky, ale spíše v podobě pokynu například vyberte pravdivá tvrzení. Prvky v dotazníku lze klasifikovat dle různých kritérií, včetně účelu, pro který je prvek určen, formy vyžadované odpovědi a obsahu. [24]

2.3.2 CÍL POLOŽKY DOTAZNÍKU

Jednotlivé položky dotazníku lze rozdělit na obsahové a funkční. Obsahové prvky sbírají data, která jsou nezbytná pro splnění cíle výzkumu, zatímco funkční prvky mají za cíl optimalizovat proces dotazování. Mezi funkční prvky patří takzvané kontaktní prvky, funkčně-psychologické prvky, filtrující prvky a kontrolní prvky. [24]

Kontaktní položky

Kontaktní položky jsou používány k navázání správného kontaktu mezi respondentem a výzkumníkem. Jsou obvykle jednoduché a přímé, slouží jako úvod do dotazování a vedou respondenta k prozkoumávanému tématu. Dotazy týkající se demografických údajů respondentů obecně nejsou vhodné jako kontaktní položky, protože mohou vyvolávat pochybnosti o anonymitě průzkumu a nedůvěru vůči výzkumníkovi. Často je výhodnější požádat o demografické údaje na konci dotazníku. Další nevhodné kontaktní položky jsou citlivé otázky nebo takové, které by mohly respondenta znepokojit. [24]

Funkčně psychologické položky

Funkčně psychologické položky použijeme jako prostředek k odstranění nežádoucího napětí u respondenta, někdy je lze využít při přechodu k novému tématu, aby se respondent naladil na nové téma nebo jako způsob, jak odstranit stereotypické postoje respondenta k tématu. Když je kladeno více otázek týkajících se téhož problému, mohou vytvořit určitý stereotyp v odpovědích respondenta. V těchto případech je výhodné přerušit dotazování funkčně psychologickou položkou, která odpoutá pozornost respondenta jinam, než se vrátí k hlavnímu tématu. [24]

Kontrolní položky

Kontrolní položky jsou navrženy tak, aby ověřily věrohodnost získaných dat. Lze použít několik variant kontrolních položek. Jednou z možností je zeptat se respondenta na několik otázek týkajících se jednoho faktu. Například, zeptat se: 'Jste spokojen ve svém zaměstnání?' a v jiné části dotazníku: 'Chcete si najít novou práci?' Pokud je zjištěn rozpor mezi odpověďmi, může být položka buď zavrhnuta jako nespolehlivá nebo může být provedeno další šetření. Další variantou kontrolních položek jsou otázky, na které je odpověď zcela jistá. Rozpor mezi faktem a odpovědí respondenta opět ukazuje na nízkou důvěryhodnost odpovědí. Další varianta používá otázky o neexistujících faktech například událostech nebo osobách. Pokud respondent odpovídá na tyto otázky určitým způsobem, může to také naznačovat nedostatek vážnosti v jeho odpovědích. Zůstává otázkou, zda můžeme vztáhnout nedostatek důvěryhodnosti nebo nevážnosti odpovědí na všechny položky dotazníku nebo jen na některé jeho části. Pravděpodobně to závisí na typu kontrolní otázky a povaze prozkoumávaného problému. Důležitým pravidlem při používání kontrolních položek je, že kontrolní otázka nesmí být umístěna ihned vedle položky, kterou kontroluje. [24]

Filtrující položky

Filtrující položky se používají při zkoumání témat, která se netýkají celého zkoumaného vzorku. Jsou typicky umístěny před hlavními položkami a mají za cíl eliminovat jedince, kteří nejsou pro studii relevantní. Například, pokud se průzkum týká studentů, kteří jsou členy sportovního klubu, jedna z prvních položek se týká členství ve sportovních klubech. Další odpovědi respondenta nejsou relevantní ve chvíli, kdy odpoví jinak než žádoucím způsobem. [24]

2.3.3 FORMA POŽADOVANÉ ODPOVĚDI

Na základě způsobu, jakým má respondent odpovědět na určitý prvek v dotazníku, lze prvky rozdělit na otevřené a uzavřené. U otevřených prvků vytvářejí respondenti své vlastní odpovědi, zatímco u uzavřených prvků manipulují s předem připravenými odpověďmi. Otevřené prvky nenavrhnou předdefinované odpovědi. Pouze stanoví téma, ke kterému mají zaujmout stanovisko, a obecně respondenty dále nesměrují. Nevýhodou těchto prvků je jejich otevřenost, která ztěžuje vyhodnocení. Po sesbírání všech odpovědí je obvykle nutné provést navíc kategorizaci, která velký počet individuálních odpovědí převede do

menšího počtu vybraných kategorií, což vždy vede k určité ztrátě informací. Zpracování otevřených odpovědí také vyžaduje poměrně kvalifikovaný personál a má vyšší časovou náročnost. Proto není použití tohoto typu prvků v rozsáhlých průzkumných studiích velmi praktické. Otevřené prvky jsou však užitečné v předběžném průzkumu, kde lze nejčastější typy odpovědí použít k sestavení možností pro uzavřené prvky. Výhodou otevřených prvků je, že často umožňují hlubší vhled do zkoumaných jevů a lépe zachycují skutečné názory respondentů než uzavřené prvky. Schopnost a ochota vyjádřit se, je velkým faktorem u výpovědní hodnoty těchto prvků. Otevřené prvky se hodí jako kontaktní prvky nebo jako funkčně-psychologické prvky. Při grafickém návrhu otevřených prvků je vždy nutné poskytnout dostatek prostoru pro odpovědi. [24]

Uzavřené prvky se vyznačují tím, že respondentům jsou prezentovány určité počty připravených odpovědí. Největší výhodou těchto prvků je, že značně zjednodušují vyhodnocení odpovědí. Respondenti často ochotněji vyplňují dotazníky s připravenými odpověďmi. Nevýhodou této formy je však to, že všechny možné kvality odpovědí jsou nevyhnutelně vtlačeny do schématu připravených odpovědí. Příkladem mohou být otázky ano, ne nebo A, B, C, D. [24]

2.3.4 ZJIŠŤOVANÝ OBSAH POLOŽKY

Položky v dotazníku lze rozdělit na prvky, které zjišťují fakta, prvky, které zjišťují znalosti a povědomí, a prvky, které zjišťují názory, postoje a motivy respondentů. [24]

Položky zjišťující fakta

Prvky, které zjišťují fakta, obvykle nevyžadují mnoho úsilí při odpovídání a často jsou používány jako úvodní prvky v dotazníku. Jsou také používány během celého procesu dotazování, aby poskytly respondentům oddech od náročnějších otázek. Prvky, které zjišťují fakta, jsou často dichotomické (ano-ne typ). Mezi ně řadíme otázky týkající se demografických údajů. Z psychologického hlediska je nejvhodnější umístit otázky na demografická data na konec dotazníku. [24]

Položky zjišťující znalosti nebo povědomí

Prvky, které zjišťují znalosti nebo povědomí, musí být ve formuláři velmi pečlivě formulovány, aby se respondenti necítili kompromitováni svým nedostatkem znalostí. Toho lze dosáhnout například formulací, která naznačuje, že nevědomost je zcela normální.

Například formulace: 'Pamatujete si, kdo byl posledním prezidentem Federálního shromáždění ČSFR?' (méně vhodná formulace: 'Kdo byl posledním prezidentem Federálního shromáždění ČSFR?') atd. [24]

Položky zjišťující názory, postoje a motivy

Prvky, které zjišťují názory, postoje a motivy, jsou velmi citlivé na formulaci a umístění v dotazníku. Důležitým principem je, že prvky nesmějí vyjadřovat názory, postoje nebo hodnocení autora dotazníku. Mnoho otázek tohoto typu může u respondentů vyvolat nepohodlí, negativní reakce atd. V takových případech se doporučuje, aby formulace prvků jasně ukázala, že různorodost názorů je zcela přirozená a normální. [24]

U prvků, které zjišťují názory, postoje a motivy, se často používají tzv. nepřímé (projektivní) otázky. Tyto se zvláště používají, když se zkoumají 'citlivá' témata, o kterých respondenti neradi mluví. V takových případech se například neptáme přímo na názory respondenta, ale na názory celé skupiny, ke které respondent patří, názory 'lidí obecně' atd. [24]

2.4 VLASTNÍ DOTAZNÍKOVÉ ŠETŘENÍ

Dotazník jako první obsahuje část na sběr osobních údajů jako je věk, vzdělání nebo třeba zkušenosti s digitálními technologiemi. Tato část bude sloužit k rozdělení jednotlivých odpovědí podle věku, vzdělání a předchozích zkušeností. V druhé části jsou již jednotlivé plakáty. Respondent si nejprve každý plakát prohlédne a následně zhodnotí na stupnici jedna až deset, jak plakátu rozumí. Dále bude následovat vysvětlení daného plakátu po němž respondent opět zhodnotí, jak plakátu rozumí po vysvětlení. Nakonec respondenti zhodnotí na stupnici jedna až pět, tedy jako ve škole, informační hodnotu a vizuální stránku plakátů. Taktéž je zde možnost napsat zde vlastní zpětnou vazbu, co by osobně změnili nebo co se jim na plakátech líbilo. [24]

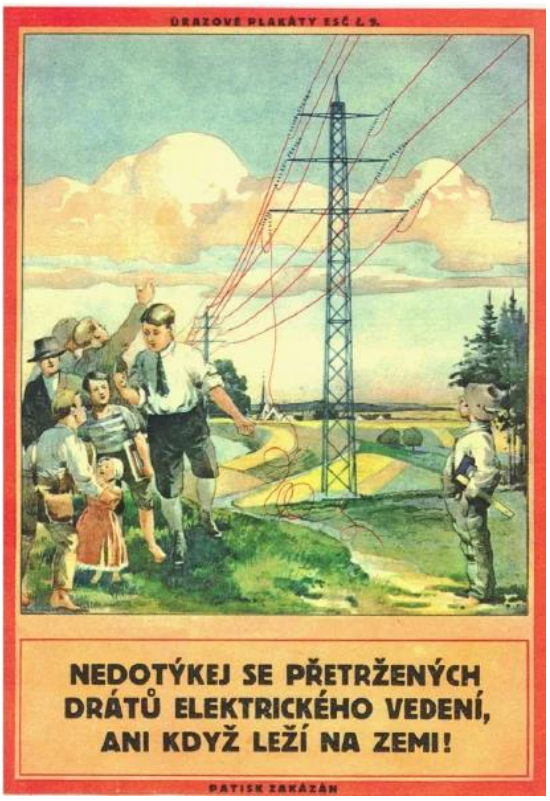
3 VYTVOŘENÍ SADY VZDĚLÁVACÍCH PLAKÁTŮ

Tato kapitola se zaměřuje na proces tvorby sady vzdělávacích plakátů na téma počítačová bezpečnost pro seniory. Zaměřuje se zejména na proces návrhu designu samotných plakátů.

3.1 NÁVRH DESIGNU PLAKÁTŮ

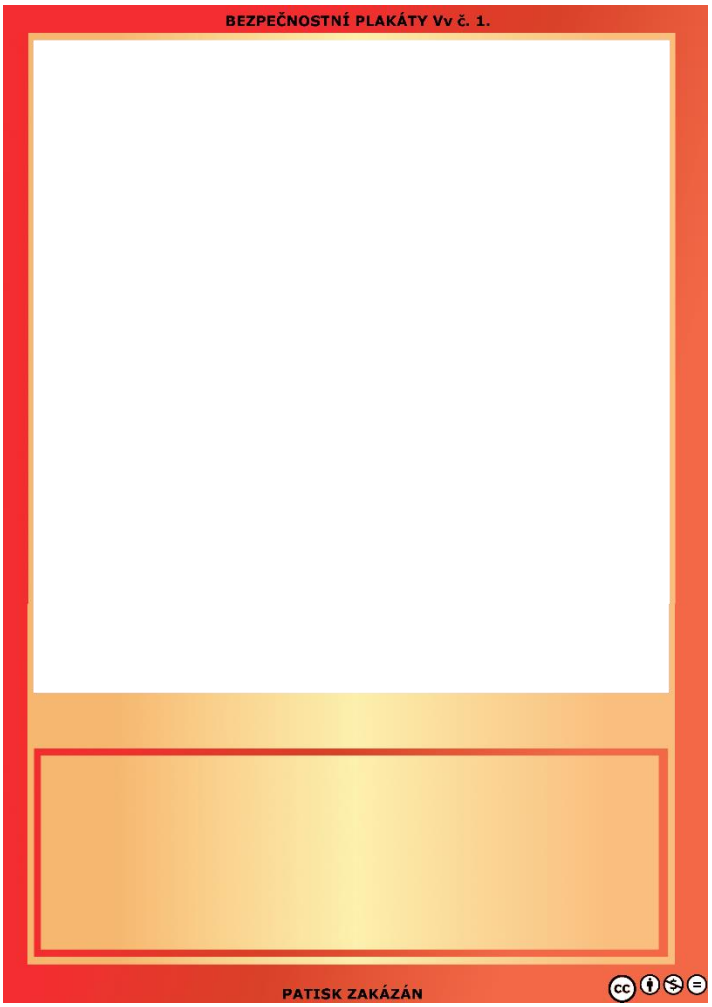
Návrh designu plakátů zahrnoval určení vizuálního stylu, barevného schématu, velikosti a rozložení textu a obrázků. Při návrhu byly zohledněny potřeby seniorů, kteří mohou mít omezené vidění a technické dovednosti. Důležité bylo zvolit design, který je přehledný, atraktivní a srozumitelný.

Pro splnění všech těchto bodů byla nalezena inspirace v minulosti. v době, kdy u nás začal být zaváděn elektrický proud se společnost setkala s podobnou situací jako s dnešním internetem. Lidé nevěděli, jak s elektrickým proudem bezpečně zacházet. Pro šíření osvěty o těchto nebezpečích, bylo vytvořeno větší množství úrazových plakátů, na kterých bylo znázorněno, jak se jednotlivým nebezpečím vyhnout. Jako příklad můžeme uvést plakát varující před houpáním na spadlých drátech elektrického vedení, ale vznikla jich celá řada.



Obrázek 1 Úrazový plakát ESČ, ukázka [25]

Vizuální styl, barevné schéma, velikost a rozložení textu a obrázků jsem založil právě na těchto úrazových plakátech. Důležité informace jsou zapsány velkým čitelným písmem. formulace které byly zvoleny jsou co možná nejpodobněji původním plakátům. Inspirace úrazovými plakáty byla zvolena z jednoduchého důvodu. Předpokladem je, že spousta seniorů zná původní úrazové plakáty a tím pádem pro ně bude atraktivní jak použité fyzické médium, tak i samotný vzhled plakátů. Každý plakát se snaží svoji problematiku metaforicky přirovnat k něčemu, co zná i člověk, co se na internetu tolik nepohybuje.



Obrázek 2 Šablona pro plakáty o bezpečnosti na internetu (Zdroj: vlastní)

Samotná šablona, která byla navržena pro jednodušší vytvoření plakátů je barevným i stylistickým obrazem své předlohy. Cílem bylo zanechat co nejvíce společných znaků s původními plakáty. Jelikož původní plakáty se jmenovaly úrazové plakáty ESČ bylo rozhodnuto pojmenovat je v podobném duchu. Zvolený název plakátů je Bezpečnostní plakáty Vv. Vv je zkratka příjmení autora. Plakát také hned za názvem obsahuje své číslo, stejně jako to měly plakáty původní. Šablona obsahuje místo pro ilustraci a text, který bude doplněn na základě tématu plakátu. Dole na plakátu je nápis patisk zakázán z důvodu co největší podobnosti s původním dílem. Kromě nápisu je dole plakát doplněn ještě o licenci.

3.2 VÝBĚR OBRÁZKŮ A ILUSTRACÍ

Nejprve tedy bylo nutné vymyslet ilustrace. Obrázky a ilustrace na plakátech byly pečlivě vybrány tak, aby doplnily text a vizuálně prezentovaly důležité koncepty. Bylo zohledněno, že seniorům mohou obrázky pomoci k lepšímu porozumění a zapamatování informací. Obrázky byly zvoleny tak, aby byly relevantní a nápomocné. Původním nápadem bylo využít pro jejich vyhotovení umělou inteligenci. S tímto řešením se však vyskytl problém, jelikož v době tvorby ilustrací nebylo možné přes umělou inteligenci vytvořit dostatečně konkrétní obrázek, který by odpovídal předem zadaným požadavkům. Bylo tedy nutné ilustrace nakreslit ručně.

Samotné ilustrace jsou vyhotoveny malířem a sochařem MgA. Petrem Filipem. Každý obrázek je vytvořen na míru ke každému plakátu. Jedná se o ruční kresbu digitálně dokončenou ve vektorovém grafickém programu.

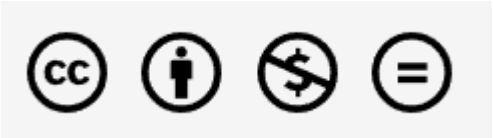
3.3 POUŽITÝ SOFTWARE

Plakáty byly vytvářeny ve dvou softwarech. První software, který sloužil k dokončení ilustrací, je CorelDraw, který je vhodný pro práci s vektorovou grafikou. Dokončení zahrnovalo převážně barevnou výplň ruční kresby. Vektorová grafika byla použita z důvodu jednoduššího škálování ilustrací.

Druhým programem, ve kterém byly plakáty tvořeny je GIMP. Je to volně dostupný rastrový grafický editor. Zde byla vytvořena šablona pro plakáty, a nakonec i doplněny ilustrace a text. Tento program byl využit hlavně z důvodu, že s ním má autor práce zkušenosti a pro potřeby této práce byl zcela dostačující.

3.4 LICENCE

Plakáty obsahují licenci creative commons. Tato licence umožní volné šíření materiálu, avšak zakazuje komerční využití. Při šíření je nutné, aby člověk, který chce dílo šířit uvedl autora. Je možné jej šířit pouze v neupravené formě, ale na jakémkoliv médiu, či formátu. Díky licenci se sníží riziko zneužití tohoto díla ke komerčním účelům, avšak bude možné jej volně distribuovat.



Obrázek 3 Použitá licence CC BY-NC-ND 4.0 [26]

3.5 FINÁLNÍ VERZE PLAKÁTŮ

Plakáty prošly několika verzemi, které jsem na základě zpětné vazby okolí a na základě dotazníku upravoval. Finální verze těchto plakátů jsou přílohou této bakalářské práce.

Výsledkem této kapitoly je sada vzdělávacích plakátů zaměřených na počítačovou bezpečnost pro seniory, které byly navrženy na základě potřeb a preferencí této cílové skupiny.

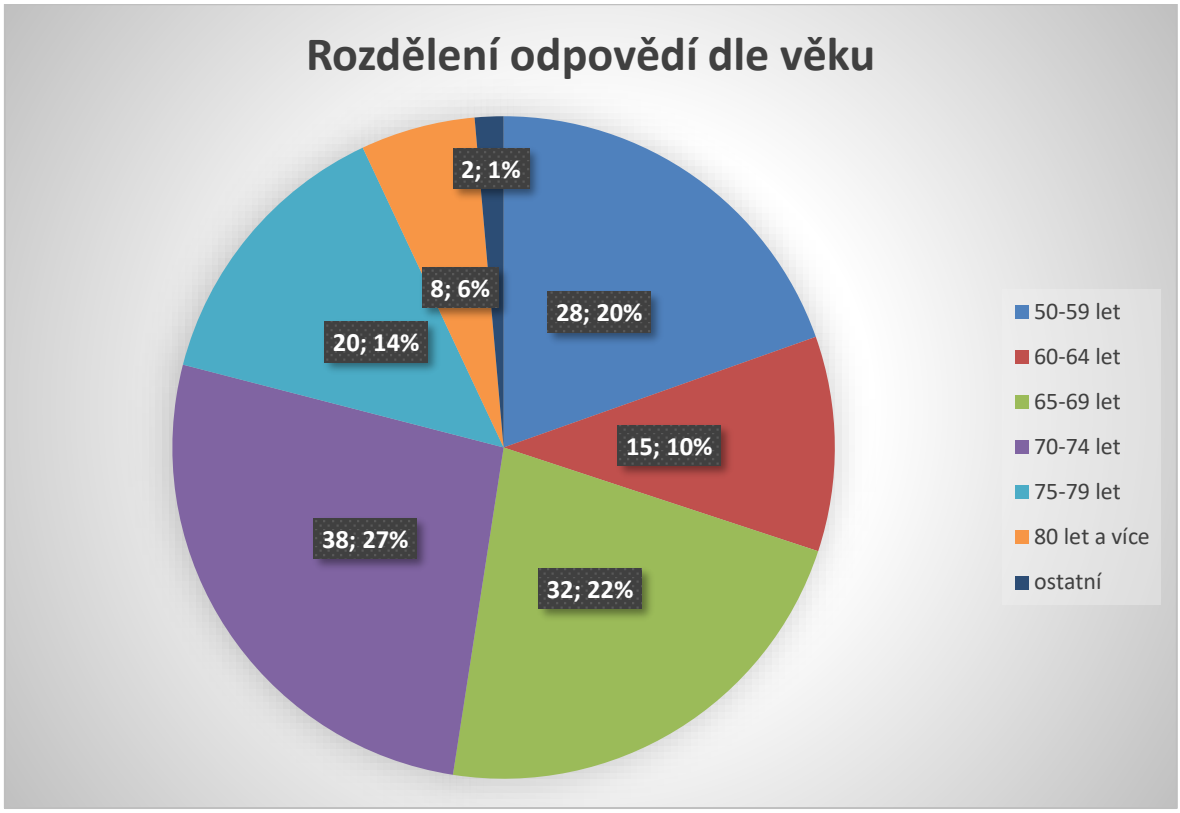
4 TESTOVÁNÍ A HODNOCENÍ ÚČINNOSTI PLAKÁTŮ

V této kapitole se zaměříme na proces testování a hodnocení účinnosti vzdělávacích plakátů na téma počítačová bezpečnost pro seniory. Cílem je zhodnotit, zda tyto plakáty splňují svůj záměr a jsou schopny zvýšit znalosti a povědomí seniorů v této oblasti.

4.1 VÝSLEDKY DOTAZNÍKU

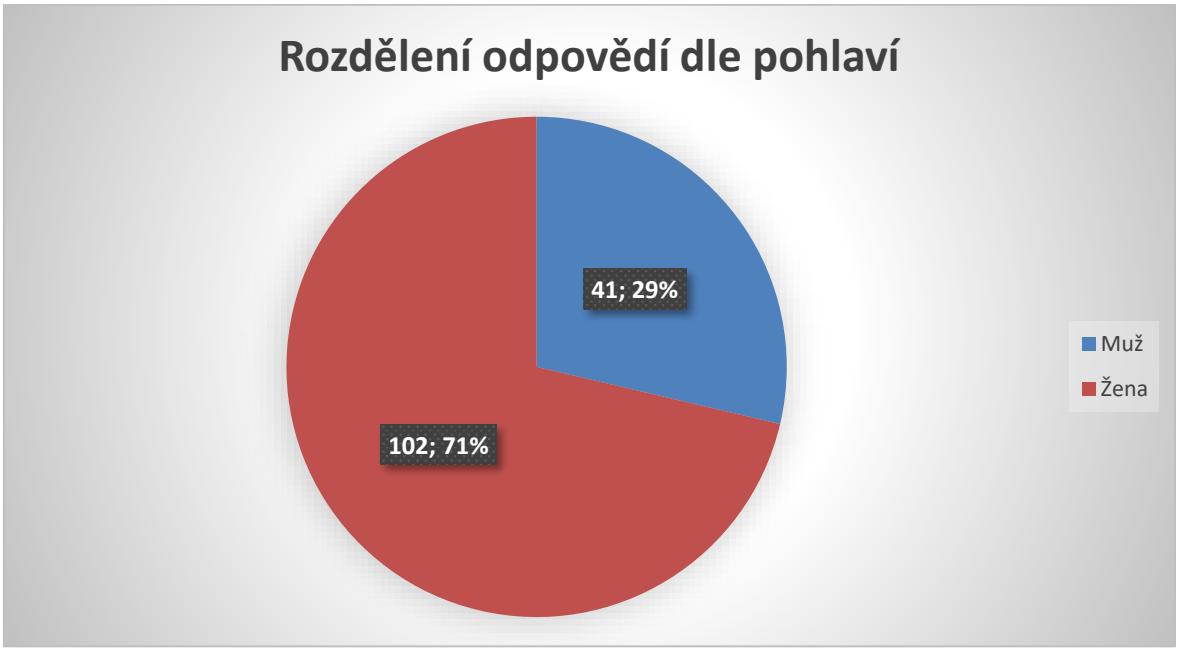
Výsledky dotazníku jsou zpracovány a vyobrazeny ve formě grafů. Jednotlivé komplexnější vazby mezi výsledky dotazníku jsou zde slovně popsány. Za dobu sběru dat se mi podařilo získat odpovědi od 143 respondentů. Sběr dat jsem ukončil ve chvíli, kdy tři dny po sobě nepřišla nová odpověď.

Prvním vyplňovaným údajem byl věk. z grafu můžeme vyčíst, že nejpočetnějšími skupinami byli lidé ve věku šedesát pět až sedmdesát čtyři let, což je téměř polovina celkového počtu odpovědí. Ve skupině ostatní jsou zahrnuty odpovědi mimo stanovené věkové rozsahy, tedy pod padesát let věku. Skupina padesát až šedesát čtyři let zahrnuje necelou třetinu odpovědí a nakonec lidé ve věku sedmdesát pět a více let zahrnují pětinu respondentů.



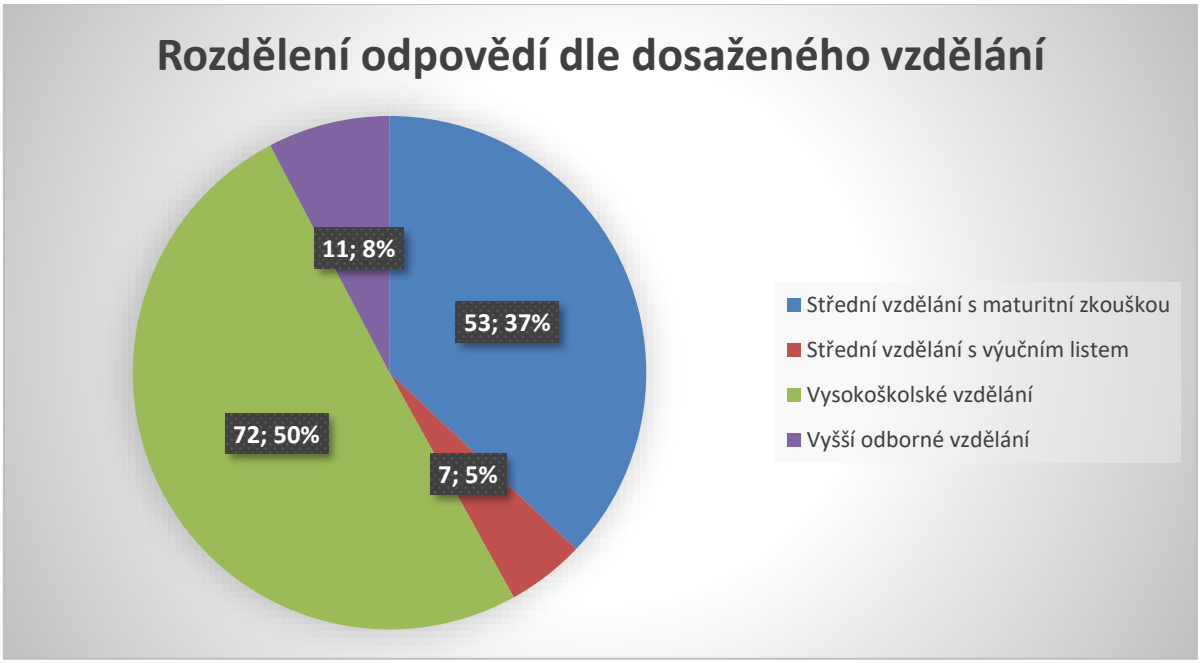
Graf 1 Odpovědi dle věku (Zdroj: vlastní)

Dalším údajem je pohlaví. Větší část odpovědí přišlo od osob ženského pohlaví.



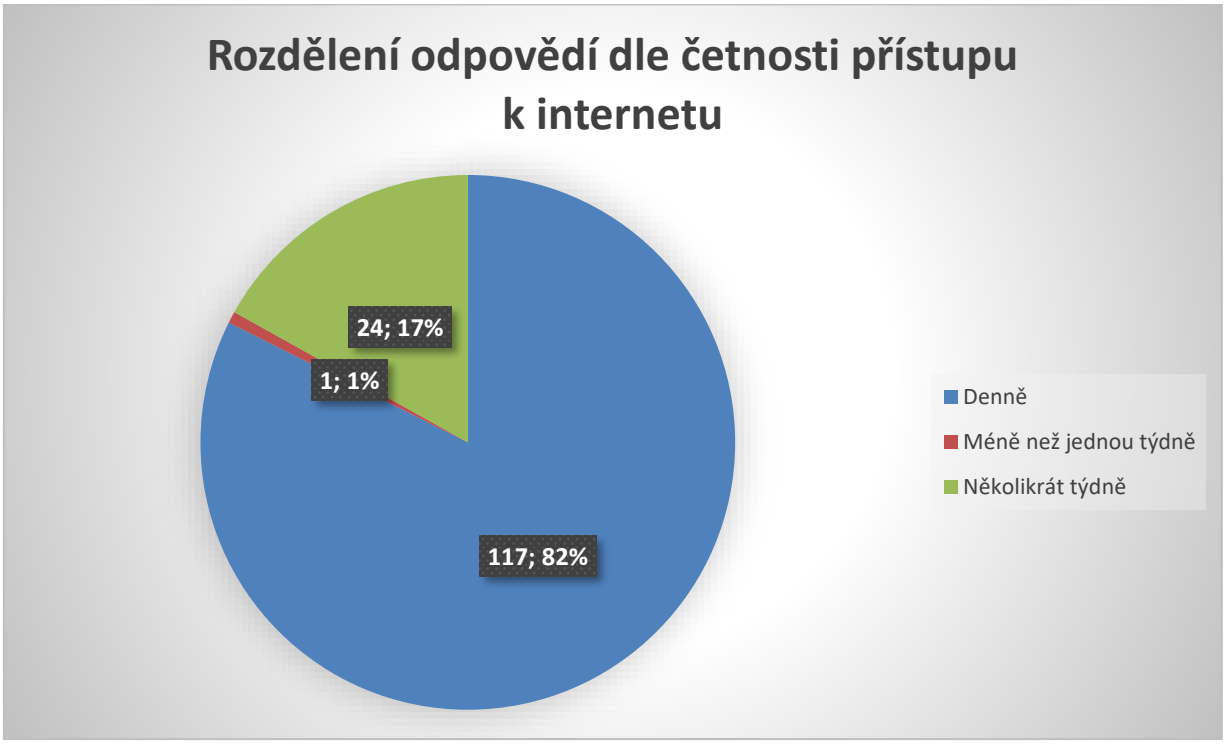
Graf 2 Odpovědí dle pohlaví (Zdroj: vlastní)

Třetím údajem je nejvyšší dosažené vzdělání. Polovina odpovědí přišla od vysokoškolsky vzdělaných lidí, což přisuzuji institucím, ve kterých byl dotazník distribuován, tedy Univerzita třetího věku a střední školy. Nikdo z respondentů neuvedl základní vzdělání jako své nejvyšší dosažené.



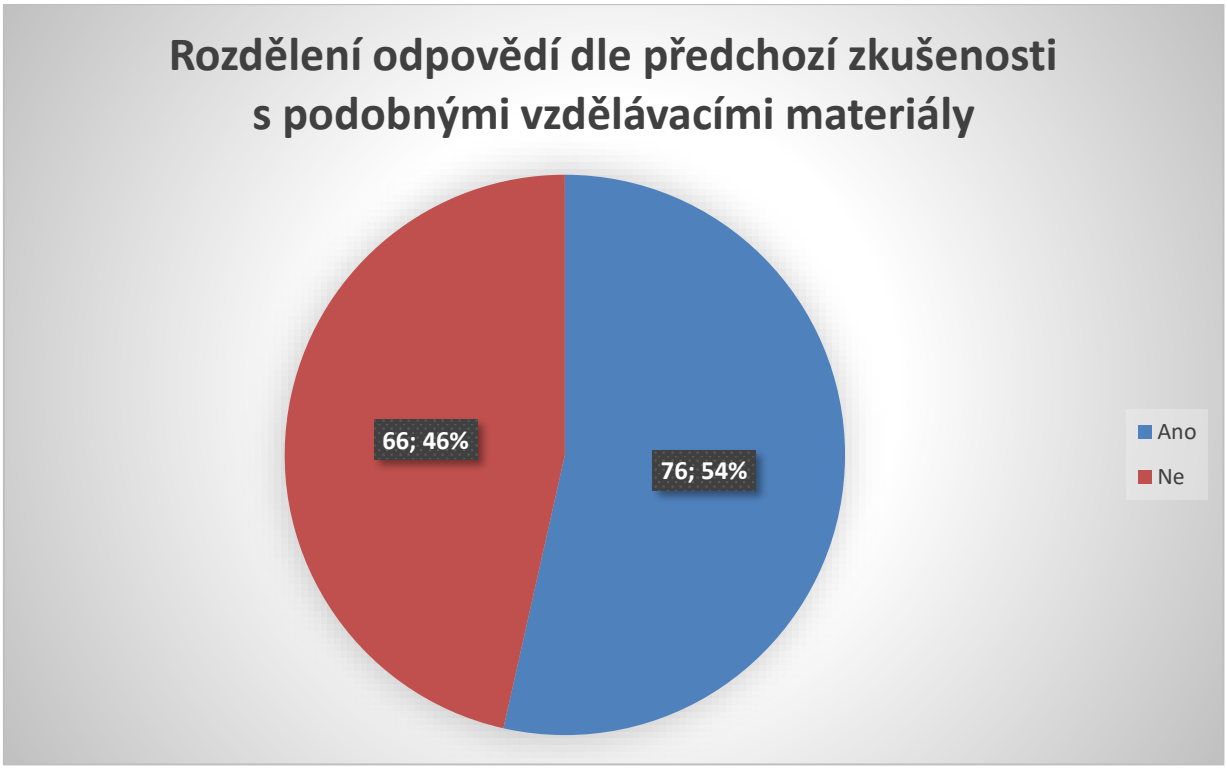
Graf 3 Odpovědi dle vzdělání (Zdroj: vlastní)

Další otázka se zabývala tím, jak často respondenti využívají internet. Většina odpověděla, že internet využívá na denní bázi.



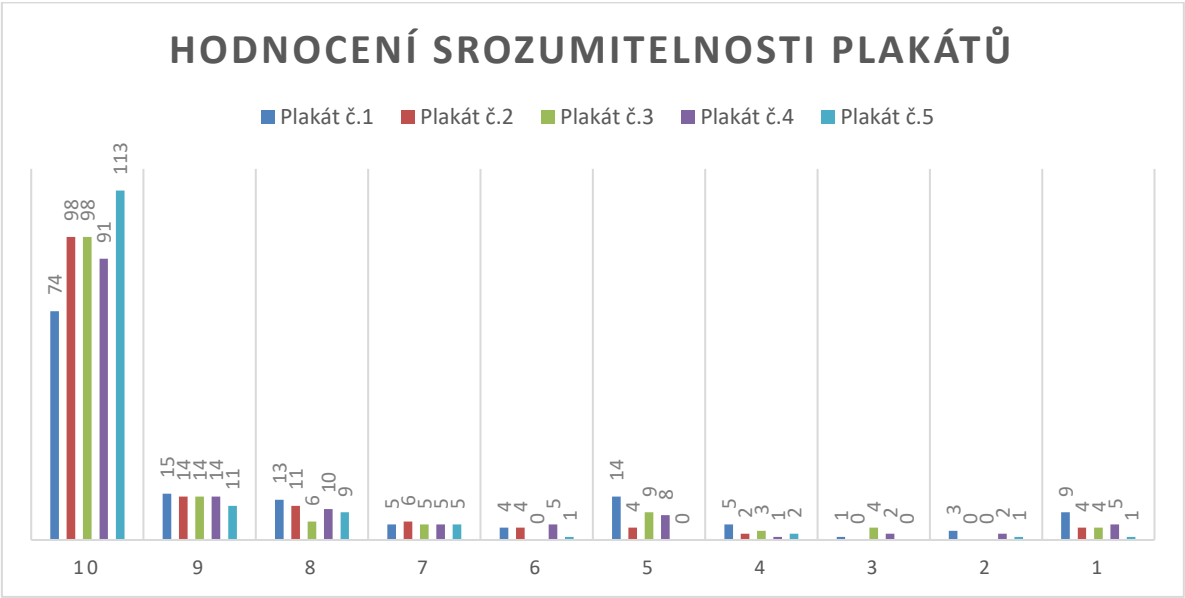
Graf 4 Odpovědi dle používání internetu (Zdroj: vlastní)

Poslední otázka tohoto segmentu dotazníku zjišťovala, zdali se respondenti již někdy setkali s podobnými materiály. Výsledkem je, že polovina se setkala s podobnými materiály a ta druhá nikoli.



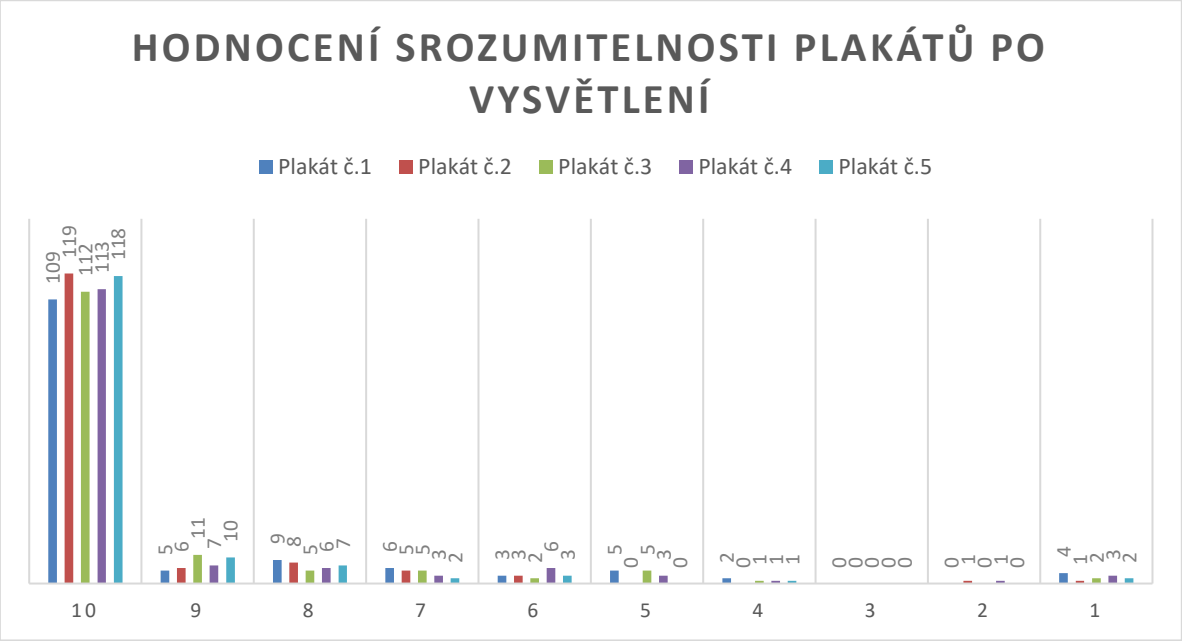
Graf 5 Odpovědi dle zkušeností se vzdělávacími materiály (Zdroj: vlastní)

Druhý segment dotazníku měl za úkol zjistit, jak respondenti plakátům rozumí. Zde hodnotili na škále od jedné do deseti, na jaké úrovni plakát chápou, přičemž deset je plně rozumím. v grafu můžeme vidět, že většina respondentů hodnotila plakáty jako plně srozumitelné.



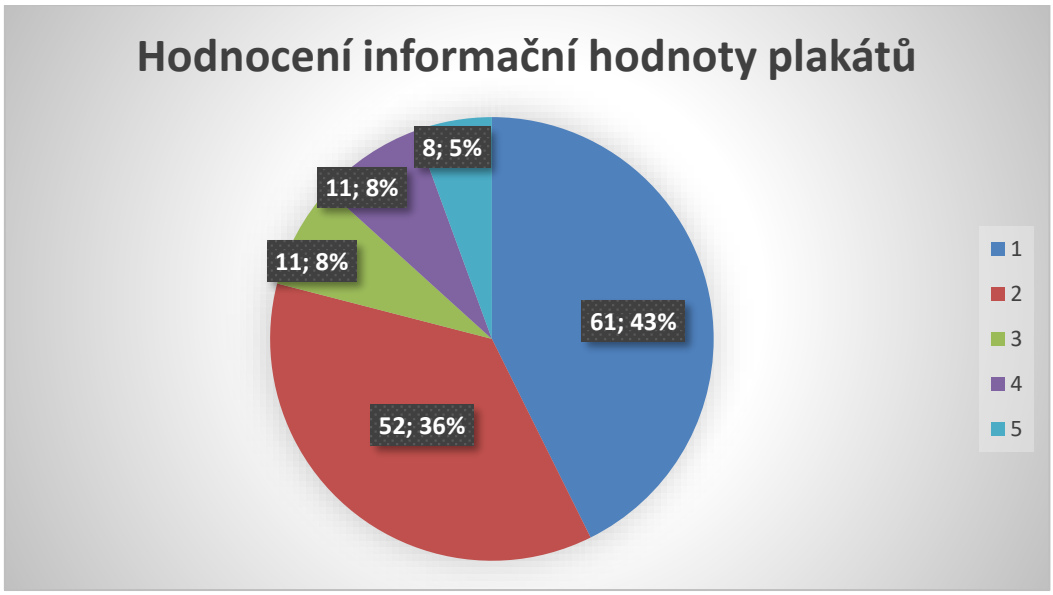
Graf 6 Hodnocení srozumitelnosti před vysvětlením (Zdroj: vlastní)

Aby si respondent mohl být jistý, že plakát opravdu pochopil následovala druhá polovina druhé části, kde ke každému plakátu bylo jednoduché vysvětlení. Po jeho přečtení byli respondenti opět dotázáni, jak rozumí jednotlivým plakátům nyní. Většina ohodnotila plakát vyšším nebo v případě předchozího hodnocení deset stejným hodnocením, jako u předchozí otázky. u některých se však i po vysvětlení hodnocení snížilo.

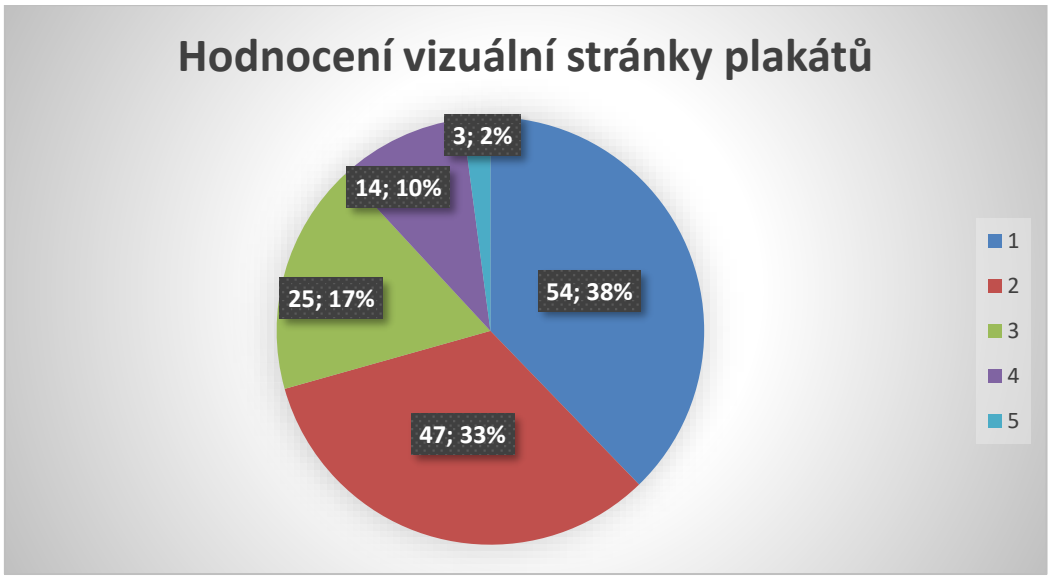


Graf 7 Hodnocení srozumitelnosti po vysvětlení (Zdroj: vlastní)

Poslední část byla zaměřena na zpětnou vazbu. Respondenti hodnotili na stupnici jedna až pět, jako při známkování ve škole, dvě kategorie, a to informační hodnotu plakátů a jejich vzhled.



Graf 8 Hodnocení informační hodnoty plakátů (Zdroj: vlastní)



Graf 9 Hodnocení vzhledu plakátů (Zdroj: vlastní)

4.2 ZPĚTNÁ VAZBA

V rámci dotazníku měli respondenti možnost zanechat zpětnou vazbu. Většině respondentů (93 %) se plakáty líbily. Hodnotili kladně jak vizuální stránku, tak i informační hodnotu plakátů. Našli se však i tací, kterým se na plakátech něco nelíbilo. Celkem deset respondentů ve zpětné vazbě nějakým způsobem záporně hodnotilo ať už vzhled, či informační hodnotu plakátů. Jejich kritika nebyla konstruktivní. Nebylo z ní možno poznat, co konkrétně je na plakátech podle nich špatně. Celkově je vidět, že záporné odpovědi jsou méně časté se zvyšujícím se věkem. Pouze dvě respondentky měly konkrétní připomínky k plakátům. První měla připomínku, že ne všichni odhalí špatný pravopis u plakátu číslo pět Rajfajzn bank, ale právě podvodníci spoléhají na to, že si lidé těchto drobných detailů nevšimnou. Plakát je podle této skutečnosti záměrně navržen tak, aby nešlo změnu na první pohled v názvu a logu jednoduše poznat. Druhá konkrétnější odpověď se vztahovala k plakátu číslo jedna. Respondentce připadá, že by nesmazatelná informace měla být frázována naléhavěji například použitím slova zloděj. Toto pro srozumitelnost plakátu není nutné, jelikož důležitější je informace o nesmazatelnosti dat z internetu a informace může být jakákoliv. Skandálnější verze informace na tabuli by mohla odvádět pozornost od zamýšleného sdělení.

4.3 PROBLÉMY S DOTAZNÍKEM

U dotazníku se vyskytly určité problémy, a to jak s distribucí, tak s pochopením zadání u některých respondentů. První problém se naskytl na Univerzitě třetího věku, kdy jsem podcenil časovou náročnost spojenou s rozesláním dotazníku. Toto se ale vyřešilo včas a dotazník se dostal ke všem zamýšleným respondentům.

V průběhu vyhodnocování odpovědí se ukázalo, že několik respondentů neporozumělo zadání, tak jak jej autor zamýšlel. Pro omezení nedostatků mohl být v dotazníku uveden příklad jednoho z původních plakátů (včetně krátkého vysvětlení), kterými jsou plakáty inspirovány. Dále by v otázkách na zpětnou vazbu mohla být použita vhodnější formulace, která by respondenty lépe nabádala ke zhodnocení, například, jak jsou plakáty srozumitelné pro seniory, jelikož si někteří v zadání nevšimli, pro jakou věkovou skupinu jsou plakáty určeny.

4.4 VYVOZENÍ ZÁVĚRŮ

Plakáty byly obecně přijaty kladně. Podle hodnocení byly srozumitelné, pochopitelné, jasné a výstižné. Lidem se líbila jejich barevnost, názornost a jednoduchá kresba, stejně tak jako jednoduché texty. Senioři ocenili neotřelý a vtipný nápad, který upozorňuje na rizika, která číhají na internetu. Také by přivítali vzdělávací materiály, zaměřující se na podobnou tématiku, jako jsou například podvodné telefonáty a SMS, bazarové podvody a další plakáty týkající se bezpečnosti na internetu.

Jedna z respondentek, která jako jediná uvedla, že internet používá méně než jednou týdně, vnímala plakáty srozumitelněji až na základě vysvětlení. Pro možnost dalšího výzkumu by bylo zajímavé, mít více respondentů, kteří používají internet méně často. Obecně by se dalo vyvodit, že malé množství respondentů z určitých skupin a celkově malé množství odpovědí zamezuje dostatečně vypovídající analýze spojitostí například mezi vzděláním a porozuměním plakátů.

Z obdržené zpětné vazby je zřejmé, že plakáty by se nejlépe uplatnily jako doprovodný materiál k nějakému vzdělávacímu kurzu o internetové bezpečnosti. Mohly by být také distribuovány v rámci komunit seniorů, vzdělávacích institucí a dalších relevantních organizací.

ZÁVĚR

V rámci této bakalářské práce byly vytvořeny vzdělávací plakáty zaměřené na počítačovou bezpečnost pro seniory, které jsou navrženy tak, aby byly srozumitelné, jasné a praktické. Design a obsah plakátů byly vytvořeny s ohledem na potřeby a preference seniorů, což zahrnuje jednoduchý jazyk, ilustrace a konkrétní rady. Jsou inspirované dobovými úrazovými plakáty ESČ, které byly vybrány pro atraktivnější vzhled pro cílovou skupinu. Plakáty byly úspěšně testovány s reálnými účastníky, kteří pozitivně hodnotili jejich srozumitelnost a užitečnost.

Testování plakátů s cílovou skupinou seniorů bylo úspěšné a poskytlo důležité poznatky o jejich účinnosti. Většina účastníků po testování projevila zvýšené znalosti a povědomí o počítačové bezpečnosti. Kvalitativní zpětná vazba účastníků přispěla k identifikaci silných a slabých stránek plakátů.

Vzhledem k dynamické povaze kybernetických hrozeb by měly být vzdělávací materiály průběžně aktualizovány a přizpůsobeny aktuálním trendům a výzvám.

Tato bakalářská práce představuje cenný příspěvek v oblasti vzdělávání seniorů, týkající se počítačové bezpečnosti a ukazuje potenciál vzdělávacích plakátů jako účinného nástroje pro zlepšení kybernetické bezpečnosti této cílové skupiny.

RESUMÉ

Tato bakalářská práce se zaměřuje na vytvoření a testování účinnosti sady vzdělávacích plakátů na téma počítačová bezpečnost pro seniory, které jsou navrženy speciálně pro ně. Cílem práce bylo vytvořit vzdělávací materiál, pomáhající seniorům zlepšit své povědomí o kybernetických hrozbách a ochranných opatřeních.

První část práce se soustředila na analýzu potřeb cílové skupiny, přičemž byly identifikovány nedostatky ve znalostech seniorů týkajících se počítačové bezpečnosti. Na základě této analýzy byly navrženy plakáty, které zahrnují jasné ilustrace, jednoduchý jazyk a konkrétní rady.

Následující kroky zahrnovaly testování plakátů s reálnými účastníky, tj. seniory. Testování prokázalo, že plakáty jsou účinným nástrojem pro zvyšování znalostí a povědomí o počítačové bezpečnosti u seniorů. Účastníci testování projevili zvýšené povědomí a pozitivně hodnotili srozumitelnost a užitečnost plakátů.

Závěr práce shrnuje klíčové závěry a doporučení pro budoucnost, včetně rozšíření distribuce vzdělávacích plakátů mezi seniory a rozvoje dalšího vzdělávacího materiálu v oblasti počítačové bezpečnosti.

RESUME

This bachelor's thesis focuses on creating and testing the effectiveness of a set of educational posters on the topic of computer security for seniors, designed specifically for them. The goal of the work was to create educational material that would help seniors improve their awareness of cyber threats and protective measures.

The first part of the work focused on the analysis of the needs of the target group, while deficiencies in the knowledge of seniors regarding computer security were identified. Based on this analysis, posters were designed that include clear illustrations, simple language and concrete advice.

The next steps involved testing the posters with real participants, i.e. seniors. Testing has shown that posters are an effective tool for increasing computer security knowledge and awareness among seniors. Test participants showed increased awareness and positively evaluated the comprehensibility and usefulness of the posters.

The conclusion of the thesis summarizes the key conclusions and recommendations for the future, including the expansion of the distribution of educational posters among seniors and the development of additional educational material in the field of computer security.

SEZNAM LITERATURY

[1] TURBONET S.R.O. *Co je to internet a jak vlastně funguje?* [online]. [cit. 2024-04-20]. Dostupné z: https://turbonet.cz/odpovedi-internetove-pripojeni/co-je-to-internet-a-jak-vlastne-funguje

[2] CZ.NIC, Z. S. P. O. *Historie internetu* [online]. [cit. 2024-04-21]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/

[3] INTERNET INFO, S.R.O. *Stručná historie emailu* [online]. [cit. 2024-04-21]. Dostupné z: https://www.cnews.cz/clanky/strucna-historie-emailu-uz-40-let-si-posilame-pocitacove-dopisy/

[4] WIKIPEDIA ORG. *Dějiny internetu* [online]. [cit. 2024-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/D%C4%9Bjiny_internetu

[5] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[6] KERNIGHAN, Brian W. *Jak porozumět digitálnímu světu: vše, co potřebujete vědět o internetu, bezpečnosti a soukromí.* Přeložil Petr HOLČÁK. Zip. Praha: Argo, 2019. ISBN 978-80-7363-903-7.

[7] ITNETWORK S.R.O. *Média fyzické vrstvy* [online]. [cit. 2024-04-20]. Dostupné z: https://www.itnetwork.cz/site/zaklady/site-media-fyzicke-vrstvy

[8] ITNETWORK S.R.O. *Typy síťových zařízení* [online]. [cit. 2024-04-20]. Dostupné z: https://www.itnetwork.cz/site/zaklady/site-typy-sitovych-zarizeni

[9] WIKIPEDIA ORG. *Datové centrum* [online]. [cit. 2024-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/Datov%C3%A9_centrum

[10] WIKIPEDIA ORG. *Poskytovatel internetového připojení* [online]. [cit. 2024-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/Poskytovatel_internetov%C3%A9ho_p%C5%99ipojen%C3%AD

[11] GOOGLE.COM. PaaS vs. IaaS vs. SaaS vs. CaaS: How are they different? [online]. [cit. 2024-04-20]. Dostupné z: https://cloud.google.com/learn/paas-vs-iaas-vs-saas

[12] MOZILLA CORPORATION. *Co je webový prohlížeč?* [online]. [cit. 2024-04-20]. Dostupné z: https://www.mozilla.org/cs/firefox/browsers/what-is-a-browser/

[13] SPIKE, INC. *Mail vs Instant Messaging - What's the Difference?* [online]. [cit. 2024-04-20]. Dostupné z: https://www.spikenow.com/blog/conversational-email/email-vs-instant-messaging-whats-the-difference/

[14] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[15] WIKIPEDIA ORG. *Streaming* [online]. [cit. 2024-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/Streaming

[16] WISE PAYMENTS LIMITED. *Co je e-commerce* [online]. [cit. 2024-04-20]. Dostupné z: https://wise.com/cz/blog/e-commerce

[17] PETROWSKI, Thorsten a KURKA, Tomáš. *Bezpečí na internetu: pro všechny*. Tajemství. Liberec: Dialog, knižní velkoobchod a nakladatelství, 2014. ISBN 978-80-7424-066-9.

[18] ECONOMIA, A.S. SIEM: *Bezpečnost pod kontrolou* [online]. [cit. 2024-04-20]. Dostupné z: https://hn.cz/c1-65283860-siem-bezpecnost-pod-kontrolou

[19] DVS. *Senioři na internetu* [online]. [cit. 2024-04-20]. Dostupné z: https://www.dvs.cz/clanek.asp?id=6951040

[20] EUROPE - ELECTRONEX S.R.O. *Senioři a IT - nejčastější problémy* [online]. [cit. 2024-04-20]. Dostupné z: https://www.eplovna.cz/blog/seniori-a-it-nejcastejsi-problemy/

[21] WIKIPEDIA ORG. *Sociální bublina* [online]. [cit. 2024-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_bublina

[22] PRO PRARODIČE S.R.O. *Nekalé praktiky: Proč jsou nebezpečné zejména pro seniory, jak je poznat a jak se jim bránit* [online]. [cit. 2024-04-21]. Dostupné z: https://www.proprarodice.cz/c/nekale-praktiky-proc-jsou-nebezpecne-zejmena-pro-seniory-jak-je-poznat-a-jak-se-jim-branit-527

[23] GODAROVÁ, Jana a Vlastimil BERAN, 2017. *Manuál volnočasových aktivit seniorů*. Vyd. 1. Praha: VÚPSV. 91 s. ISBN 978-80-7416-318-0.

[24] CHRÁSKA, Miroslav. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. 2., aktualizované vydání. Pedagogika. Praha: Grada, 2016. ISBN 978-80-247-5326-3.

[25] ČEZ. *HISTORICKÝ OSVĚTOVÝ PLAKÁT Č. 4* [online]. [cit. 2024-04-20]. Dostupné z: https://www.svetenergie.cz/cz/stahuj-zdarma/tiskoviny/plakaty/historicky-osvetovy-plakat-c-4

[26] CREATIVE COMMONS. *Creative Commons licence* [online]. [cit. 2024-04-20]. Dostupné z: https://chooser-beta.creativecommons.org/

[27] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[28] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Průvodce. Praha: Grada Publishing, 2015. ISBN 978-80-247-5453-6.

[29] POLICIE ČR. *Kyberkriminalita* [online]. [cit. 2024-02-11]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

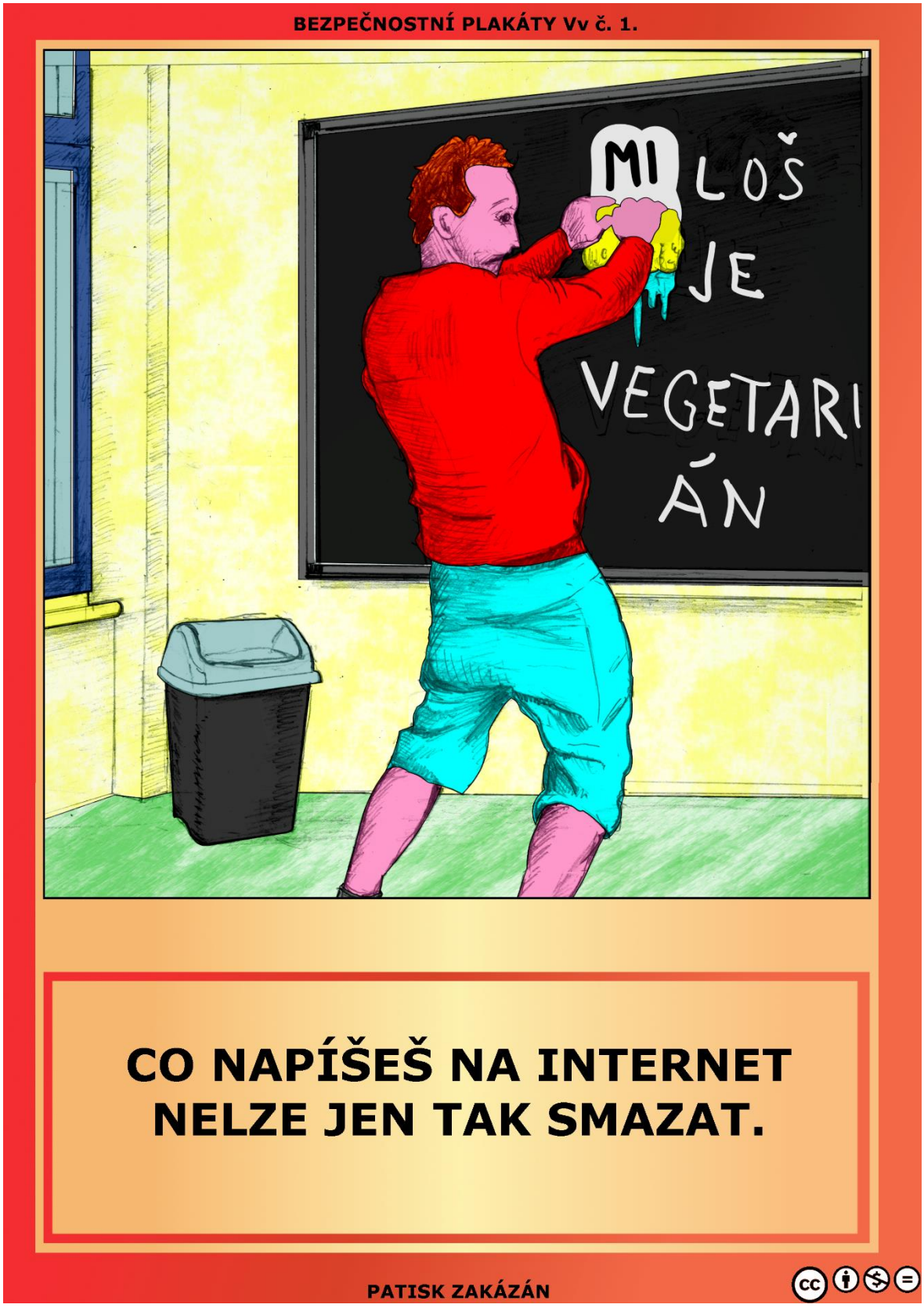
[30] GORDIC SPOL. s R. O. *Kybernetická bezpečnost* [online]. [cit. 2024-02-11]. Dostupné z: https://kybez.cz/

[31] ČESKÁ BANKOVNÍ ASOCIACE. *Kybertest* [online]. [cit. 2024-02-11]. Dostupné z: https://www.kybertest.cz/

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ A DIAGRAMŮ

PŘÍLOHY

Příloha I



Příloha II


BEZPEČNOSTNÍ PLAKÁTY Vv č. 2.
SLABÝM HESLEM OTEVÍRÁŠ OKNO NEZVANÝM HOSTŮM.
PATISK ZAKÁZÁN

Příloha III


BEZPEČNOSTNÍ PLAKÁTY Vv č. 3.
INFORMACE MOHOU BÝT ZKRESLENY. NEVĚŘ VŠEMU CO SI PŘEČTEŠ NA INTERNETU.
PATISK ZAKÁZÁN

Příloha IV


BEZPEČNOSTNÍ PLAKÁTY Vv č. 4.
IDENTITA NA INTERNETU JE POMÍJIVÁ. NESEDEJ NA LEP PODVODNÍKŮM.
PATISK ZAKÁZÁN

Příloha V


BEZPEČNOSTNÍ PLAKÁTY Vv č. 5.
Rajfajzn
BANK
ZKONTROLUJ ZDA-LI JSI NA SPRÁVNÉ ADRESE. NĚKTERÉ STRÁNKY SE SNAŽÍ VYPADAT JAKO INTERNETOVÉ BANKOVNICTVÍ A ZÍSKAT TVÉ CITLIVÉ ÚDAJE.
PATISK ZAKÁZÁN

Příloha VI

Já, MgA. Petr Filip prohlašuji, že ilustrace byly vytvořeny pro potřeby plakátů vytvořených v této bakalářské práci a uděluji souhlas s jejich použitím.

Dne: 22. 4. 2024 Stýskaly

Podpis:

Příloha VII

Odkaz na dotazník:

https://forms.gle/HB6fo3h3aRBi3vC16