UNIVERZITA KARLOVA

Filozofická fakulta

Katedra psychologie

Rigorózní práce

Mgr. Nikol Kopáňková

Bezpečnost na internetu: Vnímání bezpečnosti na internetu u respondentů ve střední dospělosti

Online safety: Perception of online safety among respondents in middle adulthood

Praha 2024

Poděkování

Na tomto místě bych ráda poděkovala Mgr. Tereze Hannemann, Ph.D. za dlouhodobou spolupráci, podporu a vedení.

Dále bych ráda poděkovala PhDr. Ivě Štětovské za vedení diplomové práce, vždy pozitivní přístup a cenné rady při vypracování práce.

Poděkování patří také PhDr. Jiřímu Vinopalovi, Ph.D. za konzultace a cenné rady při přípravě znění dotazníku. Dále za poskytnutí prostředků pro realizaci výzkumu v rámci programu Specifického vysokoškolského výzkumu „Adaptace aktérů a institucí na vývoj současné společnosti“ (SVV-Adakin) 2022.

Velké poděkování patří mé rodině. Hlavně mému partnerovi a dceři, díky kterým je pro mě každý den radostí.

Prohlášení

Prohlašuji, že jsem rigorózní práci vypracovala samostatně, že jsem řádně citovala všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 30.8.2024

Nikol Kopáňková

Abstrakt

Kopáňková, N. (2021). *Bezpečnost a chování na internetu u dospělých se základním vzděláním*. Diplomová práce. Univerzita Karlova. Filozofická fakulta.

Předložená práce se zabývá vnímáním bezpečnosti na internetu u respondentů ve střední dospělosti (35-60 let) v souvislosti s Protekčně Motivační Teorií (PMT). Bezpečnost na internetu je rozdělena do tří složek: sociální (osobní), technické a institucionální. Toto dělení vychází z výsledků výzkumu diplomové práce autorky. Mezi vybrané konstrukty PMT je zařazena vnímaná pravděpodobnost výskytu hrozby, strach z potenciální hrozny a vnímané self-efficacy respondentů. Dále bylo sledováno, zda gender a vzdělání respondentů souvisí s vnímanou závažností bezpečnosti na internetu.

V rámci výzkumu bylo realizováno CATI dotazníkové šetření s reprezentativním souborem (n = 700) respondentů. Pro analýzu dat byl využit výpočet korelace pomocí Pearsonova a Spearmanova testu nezávislosti a chí kvadrát test nezávislosti.

Výsledky ukazují, že je možné sledovat slabé korelace mezi vnímanou závažností sociální (osobní) bezpečnosti na internetu a vnímaným strachem z hrozby a vnímanou pravděpodobností vzniku hrozby. Dále existuje přímá závislost o slabé intenzitě mezi technickou bezpečností na internetu a vnímaným self-efficacy. Mezi institucionální bezpečností a strachem z potenciální hrozby i vnímanou pravděpodobností vzniku hrozby existuje přímá závislost o slabé intenzitě. Dále bylo prokázáno, že ženy vnímají jako závažnější sociální (osobní) složku bezpečnosti na internetu, zatímco muži technickou. Dosažený stupeň vzdělání se ukazuje jako nesignifikantní při vnímání závažnosti bezpečnosti na internetu.

Předložené výsledky nabízí nové poznatky k dělení bezpečnosti na internetu. Výsledky mohou být využity při tvorbě intervenčních programů či dalších výzkumných šetření.

Klíčová slova: *Bezpečnost na internetu; Protekčně motivační teorie; Střední dospělost; Korelační studie*

Abstract

Kopáňková, N. (2021). *Online safety and behavior in adults with primary education*. Diploma thesis. Charles University. Faculty of Arts.

The present thesis examines the perceptions of online safety among middle adult respondents (35-60 years old) in the context of the Protection Motivation Theory (PMT). Internet safety is divided into three components: social (personal), technical, and institutional. This division is based on the results of the author's diploma thesis research. The selected constructs of PMT include perceived likelihood of threat research, fear of potential threat, and perceived self-efficacy of respondents. It was also examined whether gender and education of the respondents were related to the perceived severity of online safety.

A CATI questionnaire survey was conducted with a representative sample of (n = 700) respondents. Pearson and Spearman's correlation and chi-square test of independence were used to analyse the data.

The results show that weak correlations can be observed between perceived severity of social (personal) safety on the Internet and perceived fear of threat and perceived likelihood of threat. Furthermore, there is a direct relationship of weak intensity between technical safety on the Internet and perceived self-efficacy. There is a direct weak-intensity relationship between institutional security and both fear of potential threat and perceived likelihood of threat. It was also shown that women perceive the social (personal) component of online safety as more important, while men perceive the technical component as more important. Educational attainment is shown to be non-significant in the perceived severity of Internet safety.

The presented results offer new insights into the division of Internet safety. The results can be used in the design of intervention programs or other research investigations.

Key words: *Internet safety; Protection-motivation theory; Middle adulthood; Correlational study*

Obsah

Seznam zkratek

APA	American Psychological Association
FOMO	Fear Of Missing Out
PMT	Protection Motivation Theory

Úvod

Předložená rigorózní práce navazuje na diplomovou práci autorky (Kopáňková, 2021) s názvem „Bezpečnost a chování na internetu u dospělých se základním vzděláním“. Rigorózní práce dále rozpracovává myšlenky diplomové práce a zároveň nabízí rozšiřující kvantitativní výzkum, který navazuje na předchozí kvalitativní výzkum. V této práci je také blíže rozpracována Protekčně Motivační Teorie (PMT), kdy prvky této teorie jsou použity i ve výzkumném dotazníku.

Bezpečnost na internetu se ukazuje být velmi komplexním fenoménem, na který neexistuje jednotný pohled. V diplomové práci bylo nastíněno, že uživatelé internetu mohou bezpečnost vnímat v rámci třech složek: sociální (osobní), technické a institucionální, kdy každá z těchto složek zahrnuje jiný typ obav, hrozeb a situací, které nejsou uživatelům internetu komfortní. Do oblasti bezpečnosti na internetu autorka práce řadí také prožívaný pocit bezpečí, ne pouze zabezpečení našich dat. Internet se stal neodmyslitelnou součástí každodenního života, i když pro někoho více a pro někoho méně. Internet zasahuje nejen do pracovní či studijní sféry života, ale hraje významnou roli i v životě osobním, jelikož se stává častým způsobem komunikace.

Práce se zaměřuje na dospělé ve střední dospělosti, kdy tato skupina byla vymezena věkem 35-60 let. Práce začíná kapitolou, která se věnuje popisu generace střední dospělosti. Nabízí přehled tradičních i moderních vývojových teorií a je zde kladen důraz na charakteristiku této generace na internetu a mezigenerační srovnání. Navazuje kapitola, která se zaměřuje na psychologické fenomény spojené s užíváním internetu, především na komunikaci na internetu, vyhledávání informací, internetový trolling nebo sociální srovnávání. Tyto psychologické fenomény mají výrazný vliv na prožívání jedince a jsou úzce spojeny s pocitem bezpečí na internetu. Další kapitoly se týkají bezpečnosti na internetu, nejčastějších obav uživatelů internetu, vnímání bezpečnosti a strategií ochrany na internetu. Teoretická část je zakončena kapitolou o protekčně motivační teorii a provázání této teorie s bezpečností na internetu.

Výzkumná část zahrnuje reprezentativní dotazníkové šetření (n = 700), které sleduje vliv zvolených prvků PMT na vnímání třech složek bezpečnosti na internetu u dospělých ve střední dospělosti (35-60 let). Dále je cílem prozkoumat souvislost genderu a vzdělání s vnímáním bezpečnosti na internetu u dospělých ve střední dospělosti (35-60 let).

V rigorózní práci autorka přidává, oproti diplomové práci, rozšíření a úpravu jak v teoretické, tak ve výzkumné části. V teoretické části jsou upraveny kapitoly týkající se charakteristiky

střední dospělosti, dále jsou mezi vybrané psychologické fenomény přidány další dva fenomény – internetový trolling a sociální srovnávání. Byla upravena kapitola týkající se popisu bezpečnosti na internetu, kde byly přidány novější vědecké poznatky a byla rozšířena o podkapitolu věnující se nejčastějším obavám, které prožívají uživatelé internetu. Dále byla přidána kapitola rozšiřující poznatky PMT.

Empirická část rigorózní práce je zcela změněna oproti diplomové práci, i když výzkum přímo navazuje na předchozí kvalitativní výzkum. V empirické části je v kapitole *5. Výchozí kvalitativní výzkum* popsán výzkum z diplomové práce pro poskytnutí lepšího kontextu navazujícího kvantitativního výzkumu.

Práce čerpá z českých i zahraničních zdrojů, kdy většina zdrojů je zahraničních. V rigorózní práci je citováno podle normy APA (2020).

Teoretická část

O bezpečnosti online se často hovoří v souvislosti s vývojem digitálních technologií a internetu, které se staly nedílnou součástí našeho každodenního života. Velké množství zaměstnání, vzdělávání a volnočasových aktivit se přesunulo na internet, zejména po celosvětové pandemii COVID-19. Počet uživatelů internetu na celém světě vzrostl mezi lety 2000 a 2019 o 1 167 %, zatímco v Evropě vzrostl počet uživatelů internetu mezi lety 2000 a 2020 o 601,3 % (MMG, 2020). Rychlý růst počtu uživatelů internetu vedl k nárůstu různých rizik, což zvýšilo význam bezpečnosti na internetu. Je třeba poznamenat, že chápání online bezpečnosti se u jednotlivých osob liší a je také značně závislé na kontextu (Quan-Haase a Ho, 2019). V dnešní době je také velmi důležité zapojit se do digitálního světa a umět se v něm orientovat. Připojení k digitálnímu světu přináší nové příležitosti, nabídky a informace. Pohyb mimo digitální sféru může v dnešní době přispět i k určitému sociálnímu vyloučení (Ragnedda, 2018), které může způsobovat úzkost a zhoršovat celkový well-being. Na druhou stranu existuje mnoho studií, které ukazují, že digitální pohoda je často prožívána prostřednictvím digitálního odpojení a digitálního detoxu (Ngyuen, 2021). Na jedné straně by tedy uživatelé měli být připojeni, aby nedocházelo k pocitu sociálního vyloučeni, ale také by neměli digitální technologie používat příliš často. Dále se ukazuje, že digitální kompetence jsou jednou ze základních dovedností pro orientaci v dnešní společnosti. Podle EU je jednou z pěti nejdůležitějších digitálních dovedností právě pochopení a zvládnutí online bezpečnosti (Vuorikari et al., 2022).

Teoretická část je věnována kapitolám, ve kterých je kladen důraz na bližší popis generace střední dospělosti a vybraných psychologických fenoménu spojených s užíváním internetu. Při psaní práce autorka narazila na mírné nuance mezi pojmy bezpečnost na internetu a bezpečí na internetu (v angličtině by bylo možné přeložit jako „online security“ vs. „online safety“). V práci je kladen důraz jak na bezpečnost, tak i na pocit bezpečí, čímž je tato práce odlišná od jiných výzkumů, které se na bezpečnost na internetu zaměřují. Některé popsané fenomény se tedy nepojí pouze s bezpečností na internetu, pod kterým si můžeme představit spíše zabezpečení počítače a dat, ale souvisí především s osobním pocitem bezpečí na internetu, jak nás všechny jako uživatele ovlivňuje čas trávený na internetu i v „reálném“ životě. Jak je popsáno výše, v dnešní době se většinou očekává, že jsme připojeni k internetu (někdy se očekává dokonce neustálé připojení), jsou kladeny nároky na určitou úroveň dovedností a internet se stává i nedílnou součástí našich osobních životů, což je také důvod, proč je práce důležitá i z pohledu oboru psychologie.

1. Střední dospělost

Období střední dospělosti je velmi rozmanité období, které bylo dřívějšími výzkumy a vývojovými teoriemi částečně opomíjeno, protože se mělo za to, že je to období relativně stabilní. Zároveň v oblasti výzkumů týkajících se bezpečnosti na internetu je skupina respondentů ve střední dospělosti často opomíjenou skupinou. V současné době je na internetu více zastoupena skupina mladších generací a většina výzkumů je spojena s dětmi a dospívajícími. Na druhou stranu se stále zvyšuje počet dospělých, kteří využívají internet, což může způsobit jejich budoucí viktimizaci a bezpečnost na internetu je tak důležitým tématem pro všechny generace (White, Gummerum, Wood & Hanoch, 2017). V následující kapitole bude blíže popsána generace střední dospělosti a výběr vývojových teorií, pro vytvoření kontextu práce a pochopení této generace i v jejich chování na internetu.

K periodizacím celoživotního vývoje člověka, které dospělost popisují blíže, je možné zařadit vícero autorů a jejich periodizace vývoje. Dle V. Příhody (1977) je věk mezi 35-60 lety vymezen následovně: mezi 30-45 rokem je typická životní stabilizace a vyvrcholením a mezi 45-60 lety tzv. interseniem. Jako další je možné zmínit periodizaci dle P. Říčana (2006), který toto období dělí na třicáté (30-40), čtyřicáté (40-50) a padesáté roky (50-60). Novější periodizaci uvádí autoři R.V. Kail a J. Cavanaugh (2017), kteří označují mladou dospělost od 20-40 let a střední dospělost právě od 40-60 let. Přesněji vymezit věkové rozmezí střední dospělosti je náročné a často se vymezení liší dle autora. Nejčastěji je střední dospělost uváděna mezi 30-60 lety (např. Merriam & Mullins, 1981; Blatný, 2017), další výzkumy odkazují spíše na věk mezi 40-60 lety (např. Willis & Martin, 2005). To je způsobeno především tím, že období střední dospělosti je v současnosti velmi různorodé, subjektivní a nenormativní. Někteří jedinci jsou v tomto období rodiči, jiní už prarodiči. Různě se dodržují tzv. sociální hodiny (různá organizace života dle požadavků společnosti) a celkově se jedinec řídí spíše prožitými životními událostmi (Blatný, 2017).

1.1. Tradiční vývojové teorie popisující střední dospělost

V minulosti bylo vytvořeno mnoho různých periodizací životního vývoje a souvisejících vývojových teorií. Starší vývojové teorie se zaměřují především na raný vývoj dítěte po pubertu/ adolescenci, ale další vývojová stádia již nepopisují. Z tradičních vývojových teorií je možné zmínit teorii psychosociálního vývoje E.H. Eriksona, který ve své známé teorii jako

jeden z prvních popsal vývoj člověka v průběhu celoživotního vývoje a popsal osm stádií vývoje člověka (1997). Jeho teorie se zaměřuje především na psychosociální vývoj, a i když vychází z S. Freudovy psychoanalýzy, byl ovlivněn také svým zájmem o antropologii a etnologii. Ve své teorii se tedy nesoustředí jako S. Freud pouze na nejužší rodinu a psychosexuální vývoj, ale klade důraz na celkové sociální prostředí člověka, a právě na psychosociální aspekty ovlivňující vývoj jedince. Ve své teorii pracuje s tzv. psychosociálními konflikty, které jsou charakteristické pro jednotlivá období. Úkolem jedince je tyto konflikty překonat a získává tak dle E.H. Eriksona ctnost pro další vývoj.

Dospělost E.H. Erikson charakterizuje konfliktem mezi generativitou a stagnací. V tomto období dochází k předávání dosavadních zkušeností dalším generacím, a zásadní je tedy jakási péče o druhé, především péče o děti a zlepšování kvality jejich života. Generativitou je v pojetí E.H. Eriksona tvořivost, prokreativita a produktivita. Při neschopnosti naplňování péče o druhé může docházet ke stagnaci a v krajních případech také k zahlcení vlastní osobou, což E.H. Erikson označuje jako sebeabsorbci. Při překonání konfliktu právě mezi generativitou a stagnací je ctností péče o druhé (Erikson, 1997). E.H. Erikson toto období vymezuje jako součást střední a pozdní dospělosti. Období generativity vs. stagnace můžeme sledovat ale i v době mladší dospělosti, vzhledem k vývojovým úkolům tohoto období. E.H. Erikson tedy nemá jasně vymezené toto období věkem, ale jedná se o fázi, která může trvat i více než 30 let, a je to tedy nejdelší vývojové období (Erikson, 1997). Pro účely této práce je ale důležité si věk generace střední dospělosti vymezit konkrétně i věkovým rozmezím.

Další z vývojových teorií je *"Teorie vývojových úkolů"* R.J. Havinghursta ovlivněná antropologií, sociologií a pedagogikou (Millová, 2017). V každém životním období se dle této teorie objevuje vývojová úloha. Při splnění dochází ke spokojenosti a k posunu k dalšímu vývojovému období. V případě neúspěchu nastává celková nespokojenost, problémy se společností a s následujícími životními úkoly, což může připomínat pojetí vývoje dle E.H. Eriksona, které je zmíněno výše. Popisuje tři zdroje, ze kterých vývojové úkoly vychází: fyzické, sociální a kulturní faktory, osobní hodnoty a aspirace jedince. Jako střední věk vymezuje období mezi 30-60 lety. V tomto období dosahují jedinci vrcholu ve společnosti. Dospělí v tomto věku se dostávají do situace, kdy si jejich děti budují vlastní rodinu, role matky nebo otce tedy ustupuje do pozadí. S přibývajícím věkem dochází ke zpětnému hodnocení života a objevují se biologické změny související se stárnutím. Úkoly v tomto období tedy jsou pomáhat dospívajícím dětem, dosáhnout společenské zodpovědnosti, udržovat uspokojivý

výkon v zaměstnání, rozvíjet své volnočasové aktivity, rozvíjet partnerský vztah a přizpůsobovat se biologickým změnám. Zároveň také autor zmiňuje péči o stárnoucí rodiče (Havinghurts, 1972). To naznačuje pozdější označení této generace - tzv. sendvičová generace, což znamená, že na jedné straně se dospělí ve věku 30-60 let starají o své vlastní děti a zároveň o své rodiče (Blatný, 2017).

Teorii R.J. Havinghurtsa podrobili bližšímu zkoumání v roce 1981 S. Merriam a L. Mullins. Ve své dotazníkové studii se ptali celkem 540 respondentů na vnímanou důležitost a aktuálnost vývojových úkolů, které R.J. Havinghurts popisuje ve své teorii, konkrétně věkové kategorii střední dospělosti. Výzkumný soubor rozdělili dle věkových kategorií, přičemž skupinu střední dospělosti určili jako respondenty ve věku 35-59 let, kterých bylo celkem 180. Při popisu vývojových úkolů zjistili, že respondenti vnímali R.J. Havinghurtsovy vývojové úkoly jako všechny stejně závažné a aktuální, čímž tento soubor potvrdil jeho teorii. Zároveň z výzkumu vychází, že v tomto období života jsou na jedince kladeny různé nároky, které musí zvládnout a objevuje se tak více stresových faktorů (Merriam & Mullins, 1981).

1.2. Moderní vývojové teorie popisující střední dospělost

V průběhu 70. a 80. let 20. století začaly vznikat novější vývojové teorie, které zkoumaly vývoj nejen do dosažení fyziologické zralosti a dospělosti, ale zaměřily se na průběh vývoje v celé ontogenezi člověka. Zároveň se jedná o teorie, které již nepracují s jasně ohraničenými vývojovými stádii. Moderní teorie nahlíží na vývoj spíše z pohledu principů vývoje a adaptačních mechanismů. Společným cílem těchto teorií byla snaha popsat celoživotní vývoj jedince. Moderní vývojové teorie je možné rozdělit až na tři skupiny dle toho, jak pracují s adaptačními mechanismy. Jedná se o lifespanové modely, modely celoživotní dráhy a teorie vývojových systémů (Millová, 2017). Vznikla například teorie lifespanového vývoje (Baltes, Staudinger, Lindenberger, 1998), bioekologická teorie (Bronfebrenner, 2005), nebo teorie životní dráhy (např. Elder, 1998). Teorie spojují nejen psychologické, ale také sociologické a antropologické poznatky.

Lifespanové teorie vývoje vychází z psychologických konceptů jako je např. zvládání stresu, kontrola, adaptace nebo mechanismy, pomocí kterých dosahují jedinci svých cílů. V lifespanových teorií je kladen důraz také na sociální, historické a environmentální faktory. Jako jednu z lifespanových teorií vývoje je možné zmínit např. "*Lifespanové teorii vývoje"* P.B.

Baltese, v níž popsal pět úrovní teoretické analýzy, která postupuje od nejobecnější ke konkrétní:

1. Biologická a kulturně evoluční perspektiva (vnitřní a vnější aspekty vývoje)
2. Vyvažování zisků a ztrát při dosahování cílů
3. Metateoretické předpoklady o celoživotním vývoji
4. Selekce, optimalizace a kompenzace (SOC)
5. Lifespanová teorie ve specifických funkcích a oblastech: inteligence, osobnost, self.

P.B. Baltes popisuje vývoj člověka nejen z individuálního hlediska, ale zaměřuje se také na změny ve fyzickém a kulturním prostředí. Nejedná se tedy o čistě psychologickou teorii nebo přístup, ale kombinuje se zde sociologický a psychologický pohled. Zároveň vývoj popisuje jako proces adaptace na možné změny, které jsou ovlivněny jak raným vývojem jedince, tak závažnými situacemi, které mohou během života jedince nastat. Nepopisuje tedy tradiční periodizaci vývoje, nahlíží na vývoj každého jedince jako na jedinečný a neopakující se. Zároveň tuto jedinečnost vývoje popisuje pomocí třech vlivů: normativních, které jsou ovlivněny lidským věkem; normativních, které jsou ovlivněny historií a nenormativních životních událostí (Baltes, Staudinger & Lindenberger, 1998) P.B. Baltes jako jeden z prvních poukazuje na komplexnost vývoje, na důležitost integrace individuálního pohledu a společenských podmínek a prostředí, které jedince v jeho vývoji ovlivňují (Millová, 2017).

Čistě psychologicky orientovaná lifespanová teorie kontroly (Schulz & Heckhausen, 1996) pracuje s procesem kontroly a byla ovlivněna Baltesovou teorií lifespanu. Zásadní v této teorii je také proces **selekce, optimalizace a kompenzace**, které probíhají ve všech stádiích vývoje člověka. Selekce souvisí s výběrem cíle, optimalizace s oblastmi růstu (zlepšování schopností) a kompenzace reguluje možné ztráty v celkovém vývoji jedince (pomůcky k zapamatování).

Pomocí těchto tří procesů se lidé v průběhu svého vývoje učí novým dovednostem a zpracovávají možné životní změny (tranzice) (Millová, 2017). Déle je možné zmínit teorie životní dráhy, které reagují na množství psychologických teorií, které dle některých autorů dostatečně nepracují s vlivem okolí na vývoj jedince, tudíž je v těchto teoriích významnější sociologický pohled, který se zaměřuje právě i na okolí jedince. Často zmiňovaným autorem je např. G.H. Elder se svou *teorií celoživotního vývoje* (1986). V této teorii je kladen větší důraz právě na prostředí jedince při jeho vývoji. Hodnotí prostředí na dvou úrovních – makroúroveň a mikroúroveň. Makroúroveň zahrnuje vliv institucí – školy, pracovního prostředí a další.

Mikroúroveň souvisí s behaviorálním, biologickým a psychologickým prostředím. Celý vývoj je ale také ovlivněn vlastní aktivitou daného jedince. V teorii životní dráhy se nepracuje s konkrétními vývojovými stádii, ale počítá se s tím, že život jedince probíhá v určitých stádiích relativní stability a životních změn. G.H. Elder & J.Z. Giele (2009) proto popsali čtyři charakteristiky vývoje: sociální trasy, vývojové trajektorie, přechody (tranzice) a bod obratu.

Následně vznikla také *bioekologická teorie vývoje*, která nepracuje pouze s jedním prostředím, ve kterém se jedinec vyvíjí, ale popisuje různá prostředí a vztahy mezi nimi. Nejbližším systémem je *mikrosystém*, který zahrnuje rodinu, pracovní prostředí, školní prostředí a vrstevníky. V tomto systému jsou přímé vztahy s okolím. Dalším systémem je *mezosystém*, který je tvořen interakcemi mikrosystému (tzn. u dítěte například interakce mezi školou a rodinou, u dospělých například interakce mezi pracovním a rodinným prostředím). *Exosystém* je třetím popsaným systémem, který sice není přímo součástí života jedince, ale jeho vývoj nějakým způsobem ovlivňuje (pracovní prostředí rodičů, partnera apod.). Čtvrtým systémem je *makrosystém*, který je tvořen historickými a společenskými podmínkami, hodnotami a zákony, které zasahují do života jedince (Bronfenbrenner, 2005). Později byl do teorie přidán ještě pátý systém *chronosystém*, který je obsažen ve všech výše popsaných systémech. Souvisí především s možnými změnami a stabilitou okolí jedince (Bronfenbrenner, 2005).

Autor	**Věk/Název teorie**	**Charakteristika**
E. Erikson	"střední dospělost" (30-64 let)	**generativita vs. stagnace**
R.J. Havinghurts	**30-60 let**	**Vývojové úkoly - pomáhat dospívajícím dětem, dosáhnout dospělé společenské zodpovědnosti, udržovat uspokojivý výkon v zaměstnání, rozvíjet své volnočasové aktivity, rozvíjet partnerský vztah a přizpůsobovat se biologickým změnám**
V. Příhoda	**35-45 let, 45-60 let**	30-45 rokem je typická životní stabilizace a vyvrcholením a mezi 45-60 lety tzv. interseniem.
R.V. Kail & J. Cavanaugh	**40-60 let**	

P. Říčan	**30.,(30-40 let) 40.(40-50 let) a 50.(50-60 let) roky**	
G.H. Elder	Teorie celoživotního vývoje	**Vliv prostředí - makroúroveň a mikroúroveň**
U. Bronfenbrenner	Bioekologická teorie vývoje	**Vliv prostředí - mikrosystém, mezosystém, exosystém a makrosystém**
P.B. Baltes	Lifespanová teorie vývoje	• **Biologická a kulturně evoluční perspektiva** • **Vyvažování zisků a ztrát při dosahování cílů** • Metateoretické předpoklady o celoživotním vývoji • Selekce, optimalizace a kompenzace (SOC) Lifespanová teorie ve specifických funkcích a oblastech: inteligence, osobnost, self.

Tabulka 1. – Přehled vývojových teorií

Pro větší přehlednost zmíněných teorií vývoje byla vytvořena *Tabulku 1. - Přehled vývojových teorií*. V tabulce je vždy v případě tradičních vývojových teorií vedle jména autora uvedeno, jakým věkovým rozmezím autor popisuje období střední dospělosti. Vedle autorů novějších vývojových teorií je vždy uveden název jejich teorie. Následně je zařazen stručný popis a charakteristika teorií. V tabulce je tučně vyznačeno to, co je považováno za esenciální při realizaci této rigorózní práce a zároveň co bylo důležité také při realizaci diplomové práce autorky, na kterou tato práce blíže navazuje.

Věkové rozmezí střední dospělosti je dle syntézy jednotlivých teorií určeno mezi 35-60 lety, jelikož se jedná o kompromis mezi tradičními a moderními vývojovými teoriemi. Zároveň se jedná o kompromis toho, s jakým věkovým rozpětím pracují starší i současné výzkumy. Jak ale bylo naznačeno výše, období střední dospělosti je velmi individuální a rozmanité. Pro tuto práci navrhuje autorka popsat období střední dospělosti pomocí specifických vývojových úkolů, které jsou pro toto období typické, jako je to v teorii E.H. Eriksona a R.J. Havinghurtsa. Pokud nahlédneme na vývojové úkoly jako je péče o vlastní děti, péče o stárnoucí rodiče či stabilizace v zaměstnání a ve volnočasových aktivitách, je možné na tyto úkoly navázat i samotné využívání internetu a informačních technologií. Péče o děti vyžaduje také starost o jejich vzdělávání a sociální vztahy, které jsou v dnešní době značně ovlivněny technologiemi. Komunikace se stárnoucími rodiči a jejich tzv. osobní well-being může být také podpořen

využíváním internetu a ve velkém množství zaměstnání je v současné době užívání technologií klíčové. Na druhé straně v *Teorii celoživotního vývoje* G.H. Eldera a v *Bioekologické teorii vývoje* U. Bronfenbrennera je popsán vliv prostředí, který má také souvislost s chováním na internetu, na frekvenci a účel užívání internetu i na vnímanou bezpečnost na internetu. S vlivem prostředí je možné propojit i další psychologické fenomény spojené s využíváním internetu, například FoMO (angl. *Fear Of Missing Out*), což je fenomén označující strach z vynechání událostí, zpráv nebo důležitých příspěvků, které se na internetu objevují (Przybylski, Murayam, DeHaan & Gladwell, 2013). Dalším fenoménem je tzv. *constant connectivity*, neboli neustále přípojení, které se často pojí s tím, že jsme neustále k internetu připojeni. Tento fenomén se často přenáší i do pracovní oblasti, kde může působit jako stresor (Wajcman & Rose, 2011).

Pro pochopení všech souvislostí, které se pojí s chováním a bezpečností na internetu je tedy důležité znát i vývojové souvislosti a charakterizaci období střední dospělosti, jelikož tyto znalosti mohou být nápomocné při pochopení komplexnosti celého fenoménu a při pochopení a případně vysvětlení některých postojů a názorů této generace.

1.3. Charakteristika období střední dospělosti

Díky velkému množství tradičních i moderních vývojových teorií, je možné na vývoj jedince nahlédnout z mnoha různých pohledů. Každá teorie má své silné a slabé stránky, stejně jako možné přístupy k celoživotnímu vývoji. I přes to, že tradiční vývojové teorie, které pracují s jasněji vymezenými stádii vývoje byly některými autory kritizovány za přílišné zobecnění a za nezahrnutí individuálního pohledu, v mnoha výzkumech se s nimi stále pracuje a je na tyto teorie odkazováno.

Přesto ale v dnešní době dochází k obratu, kdy je právě skupina dospělých ve věku střední dospělosti předmětem zájmu různých výzkumů. Jedním z důvodu je také to, že je to v současnosti nejpočetnější skupina obyvatel v USA nebo Evropě (Willis & Martin, 2005).

Střední dospělost je mnohými autory popisována krizí středního věku, která může v tomto období nastat. Lze mluvit o mezeře mezi tím, co jedinec v životě dokázal a očekáváními od budoucnosti (Herman & Oles, 1999). Období střední dospělosti je v novějších teorií spojováno s výzkumy, které se zaměřují na tzv. střední věk. I když je střední dospělost (*angl. middle adulthood*) součástí středního věku (angl. *midlife*), střední věk zasahuje i do období mladší a starší dospělosti, zatímco střední dospělost je charakterizována užším rozmezím (Blatný, 2017).

Kognice v tomto životním období v některých oblastech klesá, je stabilní a někde má rostoucí tendence. P.B. Baltes ve své "*Lifespanové teorii vývoje"* popsal 3 typy procesů:

- *Evoluční výhody selekce* (biologická plasticita; výhody, související s biologickým vývojem organismu)
- *Potřebu kultury* (s věkem se stupňuje a kompenzuje tak snižování biologického procesu)
- *Účinnost kultury*, která klesá, i když potřeba kultury stoupá. Dochází k nárůstu krystalické inteligence (založena na zkušenostech) a k poklesu fluidní inteligence (rychlost, adekvátnost a koordinace operací). I přesto, že dochází k poklesu některých kognitivních funkcí, jedinci mají již vytvořeny významnější kompenzační mechanismy (Blatný 2017).

I když je ve výzkumech často zkoumána proměnlivost kognice v období střední dospělosti, je poměrně složité srovnávat tento věk s dalšími věkovými kohortami. Na lidi ve věku střední dospělosti jsou kladeny úplně rozdílné nároky, kdy je potřeba sladit rodinný a pracovní život, k čemuž jsou potřeba dovednosti plánování, organizace, řešení problémů a tzv. multitasking. Zároveň na kognitivní schopnosti a jejich rozvoj má určitý vliv také prostředí jedince – pracovní nároky, zvyšování kompetencí apod. (Willis & Martin, 2005). Ukazuje se, že vývojové fáze a důležité životní události, jako je docházení do školy, zaměstnání, manželství, narození a výchova dětí nebo odchod do důchodu výrazně ovlivňují motivaci a vzorce chování v souvislosti se sociálními vztahy (Holmes & Rahe, 1967). Zároveň životní fáze ovlivňují jak strukturu, tak velikost sociálních vztahů jedince. Nejpočetnější sociální vztahy mají jedinci během mladé dospělosti, následně je velikost konstantní ve střední dospělosti a snižuje se s přibývajícím věkem (Wrzus, Hanel, Wagner & Neyer, 2013). **Pro pochopení pojetí bezpečnosti a chování na internetu u dospělých ve střední dospělosti je nezbytné nastínění hlavních charakteristik střední dospělosti, jelikož věk může být jednou z proměnných, která právě chování na internetu ovlivňuje.** Se zvyšujícím se věkem se ukazuje, že se například snižuje čas trávený na sociálních sítích a komunikace na internetu se omezuje na kontakt s rodinou a blízkými přáteli, zatímco mladší dospělí mají tendenci navazovat na sociálních sítích vztahy a komunikaci s širší skupinou lidí a využívají sociální sítě k více účelům (Kezer, Sevi, Cemalcilar & Baruh, 2016).

1.4. Charakteristika uživatelů internetu ve střední dospělosti

Generace střední dospělosti je pro tuto práci klíčová. Jak bylo vymezeno v kapitole *1. Střední dospělost*, jedná se o generaci nejčastěji vymezenou věkem mezi 30/40-60 lety. Jako vývojové období je tato část života poměrně individuální a nenormativní. Celkově se ale autoři různých studií shodují na tom, že je potřeba více prozkoumávat jedince ve střední a starší dospělosti na internetu, jejich chování na internetu a prvky zabezpečení, které využívají. Přitom se ale ukazuje, že starší dospělí a jedinci ve střední dospělosti se o svou bezpečnost na internetu zajímají a mají o ní obavy (Chakraborty, Vishik, & Rao, 2013). Jsou také často pod velkým rizikem kvůli možné limitaci v dovednostech v oblasti digitálních technologií, a především v oblasti bezpečnosti (Young & Quan- Hasse, 2013).

Mezi uživateli internetu je poměrně velká skupina uživatelů ve věkovém rozpětí od 35 let, kteří stejně jako mladší generace čelí potenciálním rizikům různého druhu. Většina dosavadních výzkumů se zaměřovala v souvislosti s věkovou skupinou střední dospělosti právě na nebezpečí spojené s telemarketingem a e-mailovými podvody, přičemž velmi málo výzkumu se zaměřuje na rizikové chování dospělých na internetu a na další potenciální nebezpečí, která této věkové skupině na internetu hrozí (White, Gummerum, Wood & Hanoch, 2017). V USA bylo zjištěno, že 86 % dospělých muselo podniknout kroky nutné k zajištění ochrany před nebezpečím na internetu ze strany jiných osob nebo organizací. Zároveň 21 % dospělých byla ukradena hesla k e-mailovému účtu nebo k účtu na sociálních sítích a 11 % byly na internetu ukradeny důležité osobní údaje (údaje k pojištění, k internetovému bankovnictví apod.) (Rainie, Kiesler, Kang & Madden, 2013), což ukazuje, že pro všechny generace je téma bezpečnosti na internetu důležité.

Aktivity, kterými se zabývají různé věkové kategorie na internetu se mohou lišit. V České republice byl uskutečněn mapující výzkum „Starci na internetu“, ve kterém byly sledovány aktivity dospělých nad 35 let na internetu. Mezi nejčastější aktivity patřilo používání e-mailu, komunikace s přáteli, vyhledávání informací a čtení zpráv, používání sociálních sítí, nakupování na internetu, internetové bankovnictví a využívání online map. Z mapujícího výzkumu také například vyplývá, že pouze 15 % respondentů využívá bezpečná hesla na internetu. Nákupy na internetu ale respondenti neprovádějí pouze na oficiálních e-shopech, ale také na dalších portálech jako je v ČR např. SBazar.cz nebo Bazos.cz. Konkrétně v ČR 32 % respondentů potvrdilo, že nakupují i na těchto portálech. S online nakupováním se ale mohou vyskytovat různá rizika. Celkem 40 % respondentů uvedlo, že mají zkušenost s nepoctivým

prodejcem na těchto inzertních portálech. Dále také 24 % respondentů mělo zkušenost s nepoctivým prodejcem na aukčních portálech (Kopecký, Szotkowski, Kožíšek & Kasáčková, 2018).

V případě e-mailové komunikace a podezřelých e-mailů, lidé ve střední dospělosti více inklinují k tomu, že takové e-maily vymažou, aniž by je otevřeli. N. Akdemir (2020) uvádí, že mladí dospělí mají oproti lidem ve střední dospělosti tendenci si spíše upravit nastavení soukromí a různé filtry na svůj e-mailový účet, což má za účinek předejití dostávání takových e-mailů. Tato strategie ale vyžaduje určité znalosti a dovednosti, které podle autora nemusí lidé ve střední dospělosti mít. Zároveň ale uvádí, že i vymazání podezřelých e-mailů je efektivní strategie, jak se vyhnout možným rizikům, jako je například phishing (Akdemir, 2020).

Dalším tématem při využívání e-mailu je přeposílání spamů, zpráv s pravdivými či nepravdivými informacemi, přeposílané humorné e-maily apod. Z respondentů ve věku 55-64 let, což částečně zasahuje i do skupiny střední dospělosti, celkem 38 % uvedlo, že rozesílají e-maily, které varují před možným nadcházejícím nebezpečím. To je 3 - 4krát více, než bylo uvedeno respondenty ve věku 35-44 let, což je také kategorie střední dospělosti. Zároveň starší uživatelé internetu 3 - 6krát častěji rozšiřují e-maily, které obsahují informace o politickém dění, ať už jsou obsažené informace pravdivé či nikoliv (Kopecký, Szotkowski, Kožíšek & Kasáčková, 2018).

Tyto závěry naznačují, že ve skupině střední dospělosti můžeme nacházet výrazné rozdíly s přibývajícím věkem a nejedná se tak o homogenní skupinu, která by měla ve všech oblastech stejné výsledky. Ve výzkumu realizovaném v souvislosti s nepravdivými zprávami na internetu v období pandemie COVID-19 se faktor věku ukázal jako nesignifikantní v nahlížení na nepravdivé zprávy i v oblasti reakcí, které tyto zprávy vyvolávaly. V experimentu byly posuzovány rozdíly mezi třemi skupinami – mladá dospělost, střední dospělost a starší dospělost, přičemž se signifikantně tyto skupiny nelišily (Betina & Megha, 2021).

Další oblastí výzkumu je využívání silných hesel. Lidé ve střední dospělosti mají tendenci využívat méně komplexní a složitá hesla v porovnáním s mladšími dospělými. To může být ovlivněno znalostmi a vědomím o možných rizicích, spojených s jednoduchými a lehce prolomitelnými hesly. Je možné, že mladší dospělí mají lepší povědomí a znalosti, týkající se zabezpečení svých účtu pomocí silného hesla. To, že lidé ve střední dospělosti méně často používají silná hesla, může zvýšit pravděpodobnost budoucí viktimizace na internetu

(prolomení hesla, ukradení účtů apod.) Zároveň některé internetové služby nabízejí novou metodu zabezpečení svého profilu, tzv. dvojitou kontrolu při přihlášení. Někteří mají totiž problém zapamatovat si dlouhá a složitá hesla, tak by tento způsob mohl být výhodný při lepší kontrole a zabezpečení svých účtů (Akdemir, 2020).

Dalším tématem souvisejícím s bezpečností na internetu je již zmiňované sebeodhalení a zveřejňování soukromých informací. Lidé ve střední dospělosti mohou být oproti mladým dospělým méně obezřetní ohledně informací, které zveřejňují. U respondentů ve střední dospělosti se ukazovala o 27 % nižší pravděpodobnost přidání si někoho cizího do seznamu přátel na sociálních sítí, na druhé straně byla o 23 % nižší pravděpodobnost, že se budou chovat opatrně při uvádění osobních údajů na sociálních sítích ve srovnání s mladšími uživateli (Akdemir, 2020). Zároveň se ukazuje, že lidé ve střední dospělosti využívají až o 30 % častěji sociální sítě oproti lidem nad 65 let (Kopecký, Szotkowski, Kožíšek & Kasáčková, 2018). Jak již bylo popsáno výše, s přibývajícím věkem se mění samotné využití sociálních sítí, přičemž skupina střední dospělosti využívá sociální sítě více než skupina seniorů, ale méně než skupina mladých dospělých. Zároveň se oproti mladým dospělým snižuje okruh přátel, který si tato věková kategorie udržuje na sociálních sítích (Kezer, Sevi, Cemalcilar & Baruh, 2016). Ukazuje se, že čím dál tím více dospělých ve střední dospělosti se připojuje k sociálním sítím. Zajímavým přístupem ale je také vnímání užívání sociálních sítí u dospělých ve střední dospělosti v souvislosti s jejich existujícím partnerským vztahem. V rámci studie z roku 2014 bylo zjištěno, že na užívání a chování na sociálních sítích u dospělých ve střední dospělosti má vliv také jejich partnerský vztah a konkrétně dva faktory: důvěra ve vztahu a otevřenost ve vztahu (Norton & Baptist, 2014).

V souvislosti se střední dospělostí se tedy ukazuje značný rozpor mezi výsledky některých studiích, což může být způsobeno tím, že se jedná o velmi různorodou věkovou skupinu. Zároveň v současnosti není takový důraz na sledování této věkové kategorie na internetu, což by se mohlo pro budoucí výzkumy změnit.

1.5. Mezigenerační srovnání uživatelů internetu

Pro bližší nastínění chování uživatelů střední dospělosti na internetu přidává autorka kapitolu věnující se mezigeneračnímu srovnání. Tato kapitola popisuje čtyři věkové kategorie Děti a adolescenty, mladé dospělé, dospělé ve střední dospělosti a na starší dospělost a seniory. Pro

ilustraci autorka vytvořila *Tabulku 2.- Schéma aktivit na internetu dle generací*. V tabulce jsou vypsány nejčastější aktivity, kterými se jednotlivé generace na internetu zabývají: sociální sítě, e-mail, poslech hudby či sledování videí, online nakupování a bankovnictví, vyhledávání informací, komunikace s přáteli či rodinou a využívání map na internetu. Značka mínus ("-") znázorňuje, že tato aktivita nebyla uvedena jako jedna z hlavních aktivit dané generace, následně počet značek plus ("+") znázorňuje, jak vysoko se v seznamu nejčastějších aktivit u dané generace tato aktivita objevuje, tzn. čím více plus, tím vyšší procento uživatelů dané generace se této aktivitě pravidelně věnuje. Jak je vidět z tabulky, pouze jedna aktivita se objevuje u všech generací poměrně vysoko, a to je komunikace s přáteli a rodinou. Proto je důležité věnovat se tématu bezpečnosti na internetu v rámci všech generací. Tento fakt znázorňuje, že internet můžeme chápat jako rozvíjející se způsob a prostředek sociální komunikace, který zasahuje do online i offline světa všech generací. Dále jsou však značné rozdíly v tom, k čemu různé generace internet využívají. Na tyto nejčastější aktivity jsou také nastaveny např. intervenční, výukové či preventivní materiály týkající se ochrany a zabezpečení na internetu. Spolu s tím souvisí i to, že výzkumy a studie jsou směřovány také na oblast nejčastějších aktivit.

	Sociální sítě	**E-mail**	**Sledování videí/poslech hudby**	**Online nakupování a bankovnictví**	**Vyhledávání informací**	**Komunikace s přáteli a rodinou**	**Mapy**
Děti a adolescenti	++++	-	++++	-	-	+++	-
Mladší dospělí	+++	++	+++	++	+++	+++	+
Generace střední dospělosti	++	+++	++	+++	++++	+++	+++
Starší dospělost a senioři	+	++++	-	++++	++++	+++	++++

Tabulka 2. - Schéma aktivit na internetu dle generací

I když je tedy využívání e-mailu častou aktivitou této generace i generace starších dospělých a seniorů, značná část uživatelů těchto generací využívá i sociální sítě a další aplikace, a tak by měla být pozornost zaměřena i tímto směrem. Například N. Akdemir (2020) uvádí, že výukové programy o aktivních copingových strategiích v případě online nebezpečí by mělo být

směřováno právě na generaci střední a starší dospělosti, protože je v této oblasti zatím značný nedostatek (Akdemir, 2020). Celkově se výzkumy příliš neshodují na tom, zda a jaké jsou rozdíly ve vnímání bezpečnosti a ve vlastním zabezpečení mezi generacemi. Některé studie uvádí, že rozdíly mezi generacemi jsou a některé rozdíly popírají. Zároveň je ale z tabulky zřejmé, že minimálně v jedné aktivitě, což je komunikace s přáteli a rodinou se shodují všechny generace a tento způsob komunikace využívají.

Ve výzkumu S. Livingstonové, L. Kirwilové, C. Ponteové a E. Staksrudové (2013) například děti a adolescenti uvádějí jako nejvíce znepokojující online zkušenosti vystavení sexuálnímu obsahu, obsahu spojenýého s agresí a další nechtěné zážitky jako je online obtěžování, kyberšikana, hackerství, sdílení osobních informací, poškození reputace a také viry, spamy a reklamy. Z kvalitativního výzkumu (Šmahel & Wright, 2014) se ukazuje, že děti často uvádějí jako obtěžující zkušenosti také technické problémy spojené s užíváním internetu, jako je pomalý nebo nefunkční připojení k internetu.

Nejčastějšími strategiemi, jak se bránit negativní zkušenosti na internetu mezi dětmi a adolescenty je zablokování jedince, který způsobuje negativní zážitky a vnímanou nepohodu, promluví si s někým blízkým o nastalé situaci, využijí technické možnosti, konfrontují agresora nebo samotný problém ignorují (Parris, Varjas, Meyers, & Cutts, 2012). Průměrně 40 % dětí uvedlo, že by o problému mluvilo s matkou nebo otcem, 50 % by si promluvilo s blízkým vrstevníkem a 14 % uvedlo, že by si o problému promluvilo se sourozencem. Pouze 3 % dětí uvedlo, že by oslovilo např. psychologa či výchovného poradce (Šmahel a kol., 2020).

Další generací je mladá dospělost, která je ve většině výzkumů vymezována mezi 18 - 30/40 lety (Kezer, Sevi, Cemalcilar & Baruh, 2016). Využívání technologií je v období mladší dospělosti čím dál častěji nutností, jelikož je vyžadováno jak během vzdělávání, tak i v zaměstnání. Lidé v období mladé dospělosti jsou často označovány za technicky zdatnější v otázce využívání technologií oproti dospělým ve střední (30/40 - 60 let) nebo starší dospělosti (60+ let). Zároveň mají tendenci častěji využívat sociální sítě (Kezer, Sevi, Cemalcilar & Baruh, 2016). Mohou tedy mít nejen vyšší povědomí o možných rizicích spojených s užíváním internetu, ale i o ochraně soukromí. Mohou tak lépe upravovat nastavení svého soukromí na různých online platformách tak, aby se před možnými riziky mohli chránit (Bolton a kol. 2013; Litt, 2013).

Dále se ukazuje se, že s přibývajícím věkem se zmenšuje okruh přátel, se kterými jedinci komunikují online. To znamená, že skupina mladých dospělý má na sociálních sítích menší skupinu přátel oproti adolescentům, nicméně mají širší sociální síť přátel než jedinci ve střední nebo starší dospělosti. Zároveň se neprokázal statisticky významný rozdíl mezi tím, kolik respondenti mají v seznamu přátel osob, které dříve nepotkali a neznají se s nimi osobně. To znamená, že mezi mladou, střední a starší dospělostí nebyl rozdíl v tom, zda si na sociálních sítích do seznamu přátel přidávali i neznámé osoby. Zároveň se ale ukazuje, že mladší dospělí využívají více než lidé ve střední a starší dospělosti sociální sítě k sociální interakci (Kezer, Sevi, Cemalcilar & Baruh, 2016).

V otázce bezpečnosti na sociálních sítích a na internetu se ukazuje, že mladí dospělí častěji, než starší věkové skupiny zveřejňují soukromé informace, ale na druhé straně se více angažují k aktivní kontrole a ochraně svého soukromí. V souvislosti s výše zmíněnými čtyřmi potenciálními dimenzemi postojů k ochraně soukromí (dle Baruh a Cemalcilar 2014) se ukazuje, že u mladých dospělých není pravděpodobné, že jejich soukromí závisí na tom, zda ostatní lidé chrání své soukromí a že berou ohled na soukromí ostatních jedinců (Kezer, Sevi, Cemalcilar & Baruh, 2016). Dle autorů je tedy pravděpodobné, že jejich obavy o soukromí ostatních se nebudou promítat do jejich rozhodování o ochraně vlastního soukromí. Mladí dospělí s větší pravděpodobností využívají sociální sítě jako nástroj ke komunikaci a socializaci, sdílejí více informací o sobě a prohlížejí si informace o ostatních jedincích, než lidé ve střední či pozdní dospělosti (Kezer, Sevi, Cemalcilar & Baruh, 2016).

Zároveň například u online nakupování mají mladí dospělí oproti uživatelům ve střední dospělosti vyšší pravděpodobnost nakupovat na ověřených e-shopech a na důvěryhodných webových stránkách (Akdemir, 2020).

V případě obav z možného nebezpečí na internetu se ukazuje, že starší dospělý mají větší starosti ohledně bezpečnost na internetu než mladší dospělí a lidé ve střední dospělosti (Akdemir, 2020). V souvislosti s bezpečností na internetu se ukazuje, že lidé nad 65 mají větší obavy z institucionální bezpečnosti než ze sociální či technické (Quan-Haase & Ho, 2019). Výsledky několika studií ale ukazují, že u seniorů je méně pravděpodobné, že budou odhalovat sebe sama na sociálních sítích, že budou zveřejňovat soukromé informace a naopak, že by využívali bezpečnostní nastavení a nastavení poskytující vyšší ochranu soukromí (Van den Broeck, Poels & Walrave, 2015; Kezer, Sevi, Cemalcilar & Baruh, 2016, 2016). To může být spojeno také s tím, že starší dospělí a senioři netráví na sociálních sítích tolik času.

Takto popsané mezigenerační srovnání chování na internetu nám může pomoci blíže pochopit chování jednotlivých generací, v případě této práce generace střední dospělosti. Někdy je také o střední generaci uvažováno jako nad tzv. sendvičovou generací, kdy mají často v péči své děti a zároveň už se starají o své starší rodiče. I z tohoto důvodu je důležité se na tuto generaci zaměřit i z hlediska ochrany na internetu a směřovat informace o ochraně na internetu právě na ně. Mohou pak ochránit nejenom sebe, ale předávat své zkušenosti, dovednosti a názory mladším i starším generacím, které si k nim mohou chodit pro cenné rady.

2. Psychologické fenomény spojené s užíváním internetu

S využíváním internetu se pojí mnoho psychologických fenoménu, se kterými se setkává téměř každý jedinec, který se pravidelně na internetu pohybuje. Mezi tyto fenomény patří například disinhibiční efekt v rámci online komunikace, fenomény spojené s časem trávený na internetu, efekt trollování na internetu, šíření nepravdivých zpráv, efekty spojené s vyhledáváním informací nebo sociální sronávání na internetu. Tyto fenomény mohou být vnímány jako ohrožující či rizikové aspekty spojené s internetem. Výsledkem těchto fenoménu může být vnímaná osobní nepohoda a pro některé uživatele můžou představovat to, co na internetu vnímají jako negativní či ohrožující. Tato kapitola je zařazena právě proto, že popsané fenomény se ukázaly jako zásadní při hloubkových rozhovorech realizovaných v diplomové práci a byly velmi úzce spjaty s vnímáním bezpečnosti na internetu. Popsané fenomény byly také zařazeny do dotazníku, který byl využit pro výzkumnou část práce.

2.1. Komunikace na internetu

Komunikace na internetu probíhá v různých kontextech (sociální sítě, online hry, maily, messenger apod.), přičemž je velmi odlišná od komunikace tváří v tvář. Nabízí nám možnost asynchronicity komunikace, mizí fyzický kontakt, boří se problémy spojené se vzdáleností a máme možnost kontroly nad celou interakcí (můžeme si lépe promyslet, co napíšeme, jak se budeme prezentovat, a navíc můžeme interakci ukončit jedním kliknutím) (Danet & Miljkovitch, 2017).

Součástí komunikace na internetu je sdílení a poskytování osobních informací, což považujeme za druh sebeodhalení sebe sama. To můžeme označit jako předání zprávy či informace o sobě druhému člověku. Obecně se tedy sebeodhalení a poskytování informací o sobě vyskytuje v jakémkoliv komunikačním procesu (Wheeless & Grotz, 1976). To se týká jak komunikace v offline, tak v online světě. Sebeodhalení je tedy předpokladem jakéhokoli sociálního vztahu (Altman & Taylor, 1973). To, kolik o sobě předáme informací se ale liší v šíři informací, v míře intimity či citlivosti, v upřímnosti, přesnosti nebo uvědomění (Altman & Taylor, 1973). Zároveň je přirozené, že v jakékoliv komunikaci zvažujeme možné zisky a ztráty, které nám v konečném důsledku může sebeodhalení přinést. To ukazuje, že v každé interakci přemýšlíme o tom, co druhému nebo skupině dalších lidí chceme o sobě předat, jaké informace nám mohou usnadnit navazování vztahů a naopak, co pro nás může v další komunikaci zraňující nebo jaké informace jsou už ke sdílení s dalšími lidmi za osobní hranicí (Petronio, 2002). Mezi tím, co o

sobě chceme říct a tím, že chceme chránit své soukromí může panovat napětí (Taddicken, 2014).

Obecně lze soukromí definovat jako právo jedince na určení toho, jaké informace, komu a kdy jsou zpřístupněny (Westin, 1967). Míra soukromí tedy zahrnuje různé aspekty. Z psychologického hlediska může být ochrana soukromých informací chápána jako obrana před vnějšími vlivy, které mohou mít dopad na naše myšlenky, postoje a vlastní osobu. Tudíž je přirozené, že každý jedinec má zájem o to, kdo má přístup k jeho informacím, kdo je nějakým způsobem shromažďuje a případě předává dalším stranám. Zvažování možných zisků a ztrát tedy implikuje to, že ideální míra soukromí je dosažena v momentě, kdy je potřeba sociální interakce v souladu s potřebou soukromí (Taddicken, 2014).

Výše zmíněné poznatky o soukromí v rámci komunikačního procesu jsou původně vztaženy ke komunikaci v tváří v tvář, přičemž je možné je vztáhnout i ke komunikaci v online prostředí. V offline komunikaci máme kontrolu nad tím, komu jaké informace sdělujeme a zároveň naše sebeodhalení je závislé na kontextu a náladě interakce. To by v ideálním případě mělo fungovat i v online světě, ale vzhledem k odlišnostem online světa je tomu jinak. V online světě jsou sdílené informace o nás v digitální podobě, což znamená, že jsou lépe dohledatelné a zároveň trvale (nebo dlouhodobě) uložené. Dostupnost digitálních informací je výrazně vyšší než v tradiční offline komunikaci. To, že je obsah komunikace v digitální podobě zároveň umožňuje a zjednodušuje kombinaci informací z různých aplikací. Informace zveřejněné na internetu jsou proto trvalé, replikovatelné, škálovatelné, prohledávatelné a sdílitelné (Boyd, 2008; Papacharissi & Gibson, 2011).

Tyto rozdíly ve vlastnostech informací, které sdílíme v online prostředí na rozdíl od prostředí offline světa dle Taddickenové (2014) vedou k nutnosti rekontextualizace pojetí sebeodhalení v různých komunikačních kontextech. Na internetu, především na sociálních sítích, máme často pocit, že informace, které sdílíme, sdílíme pouze nejbližšímu okruhu přátel. Mezi tento okruh řadíme skupinu lidí, které jsme „pozvali“ do našeho online světa. Jsou to často naši přátelé, rodina, kolegové z práce a další. Často ale není úplně jasné, komu informace o sobě předáváme a tedy skupina, které myslíme, že informace předáváme se může lišit od skupiny lidí, kterým doopravdy odhalujeme informace o sobě. To, že například na sociálních sítích sdělujeme své názory nebo myšlenky a že sdílíme soukromé fotky pro jednu skupinu lidí, může způsobit problémy v komunikaci s dalšími skupinami, u kterých jsme nepočítali, že budou mít tyto informace k dispozici. Pokud nemá jedinec na své sociální síti nastavená pravidla pro soukromí,

můžou následně jeho fotografie a příspěvky vyhledat další osoby, pro které jedinec původně tyto informace nesdílel (např. potenciální zaměstnavatel). Zároveň je možné, že jsou informace o nás předávány třetím stranám a jsou tak přenášeny do dalších kontextů jako je například personalizovaná reklama nebo obsah našich příspěvků může být kopírován a sdílen dalšími uživateli. To může uživatelům sociálních sítí přinášet nepříjemné důsledky jak v osobním, tak v pracovním životě. Tento popsaný jev popisující to, že můžeme odlišně vnímat skupinu jedinců, pro které sdílíme naše informace a skupinu lidí, která k nim skutečně má přístup, je označováno jako tzv. *kontextový kolaps* (Marwick & Boyd, 2011).

Z různých výzkumů vychází, že např. lidé, kteří jsou nespokojeni se svým "skutečným" životem a se svými sociálními interakcemi a vztahy, mohou používat internet jako náhradu interakce tváří v tvář. Zároveň bylo zjištěno, že sociálně úzkostlivější lidé se mohou cítit sebejistěji a pohodlněji na internetu a při virtuální komunikaci než při komunikaci tváří v tvář (Danet & Miljkovitch, 2017). S komunikací na internetu se také pojí tzv. *disinhibiční efekt*. Během online komunikace mohou mít někteří lidé tendenci zveřejňovat o sobě více informací, vyjadřují se s větší intenzitou či frekvencí než by se vyjadřovali tváří v tvář. Na internetu mají tedy někteří lidé tendenci posunout své osobní hranice komunikace a vyjadřují se otevřeněji a uvolněněji. Tento efekt se dělí na dva druhy: **vlídná disinhibice a toxická disinhibice.** Vlídná disinhibice zahrnuje jev, kdy lidé více vyjadřují své emoce, pocity, strachy a přání. Komunikují s větší přívětivostí, otevřeností a mohou vyjadřovat větší ochotu pomáhat ostatním. Některé projevy vlídné disinhibice mohou naznačovat pokus lépe porozumět sám sobě a rozvíjet se, řešit interpsychické a intrapsychické problémy, či prozkoumat nové emocionální dimenze vlastní identity (Suler, 2002). Na druhé straně je ale toxická disinhibice. V případě toxické disinhibice se setkáváme s vyšší drzostí, kritikou, vztekem až nenávistí, někdy se objevuje i vyhrožování a vulgarismy. Zároveň mohou lidé inklinovat k navštěvování stránek s nelegálním sexuálním obsahem nebo stránek, obsahující zobrazení násilí a dalšího kriminálního chování. Dostávají se tak do sfér, které by ve světě mimo internet nikdy nezkoumali (Suler, 2004). J.R. Suler (1999) toxickou disinhibici označuje jako možnou slepou katarzi, opakování vlastních kompulzí a jednání negativních potřeb, které nevedou k žádnému osobnostnímu růstu (Suler, 1999). J.R. Suler (2004) dále popisuje šest zdrojů, ze kterých disinhibiční efekt vychází: anonymitu, neviditelnost, asynchronicitu, solipstickou introjekci, disociativní představivost a minimalizaci autority.

Anonymita:	Přezdívky, falešné profily, identita
Neviditelnost:	Absence neverbálních projevů, minimalizace vlivu vzhledu
Asynchronicita:	Časová odmlka v komunikaci
Solipstická introjekce:	Vlastní představa o partnerovi, se kterým komunikujeme; dominance vlastních představ (očekávání) nad realitou
Disociativní představivost:	"Internetové já jako" virtuální postava (nižší zodpovědnost za chování na internetu; nezávislé chování, které nemá vliv na offline svět
Minimalizace autority:	Smazání reálných sociálních rolí a statusů

Tabulka 3. - Zdroje online disinhibičního efektu

Toxický disinhibiční efekt může působit na vnímání sociální bezpečnosti na internetu, kdy právě urážlivé a vulgární reakce jiných lidí mohou dalším uživatelům ublížit a způsobit psychickou nepohodu. Zároveň někdo, kdo se nechává unést internetovou komunikací následně může řešit disociaci mezi tím, jak sám sebe vnímá v online či offline světě. Pro ty, kdo se spíše nacházejí na straně vlídné disinhibice může vlastní sebeodhalení nakonec působit negativně a mohou později litovat, že o sobě prozradili více, než původně chtěli nebo než odhalují v offline komunikace. Zároveň ale může mít disinhibice pozitivní efekt v oblasti nácviku komunikace, posouvání vlastních zábran v komunikaci a testování si různých komunikačních stylů (Suler, 2004). Komunikace na internetu je velmi specifická svými odlišnostmi od offline komunikace. Je tedy nezbytné přemýšlet jak nad pozitivy, tak nad negativy, které online komunikace může přinášet.

2.2. Připojení k internetu

S tím, že internet využíváme ke stále více aktivitám souvisí také to, že jsme více času k samotnému internetu opravdu připojeni. Stále více uživatelů se přesouvá k využívání chytrých telefonů a k dalším zařízením, které máme neustále u sebe a téměř neustále jsou tato zařízení připojena k internetu. S tím se pojí fenomén tzv. *neustálého připojení* (*angl. constant connectivity*), který se primárně pozoroval v oblasti pracovní psychologie. Tento fenomén popisuje fakt, že jsme našich neustále připojeni k online světu (nejčastěji přes chytré telefony), ať už za účelem řešení rodinných a podobných záležitostí, či pro připojení k práci (Wajcman &

Rose, 2011). To, že jsme neustále připojeni k internetu se stává standardem současné doby. Má to za následek to, že můžeme rychle reagovat na jakoukoliv internetovou komunikaci jako je e-mail či online zprávy (pomocí aplikací jako je messenger, WhatsApp, Viber a další komunikační aplikace). Původně se nad neustálým připojením přemýšlelo jako nad rušivým vlivem moderních technologií, ale následně se tento pohled změnil v to, že se jedná o možnost, jak zrychlit a zefektivnit komunikaci například v pracovním prostředí. Právě J. Wajcman a E. Rose (2011) uvádějí, že není nutné na neustálé připojení a na přicházející upozornění nahlížet jako na vyrušování od pracovního procesu, ale jako na novou normu, která se objevuje ve firmách a organizacích, kde je zároveň normou, že jsou digitální technologie všudypřítomné.

V souvislosti s neustálým připojením se uvádí také tzv. *paradox autonomie*, který vysvětluje, to, že může být autonomie spojená s flexibilním připojením dvousečná. Na jedné straně je právě možnost připojit se k práci kdekoli a kdykoli zvyšuje pocit autonomie. Uživatelé se tedy mohou díky digitální komunikací a technologiím (e-mailem, zprávami) cítit, že se mohou rozhodnout, kdy a pro koho se mohou připojit k vyřízení různých záležitostí, ať už pracovních či osobních. Zároveň neustálé přípojení a související dostupnost mohou v pracovním prostředí dodávat pocit, že se udržují na vrcholu své pracovní pozice a efektivity práce (Mazmanian, Orlikowski & Yates, 2013; Day, Barber & Tonet, 2019). Na druhé straně je zde kolektivní úroveň neustálého připojení, kdy právě neustálé příchozí zprávy a upozornění mohou působit vyrušení při dalších činnostech, což může snižovat pocit autonomie (Day, Barber & Toner, 2019; ten Brummelhuis, ter Hoeven & Toniolo-Barrios, 2021).

Dále A. Dayová, L. Barberová a J. Tonetová (2019) popsaly další dva paradoxy spojené s neustálým připojením. Jedná se o *pracovní paradox produktivity* a *sociální pracovní paradox*. Pracovní paradox produktivity popisuje fakt, že zaměstnanci jsou neustále připojení a je možné jim kdykoliv napsat. To umožňuje rychlou a efektivní komunikaci a následně se může zvyšovat i efektivita práce zaměstnanců. Na druhou stranu zvýšené množství příchozích zpráv zvyšuje množství přerušení pracovního procesu, narušuje pozornost a může vést ke komunikačním chybám, přetížení zaměstnanců nebo ke snížení kvality komunikace. Zároveň se zvyšuje čas, který zaměstnanci potřebují k tomu, aby zpracovali informace z přicházejících zpráv a aplikovali nové úkoly do pracovního procesu. Sociální paradox v pracovní oblasti je vztažen k vztahům v pracovním týmu.

Sociální pracovní paradox popisuje to, že spojení s ostatními zaměstnanci může snížit pocit izolace a podporuje spolupráci v týmu. Na druhé straně průběžná komunikace po celý den může

narušovat pracovní proces, může vyvolávat negativní emoce či neporozumění mezi členy týmu, čímž se mohou narušovat vztahy na pracovišti (Day, Barber & Tonet, 2019).

Tyto tři výše popsané paradoxy neustálého připojení (paradox autonomie, produktivity a sociální paradox) jsou ve výzkumech často spojovány se sebedeterminační teorií (angl. *STD - Self- Determination Theory*). Tato teorie byla vytvořena americkými psychology R.M. Ryanem a E.L. Decim, přičemž tato teorie se zaměřuje na motivaci, seberozvoj a zdravý životní styl. V teorii jsou rozlišeny tři základní potřeby: potřeba sounáležitosti, kompetentnosti a autonomie (Ryan & Deci, 2010). Potřebu sounáležitosti je možné spojit právě se sociálním paradoxem, konkrétně se vztahy na pracovišti a zapojení do komunikace. Potřeba kompetentnosti je naplněna nebo narušena právě efektivitou komunikace a spojenou produktivitou práce. Paradox autonomie je logicky spojen s potřebou vlastní autonomie i v rámci komunikace v digitálním prostředí.

Neustálé připojení sledovali autoři v souvislosti s STD ve studii publikované v roce 2021. Autoři realizovali dvě pětidenní deníkové studie. V první fázi se studie zúčastnilo 317 zaměstnanců a v druhé 72 zaměstnanců. Studie ukázala, že neustálé připojení pozitivně souvisí s pracovním výkonem díky vyšší efektivitě komunikace. Na druhou stranu je ale časté přerušování příchozími zprávami spojeno se sníženou efektivitou práce a výkonu. Dostupnost a připojení na jedné straně pozitivně souvisí s prožívanou kontrolou nad komunikací, ale právě přerušení příchozími zprávami na druhé straně negativně souvisí s pocitem kontroly. Touto studií se tedy ukazuje, že neustálé připojení přináší do komunikace ve firmách svá pro a proti a je nutné tento fenomén zvažovat i při nastavování firemní komunikační kultury. Autoři také nahlížejí na neustálé připojení ve dvou dimenzích: dostupnost jako pozitivum a přerušení zprávami jako negativum (ten Brummelhuis, ter Hoeven & Toniolo-Barrios, 2021).

Neustálé připojení je tedy spojováno s efektivnější komunikací, pocitem autonomie, zefektivnění výkonu, ale na druhé straně to může působit úplně opačně a lidé se pak necítí dostatečně autonomní, může se zhoršovat kvalita komunikace, a navíc může neustálé připojení zvyšovat stres, prodlužovat pracovní dobu (když zaměstnanci odpovídají na pracovní e-maily i mimo pracovní dobu) nebo osobní well-being. Zároveň ale to, zda lidé budou nebo nebudou připojeni a zda se nechají vyrušit příchozími zprávami je také jejich rozhodnutí, zvlášť pokud se jedná o odpojení po pracovní době (Russo, Ollier-Malaterre & Morandin, 2019).

Neustálé připojení lze vztáhnout i k osobními životu a k čase mimo pracovní dobu. V kvalitativní studii L. Harkinové a D. Kussové (2021) se neustálé připojení ukazuje jako jedna z podkategorií, vzniklých při analýze užívání chytrého telefonu. Z analýzy vyplývá, že respondenti využívají své telefony jako "extenzi vlastního já". To znamená, že lidé využívají své telefony na denní bázi a telefony tak zasahují do každodenních aktivit, dodávají jim přístup k informacím, pomáhají při vzdělávání, v pracovním procesu, při využívání různých aplikací. Jednou z podkategorií tedy bylo neustálé připojení, které respondenti vnímali jak pozitivně, tak negativně. To, že mají respondenti u sebe neustále telefon jim umožňuje být neustále ve spojení s kýmkoliv a kdykoliv. To může dodávat pocit, že nikdy nejsme sami, což může mít pozitivní, ale i negativní dopad. Tím, že můžeme ke komunikaci využívat internet, překonáváme vzdálenosti mezi přáteli a rodinou a celá komunikace je ulehčená. V osobním životě tedy neustálé připojení přináší také pozitiva i negativa. V souvislosti s výše zmiňovanými výzkumy z pracovního prostředí (ten Brummelhuis, ter Hoeven & Toniolo- Barrios, 2021), i v tomto výzkumu respondenti zmiňovali přesah pracovní doby do jejich osobního života. Tuto skutečnost většinou považují respondenti za negativní, jelikož pracovní doba zasahuje do jejich volného času a prodlužuje se. Dále respondenti uvádějí, že je poměrně těžké neodpovídat na pracovní e-maily a další zprávy ihned po přečtení, což negativně ovlivňuje jejich osobní pohodu (Harkin & Kuss, 2021).

Konkrétně tedy na využívání chytrých telefonů, které jsou připojeny k internetu se v současnosti zaměřuje poměrně velké množství výzkumů, které zkoumají vliv mobilních telefonů na kognitivní funkce uživatelů (především na pozornost a další). Ukazuje se, že příchozí zprávy a další upozornění mohou být spojeny s negativními účinky na naši pozornost od dalších úkolů. Především to, že telefony jsou zařízení, která má většina lidí neustále u sebe je zajímavá právě frekvence, se kterou se objevují odklony pozornosti v souvislosti s telefony (Ward, Duke, Gneezy & Bos, 2017).

Málo studií se však zaměřuje na efekt pouhé přítomnosti chytrého telefonu při plnění nějakého úkolu. Při experimentální studii z roku 2017 se autoři zaměřili právě na efekt přítomnosti telefonu při plnění úkolu. V experimentu rozdělili skupinu respondentů na ty, kteří měli telefon položen obrazovkou dolů na stole před sebou, další respondenti měli telefon v kapse, další skupina měla telefon v tašce či batohu a poslední skupina měla telefon v jiné místnosti. V tomto výzkumu byl prokázán negativní efekt pouhé přítomnosti telefonu bez notifikací (při vypnutém zvuku i vibracích) na pozornost a kognitivní kapacitu. Zároveň se autoři ptali respondentů, zda

v průběhu plnění testů mysleli na svůj telefon a případně kolikrát si na něj vzpomněli. Ukázalo se, že se snižoval výkon v úkolech, i když respondenti v sebehodnotících dotaznících odpovídali tak, že na telefon ve většině případů nemysleli. To ukazuje, že tříštění pozornosti působí i když si toho jedinec není vědom (Ward, Duke, Gneezy & Bos, 2017). V roce 2014 byla realizována podobná studie, která zkoumala kognitivní účinky pouhé přítomnosti mobilního telefonu, který má vypnutý zvuk, vibrace a nijak aktivně nezasahuje do plnění úkolu. V této studii bylo také zjištěno, že přítomnost telefonu může zhoršit výkon při plnění úkolů, které vyžadují trvalou pozornost. Autoři uvádějí, že pozornost může být narušena právě tím, že přítomnost telefonu vyvolává nepříjemný pocit, že nejsme součástí a nejsme připojeni k sociální a informační síti a k událostem, které mohou v danou chvíli probíhat (Thornton, Faires, Robbing & Rollins, 2014).

Tento nepříjemný pocit, že nejsme připojeni a přicházíme o důležité události souvisí s dalším psychologickým fenoménem, který se spojuje s užíváním technologií a to je tzv. FoMO (*angl. Fear of Missing Out)* neboli strach ze zmeškání nějaké události. FoMO lze opět propojit s výše zmíněnou sebedeterminační teorií (STD), která popisuje tři základní lidské potřeby (potřeba sounáležitosti, kompetentnosti a autonomie). To, že jsme připojeni k sociálním sítím nám nabízí naplnění těchto tří základních potřeb, a tak může být FoMO chápáno jako *"seberegulační limbo vyplývající ze situačních či chronických deficitů v uspokojování psychologických potřeb"* (Przybylski, Murayama, DeHaan & Gladwell, 2013). Naplnění těchto potřeb v souvislosti s užíváním digitálních technologií, konkrétně sociálních sítí, lze propojit tak, že jednotlivci s málo uspokojenými potřebami mohou používat sociální sítě jako nástroj pro kontakt s jinými lidmi, pro rozvoj sociálních kompetencí a jako možnost navazovat vztahy. Nenaplnění potřeb může vést k vyšší senzitivitě k FoMO, a tak je možné, že naplnění potřeb pomocí sociálních sítí je regulováno právě FoMO, strachem ze zmeškání nějaké události. To znamená, že by tento strach mohl fungovat jako prostředník mezi užíváním sociálních sítí a dalších platformem, kde mohou uživatelé komunikovat a navazovat vztahy, a naplňováním základních psychologických potřeb. FoMO lze definovat jako *"obavu, že jiní prožívají události či zážitky, kterých jedinec není přítomen. Pro fenomén FoMO je charakteristická touha neustále zůstat ve spojení s tím, co dělají ostatní"* (Przybylski, Murayama, DeHaan & Gladwell, 2013).

S tím, že máme naše zařízení, která jsou připojena k internetu, neustále u sebe se tedy pojí mnoho psychologických fenoménu. Prvním zmíněným bylo právě neustálé připojení, které může zasahovat do našeho osobního i pracovního života. Dále přítomnost telefonu ovlivňuje i naši kognitivní kapacitu, přičemž se ve výzkumech prokázal signifikantní vliv i když je telefon

neaktivní, nezvoní, nesvítí ani nebzučí. S tím se pojí poslední představený fenomén, kterým je FoMO, neboli strach ze zmeškání nějaké události. To, že jsme si přivykli na to, že jsme neustále připojeni a že na sociálních sítích a na internetu se pořád něco děje, vede k tomu, že často kontrolujeme aktivitu na našem telefonu, připojení nám zabírá více času, než bychom si možná přáli, ubírá nám to kapacitu pozornosti a můžeme prožívat úzkost spojenou s tím, že něco prošvihneme. Na druhou stranu můžeme takto naplňovat psychologické potřeby spojené s komunikací, autonomitou, sociabilitou a vlastními kompetencemi, můžeme zlepšovat komunikaci na pracovišti i komunikaci s našimi blízkými. Tyto fenomény přináší jak pozitiva, tak negativa, nad kterými je důležité se zamýšlet i v souvislosti s tématem této práce, což je bezpečnost na internetu.

2.3. *Vyhledávání informací na internetu*

Internet nám kromě sociálního vyžití a naplňování dalších psychologických potřeb nabízí i místo pro vyhledávání veškerých informací. Celkově s přístupem k internetu se také zjednodušuje přísun informací, otevírá se více možností pro dalších vzdělávání, ověřování informací, ale také například hledání spojů v dopravě, užívání map čtení zpráv, čtení elektronických novin, časopisů, najdeme zde např. recepty a mnoho dalších informací. Tento typ informací byl nejčastěji zmiňován respondenty ve výzkumné části. S vyhledáváním na internetu se pojí také šíření nepravdivých zpráv, které jsou v anglické literatuře označovány jako *fake news*. Tyto nepravdivé zprávy obsahují informace, které nejsou nijak podložené a často nejsou pravdivé. Mohou se šířit dále a rychleji než pravdivé zprávy a mohou zůstávat v povědomí lidí déle (Newman, Fletcher, Kalogeropoulos, Levy & Nielsen, 2017). Narůstajícím problémem je právě šíření nepravdivých zpráv přes sociální sítě. Například v USA bylo zjištěno, že až 62 % dospělých vyhledává zprávy na sociálních sítích místo na tradičních či ověřených zpravodajských portálech. Zároveň počet dospělých, kteří hledají informace a zprávy ze světa na sociálních sítích roste, v roce 2012 zjišťovalo tyto informace na sociálních sítích "pouze" 49 % dospělých (Newman, Fletcher, Kalogeropoulos, Levy & Nielsen, 2017).

Šíření nepravdivých zpráv je problémem, který zasahuje do celé společnosti. Konkrétně sociální sítě jsou velmi náchylné k tomu, aby se na těchto platformách rychle nepravdivé zprávy šířily. V tomto případě dochází k posunu od toho, čemu se tradičně věnují žurnalisté, jejichž práce zahrnuje právě ověřování a potvrzování či vyvracení zpráv, které se stávají součástí veřejného prostoru. Tato funkce, se stále rostoucím fenoménem nepravdivých zpráv, upadá a

žurnalisté a novináři mají již menší vliv na to, jaké informace jsou ve veřejném prostoru či jaké informace můžeme označit za důležité a zásadní. Nepravdivé zprávy můžeme rozdělit na tři podkategorie. První kategorií jsou **vymyšlené zprávy**, druhou jsou **podvodné zprávy** (angl. *hoax*) a třetí kategorií jsou **vtipné, satirické nepravdivé zprávy** (Rubin, Chen & Conroy, 2016).

Vymyšlené, fabrikované zprávy obsahují často výrazný titulek, který je napsán tak, aby na něj lidé chtěli kliknout (tzv. *clickbaits*), následně tyto zprávy obsahují skandální zprávy, pomluvy, kriminální příběhy, nepravdivé zprávy o známých osobnostech apod. Podvodné zprávy (hoaxy) obsahují vymyšlené a zfalšované zprávy, které vypadají jako tradiční zpravodajský článek. Zároveň ale účelem těchto zpráv je ublížit či poškodit čtenáře či jedince, kteří jsou obsaženi v těchto zprávách. Vtipné, satirické a humorné zprávy obsahují nepravdivé informace, ale cílem těchto zpráv není poškodit čtenáře ani ty, kteří jsou obsahem článku, cílem těchto zpráv má být pobavení (Rubin, Chen & Conroy, 2016). Zároveň se ukazuje, že šíření těchto falešných či poplašných zpráv se často objevuje s přibývajícícm věkem. Nejčastěji se tyto zprávy rozesílají právě přes sociální sítě nebo pomocí e-mailové komunikace (Kopecký, Szotkowski, Kožíšek & Kasáčková, 2018). V současné době, kdy velkým celospolečenským tématem a problémem je právě pandemie COVID-19 bylo do světa vypuštěno poměrně velké množství zpráv týkajících se pandemie, kdy zároveň část těchto zpráv byla nepravdivá či neověřená. V letošním roce (2021) byla v reakci na tyto zprávy spojené s COVID-19 publikována studie, sledující právě náchylnost k nepravdivým zprávám v souvislosti s věkem uživatelů. Výsledky studie ukázaly, že mezi věkovými skupinami (mladá dospělost, střední dospělost a starší dospělost) nebyly signifikantní rozdíly v náchylnosti k nepravdivým zprávám a v dalším chování souvisejícím s reakcí na tyto zprávy. Ukázalo se ale, že nepravdivé zprávy jsou rozšířenější než ty pravdivé. Nejčastější emoce vyjadřované v souvislosti se sledovanými zprávami byly napříč věkovými kategoriemi stejné a jednalo se především o lhostejnost, znechucení či překvapení. Zároveň se neukázaly signifikantní rozdíly v rozesílání těchto zpráv napříč skupinami. To znamená, že nebyl rozdíl v tom, jak jaká věková skupina rozšiřuje či nerozšiřuje nepravdivé informace (Betina & Megha, 2021).

Šíření nepravdivých či poplašných zpráv je možné zařadit do oblasti sociální psychologie. Souvislosti s vyhledáváním na internetu je ale možné sledovat i z pohledu kognitivní psychologie, konkrétně například v oblasti internetových prohlížečů a jejich vlivu na rychlost řešení otázek. V současnosti máme díky internetovému připojení dostupné jakékoli informace,

které potřebujeme vyhledat. Ať už se jedná o vyhledání našich přátel, které jsme dlouho neviděli, až po informace týkajících se filmů, které jsme viděli, receptů, které chceme uvařit či v případě, že si chceme najít nějaké faktického informace, které potřebujeme během vzdělávání či v pracovním procesu. S tímto přístupem k obrovskému množství informací se pojí to, že na internet můžeme nyní nahlížet jako na určitou externí paměť, kterou můžeme využívat v případě, že si na něco nemůžeme vzpomenout.

V této souvislosti se mluví o tzv. *Google efektu*. Experimentálně byl sledován vliv primingu na slova spojená s vyhledávači (Yahoo, Google) a na následné vybavování odpovědí na otázky. Studie ukazuje, že lidé při vybavování informací zároveň hned přemýšlí o tom, že si mohou tyto informace vyhledat kdykoliv je budou potřebovat. Také se ukazuje, že lidé mají tendence zapomínat informace, o kterých vědí, že je mohou v budoucnu vyhledat na internetu či jiných externích zdrojích, kde jsou tyto informace uloženy. Na druhou stranu si respondenti ve studii lépe pamatovaly informace, o kterých jim bylo řečeno, že nebudou uloženy a nebude možné je dohledat. Zároveň si respondenti lépe pamatovali, kde mají určitou informaci uloženou než to, co tato informace přesně obsahovala. Automaticky si tedy při vybavování některých informací vybavíme jako první spíše vyhledávač, řekneme si, že si to můžeme "vygoogliť" a až poté přemýšlíme.

Autoři tedy naznačují, že lidská paměť se začíná přizpůsobovat tomu, že máme k dispozici externí zdroj informací a nemusíme si tak zahlcovat vlastní paměť (Sparrow, Liu & Wegner, 2011). Možnost vyhledání jakékoli informace na internetu je často zmiňováno jako jedna z výhod internetu, stejná tvrzení se často objevují i v rozhovorech ve výzkumné části. Zároveň je důležité myslet na to, že informace na internetu nemusí být pravdivé či ověřené a velkou část obsahu internetu tvoří právě uživatelé. Šíření nepravdivých zpráv je ve výzkumné části zmiňováno jako nevýhoda internetu a respondenti tento fakt vnímají jako negativum. Je tedy důležité při vyhledávání informací využívat, pokud možno ověřené zdroje a vlastní kritické myšlení.

2.4. Internetový trolling

S rozvojem komunikace na internetu se pojí mnoho způsobů online chování. Jedna kategorie, která v posledních letech získává stále větší pozornost jak uživatelů, tak odborné veřejnosti, je právě internetový trolling, které se vyznačuje především rušivým a takticky agresivním chováním na internetu (Hardacker, 2010).

Pod termín „internetový trolling" je možné řadit velké množství online chování, které zahrnuje posílání urážejících a ponižujících zpráv, sarkastický humor, ale také přátelské „pošťuchování". V některých případech může internetový trolling mít až kriminální dopad, někdy se jedná o antisociální chování a někdy jeho humorná složka může také sloužit jako jistý druh prosociálního chování (Chen, 2018). Ukazuje se, že působení internetových trollů může mít negativní vliv na psychické rozpoložení oběti trollingu (Satista, 2016) a že trollové mohou mít rušivý a destabilizující vliv. Mohou podkopávat důvěru, sabotují sociální interakce, a dokonce mohou webovým stránkám způsobit právní problémy (Binns, 2012). V roce 2016 uvedlo 88 % adolescentů ve Velké Británii, že na sociálních sítích byli obětí šikany nebo trollingu. Ve výzkumu ve Velké Británii respondenti uváděli, že byli obětí trollingu a u žen se to dále pojilo s obavami o jejich bezpečí i mimo internet (Akhtar & Morrison, 2019).

Internetového „trolla" je možné definovat jako osobu, která schválně vyvolává nebo vyhrocuje konflikty na internetu s účelem vlastního pobavení. Tato osoba často ve svých reakcích či zprávách lže, využívá falešné profily, je takticky agresivní pro zvýšení emocionálních reakcí ostatních uživatelů a upoutává na sebe pozornost tím, že narušuje jinak běžné diskuse či interakce na internetu, především na sociálních sítích a dalších platformách (Hardacker, 2010). Trollové mohou být ve svých reakcích schválně velmi kontroverzní, ponižují nebo urážejí ostatní, právě pro vyvolání reakce (Kunst, 2017).

Ve studii z roku 2018 se dle hloubkových rozhovorů ukazuje, že pod internetovým trollingem je možné najít několik základních vnímaných aspektů. Jako hlavní vlastnost trolla je schopnost provokace, to znamená, že základním úkolem každého trolla je vyprovokovat ostatní uživatele. Zároveň se účastníci výzkumu shodli na tom, že jsou dle jejich názoru schopni rozpoznat v diskusích trolla, jelikož je jeho chování více provokativní a okázalé. Dalším aspektem trollů je klam, podvod nebo lež. Komentáře nebo reakce takového trolla tedy nemusí přesně reflektovat to, co si troll myslí, ale to, co ví, že naštve ostatní uživatele a vyvolá reakci.

Účastníci studie také uváděli, že trolling pro ně je za hranicí únosného chování a shodují se na tom, že trolling může hraničit až s online šikanou ostatních. Na druhou stranu se ale účastníci studie shodli na tom, že humor je také velkou součástí trollingu a některé reakce trollů mohou být humorné. S tím souvisí například vytváření internetových „memes“, což jsou obrázky s vtipným popisem nebo popisující určitou událost, která sice může být vnímána humorně, ale často také může útočit na okolí (Chen, 2018).

Dle starší studie, která se zabývala internetovými trolly se ukazuje, že důvodem rozpoutávání této kontroverze je především to, že jsou někteří uživatelé znudění, vyhledávají pozornost nebo se mstí. Zároveň některým přijde humorné vytvářet uměle konflikty a následně sledovat reakce ostatních uživatelů (Schachaf & Hara, 2010).

Vnímání internetových trollů se mezi uživateli obecně liší a můžeme rozlišit dvě názorové skupiny. První a zároveň větší skupina uživatelů vnímá internetové trolly velmi negativně. Vypovídají o tom, že trollové jednají se zlými úmysly, chtějí ublížit a mohou být potenciálně nebezpeční jak pro jednotlivce, tak pro celé skupiny lidí, jako jsou různé komunity, menšiny apod. Druhá názorová skupina vnímá internetové trolly spíše s humorem, jako uživatele, kteří posouvají obecné hranice, jednají s humorem a rozpoutávají zajímavé názorové debaty. Ti, kteří takto hodnotí internetové trolly se spíše přiklánějí k tomu, že by trollové neměli být bráni vážně a měli by i pro ostatní fungovat pouze jako pobavení (Chen, 2018).

Co se týče prediktorů internetového trollingu, existují důkazy například o tom, že muži se mohou více angažovat v internetovém trollingu než ženy. Zároveň i věk může být prediktorem, kdy mladší uživatelé mají větší tendenci k internetovému trollingu (Cracker & March, 2016). Jedním z často diskutovaných osobnostních rysů, které mohou být prediktorem tohoto chování je spojení s tzv. „temnou tetrádou“ osobnostních rysů, kam patří sadismus, psychopatie, machiavellismus a narcismus. Některé studie ukazují, že jedinci s vysokým skóre v těchto osobnostních rysech mají větší sklon k internetovému trollingu, kdy se ukazuje, že sadismus může být nejsilnějším prediktorem. Lidé s vysokým skóre v sadismu vykazují nižší úroveň empatie a vysokou míru morálního odpoutání, což jim umožňuje „trollovat“ ostatním bez pocitu viny (Volkmer, Gaube, Raue & Lermer, 2023). Dále se ukazuje, že lidé s vyšším skóre dominance a soutěživosti se mohou častěji angažovat v internetovém trollingu. I podle této studie se ukazuje vyšší skóre psychopatie a sadismu jako prediktor internetového trollingu.

Autoři to vysvětlují právě nižší empatií a schopností lhát v mezilidských vztazích (March & Steele, 2020).

Dále se ukazuje, že styl humoru jedince může být dalším faktorem, který predikuje toto antisociální chování. Lidé využívající tzv. agresivní humor mohou mít větší tendenci uchylovat se k internetovému trollingu. Agresivní humor je popisován jako humor zaměřující se na ublížení ostatním za účelem pobavení se. Dále se ukazuje, že agresivní humor může přecházet až do tzv. katagelasticismu, což je pojem označující excesivní posmívání se ostatním vyvolávající pobavení (Brauer, Sendatzki & Proyer, 2022).

Chování jako takové je obecně ovlivněno nejen osobnostními rysy, ale také okolím a situačními faktory, a tak tomu může být i při internetovém trollingu. Ukazuje se, že obecně negativní nálada u některých jedinců může fungovat jako spouštěč internetového trollování. Dalšími faktory může být pocit samoty (Masui, 2022), pocit nudy (Pfattheicher, Lazarevic, Westgate & Schindler, 2021) a pocit anonymity, který dodává internet. Výzkumy tedy ukazují, že trollové nejsou homogenní skupinou – jejich chování a motivace se mohou lišit v závislosti na jejich cílech, platformách, kde působí, a jejich osobnostních rysech (Volkmer, Gaube, Raue & Lermer, 2023).

Internetový trolling je jedním z vybraných psychologických fenoménů, který souvisí s užíváním internetu a do této práce byl blíže popsán právě proto, že uživatelům, kteří jsou obětí trollingu může způsobit výraznou psychickou nepohodu spojenou například s úzkostmi. Internetoví trollové mohou dalším uživatelům způsobit pocit nebezpečí (nebo narušeného bezpečí) na internetu a mohou tak internet udělat místem, kde ostatním uživatelům znepříjemňují jak online, tak off-line život.

2.5. Sociální srovnávání na internetu

Teorii sociálního srovnávání představuje už v roce 1954 sociální psycholog Leon Festinger. V této teorii říká, že lidé mají tendenci se srovnávat s ostatními, s vnějším světem. Jedinci mají tendenci srovnávat své názory, postoje, schopnosti, ale i vzhled. Při sociálním srovnávání mohou nastat tři situace:

- Jedinec srovnává s lidmi na stejné úrovni
- Jedinec se srovnává s lidmi, kteří jsou na tom lépe než on sám – může se tak v něčem zlepšit (srovnávání směrem nahoru)
- Jedinec se srovnává s lidmi, kteří jsou na tom hůře – může si tak říct, že „na tom může být hůř (srovnávání směrem dolu) (Festinger, 1954).

Výzkumy ukazují, že pokud se jedinec srovnává s lidmi, kteří jsou na tom lépe než on sám (směrem nahoru) může zažívat pocit aspirace, optimismu nebo obdivu, stejně tak ale pocit studu, závisti, odporu nebo až deprese. Pokud se jedinec srovnává s lidmi, kteří jsou na tom hůře, než on sám (směrem dolu) může prožívat pocit lítosti, strachu, pýchy, pohrdání, obav nebo soucitu. Zároveň se ukazuje, že princip sociálního srovnávání lidé obecně uplatňují i v situacích, kdy není potřeba nebo jenom v omezené míře (Rosenthal-von der Pütten a kol., 2019).

Sociální sítě a internet obecně nabízí platformu, kde může probíhat sociální srovnávání na každodenní bázi. Sledováním profilů dalších uživatelů je téměř nemožné se vyhnout nějakému srovnávání, ať už směrem nahoru nebo dolů. Dále je důležité si uvědomit, že v off-line světě se většinou jedinci mohou srovnávat pouze s omezeným počtem dalších lidí, se kterými přijdou do kontaktu. V rámci internetu, především sociálních sítí, ale mohou všichni sledovat další uživatele z celého světa, a tak mají mnohem více podnětů pro srovnávání. Zároveň na sociálních sítích má každý uživatel šanci vytvořit co nejlépe vypadající profil sebe sama. Sdílením pouze pozitivních zážitků, radostí či úspěchů, kdy už není nutné sdílet své trápení, těžkosti nebo překážky, které se uživatelům staví do cesty. Na internetu tak každý může vytvořit obraz dokonalého života, kterým se prezentuje, což může být v off-line světě často náročné.

Na sociálních sítích se také setkáváme s tzv. „Likes“ neboli tlačítek „Líbí se mi“, čímž mohou ostatní uživatelé vyjadřovat podporu, zalíbení nebo ocenění zveřejněného příspěvku. Tato malá

ocenění mohou v lidech vyvolávat pocity uspokojení, pochvaly a zároveň podporují v celkovém srovnávání se s ostatními uživateli. Tato ocenění v podobě „likeování“ od ostatních uživatelů funguje také jako odměna (Rosenthal-von der Pütten a kol., 2019).
Očekávání tohoto ocenění na sociálních sítích je dle studií závislé na věku, genderu a množství aktivit a sdíleného obsahu na sociálních sítích. (Grinberg a kol., 2017). Zároveň množství „Líbí se mi“ nebo „srdíček“ na sociálních sítích je některými uživateli vnímáno také jako sociální opora okolí (Wohn a kol., 2016).

Na sociálních sítích se mohou všichni uživatelé srovnávat s ostatními a tyto měřítka se ze subjektivních dojmů mohou nyní kvantifikovat a uživatelé tak mohou porovnávat nejen svůj osobní pocit, ale právě počty ocenění, počet přátel, počet komentářů a interakcí na profilu apod. (Hayes a kol., 2016).

Ukazuje se, že častí uživatelé sociálních sítí mohou mít nižší skóre v oblasti sebehodnocení v souvislosti s neustálým sociálním srovnáváním směrem nahoru na sociálních sítích. Pokud byli respondenti vystaveni profilu, který měl více sociálních interakcí a ocenění než jejich, snižovalo se v důsledku sociálního srovnávání jejich sebehodnocení. Pokud byli respondenti vystaveni profilům, které měli méně aktivit, méně ocenění a srovnávali se tak směrem dolu, nemělo to na jejich sebehodnocení žádný signifikantní vliv. Zároveň čím více respondenti využívali sociální sítě, tím nižší měli celkové hodnocení v oblasti sebehodnocení (self-esteem) (Rosenthal-von der Pütten a kol., 2019). Tato zjištění jsou zajímavá právě z toho důvodu, že srovnávání směrem nahoru, kdy respondenti byli vystaveni zdánlivě „lepším“ či více oceňovaným uživatelům, snižovalo se jejich sebehodnocení, ale pokud byli vystaveni profilům, kde se mohli porovnávat směrem dolů, tak se s jejich sebehodnocením nic nestalo, tzn. nezvýšilo se jim jejich sebehodnocení. Ne všechny výzkumy však ukazují na negativní výsledky. Některé studie zdůrazňují pozitivní aspekty používání sociálních médií, jako je možnost zvýšit sociální kapitál, získat pozitivní zpětnou vazbu a zažít stav „flow“ během pohlcujících aktivit, což může zvýšit psychický well-being. Zdá se, že klíčové faktory určující, zda má používání sociálních médií pozitivní nebo negativní dopad, závisí na tom, jak a proč jednotlivci tyto platformy používají, a také na jejich osobních charakteristikách, jako je sebehodnocení a sítě sociální podpory (Vogel, Rose, Roberts & Eckles, 2014).

Obecně se tedy ve výzkumech ukazují rozporuplné výsledky, kdy sociální srovnávání na sociálních může mít negativní vliv na vlastní sebehodnocení, může způsobovat nižší sebevědomí a negativně tak působit na well-being jedinců. Na druhé straně může užívání sociálních sítích snižovat pocit izolovanosti, zvyšuje pocit intimity a pomáhá navazovat vztahy.

3. Bezpečnost na internetu

Celosvětově se počet uživatelů internetu od roku 2000 do roku 2019 zvedl o 1167 %, přičemž v Evropě došlo k nárůstu uživatelů internetu od roku 2000 do roku 2020 o 601,3 % (Miniwatts, 2021). Téma bezpečnosti na internetu není tématem pro výzkumy novým. Například hrozby napadení počítače virem lze sledovat až 30 let nazpět a fenomén známý jako phishing je možné zdokumentovat až do roku 2003. Přesto se s rozrůstajícím užíváním internetu zvyšuje množství potenciálních rizik, což poukazuje na větší nutnost ochrany uživatelů internetu (Furnell, 2008).

S celkovým nárůstem uživatelů internetu se pojí i zvýšení možných rizik. Je nutné zmínit, že chápání bezpečnosti na internetu může být u každého jedince odlišné a je velmi závislé na kontextu (Quan-Hasse & Ho, 2019). Ani jednotlivé aktivity na internetu nelze apriori označit za pozitivní či negativní. Závislost na kontextu a osobním vnímání každého jednotlivce lze prezentovat na příkladu "sextingu" (psaní a přijímání zpráv se sexuálním kontextem), kdy sexting může být zasazen do různého kontextu. Například pokud jedinec dostane zprávu se sexuálním kontextem od neznámého člověka, může to být zraňující, nepříjemné nebo urážlivé. Na druhé straně může jedinec takové zprávy ignorovat či dokonce vnímat jako pozitivní. Jiná situace může nastat, když taková zpráva přijde od blízkého člověka - partnera/partnerky. Takové zprávy mohou být potěšující či vzrušující, ale také mohou být vnímané nevhodně. Je tedy důležité se vždy zamyslet nad kontextem, nad každým jednotlivcem a jeho vnímáním konkrétní situace.

Velkou součástí bezpečnosti na internetu je samotné soukromí na internetu. Soukromí na internetu je chápáno jako *"právo každého jednotlivce na ochranu před neoprávněným zveřejněním osobních údajů, před neoprávněnou publicitou, kontrolou, použitím nebo dohledem nad informacemi nebo činnostmi, které jedinec zveřejňuje nebo provozuje na internetu"* (Quan-Hasse & Ho, 2019). Jednou věcí je právo na soukromí každého jedince, na druhé straně je ale nutné vyvážit množství informací, které o sobě na internetu sdílíme. Pokud stále zveřejňujeme soukromé informace, které nechceme, aby byly zneužity třetí stranou, musíme také myslet na to, že rizika zneužití dat jsou stále aktuální a mohou ohrozit každého, kdo se nechová na internetu zodpovědně. S tím je důležité dodat, že bezpečnost na internetu a ochrana vlastních dat je velmi ovlivněná osobní zodpovědností každého jedince, který se na internetu pohybuje (Shillair a kol., 2015). V roce 2007 se ale ve výzkumu ukázalo, že někteří respondenti nepovažují ochranu a bezpečnost na internetu za svou zodpovědnost nebo se

považují za nekompetentní se na internetu efektivně ochránit. Mají tedy pocit, že za bezpečnost na internetu by měly zodpovídat vyšší instituce či organizace a firmy, které poskytují internetové služby (LaRose & Rifon, 2007). R. Shillairová a kolegové (2015) se ale shodují na tom, že pro zabezpečení uživatelů na internetu je nezbytné, aby získali více sebevědomí ve vlastní schopnosti při ochraně dat, měly by se podporovat výukové programy, ale zároveň je nezbytné, aby uživatelé přijali svou osobní zodpovědnost jako důležitý protektivní faktor (Shillair a kol., 2015).

Chování směřující k vyšší bezpečnost na internetu je přímo spojené s prožívaným pocitem soukromí na internetu. Soukromí je chápáno jako vícerozměrný konstrukt, na který je téměř nutné nahlížet multidimenzionálně. L. Baruh a Z. Cemalcilar (2014) navrhují čtyři potenciální dimenze postojů k ochraně soukromí:

1. Obavy o vlastní soukromí
2. Přesvědčení, že soukromí na internetu je hodnota, kterou je potřeba zákonně chránit;
3. Spoluzávislost soukromí (víra, že soukromí jednoho člověka je nějakým způsobem závislé na tom, jak opatrní jsou ostatní uživatelé internetu)
4. Obavy o soukromí ostatních (především respektování soukromí ostatních uživatelů)

Ukazuje se, že všechny čtyři zmíněné dimenze postojů k ochraně soukromí souvisí s přijetím bezpečnostních opatření na ochranu soukromí. Žádná z nich ale významně nesouvisela s chováním na internetu, především se zveřejňováním informací na sociálních sítích, konkrétně na Facebooku. Toto čtyřrozměrné pojetí zahrnuje výsledky studií a poznatky z dalších výzkumů zmíněných výše (LaRose & Rifon, 2007; Shillair a kol., 2015). Součástí bezpečnosti na internetu je tedy osobní zodpovědnost a obavy o své soukromí, které vedou k ochraně svých dat. Dále je to bezpečnost jako hodnota, kterou by měly zajišťovat vyšší instituce. K tomu je možné přidat také zmíněné obavy o soukromí dalších uživatelů a to, jak se ostatní na internetu chrání.

3.1. Obavy uživatelů internetu

Čas trávený na internetu může způsobit jisté odpojení od fyzické reality a uživatelé jsou mnohdy připojeni několik hodin v kuse. Zároveň dnešní doba očekává, že k internetu jsme připojeni a budeme takto propojeni s okolním světem. S tím také souvisí fakt, že na internetu sdílíme velké množství informací, které mohou být zneužity. Čím vyšší je využívání internetu, tím větší jsou potenciální hrozby (Mehraj, Jayadevappa, Haleem et al., 2021).

Samotná myšlenka „odpojení" a odpojení se od online světa a s ním spojených technologií stále méně lákavá., protože může vést k sociální izolaci i mimo online svět, způsobuje FOMO apod. Ve studii k 25. výročí internetu (World wide web) organizace Pew Internet and American Life Project uvádějí, že 87 % dospělých američanů je online, z toho 53 % potvrdilo, že internet je nezbytnou součástí jejich života. Výzkumy v dalších letech s podobnou tematikou ale toto dřívější pozitivní hodnocení nepotvrzují. Studie Pew Internet říká, že 41 % všech dospělých Američanů osobně zažilo nějaký druh internetového obtěžování a 62 % považuje online obtěžování za velký problém (Duggan, 2017).

Schaik a kolektiv (2021) porovnávali vnímaná online rizika vysokoškolských studentů ve Velké Británii a USA. Potenciální rizika na internetu rozdělili do několika kategorií: Online sociální (virtuální stalking, kyberšikana, ...), rizika související s identitou uživatelů (krádež identity, phishing), softwarová rizika (viry, spyware, trojské koně, ...), monitorovací rizika (sledování internetu) a bez odpovědi (N/A). Nejvyšší vnímaná rizika jsou krádež identity, keylogger, kyberšikana a sociální inženýrství (Schaik et al., 2021). Z těchto výsledků je zřejmé, že uživatelé se neobávají pouze technických a softwarových rizik, ale zaměřují se také na svou osobní bezpečnost, narušení vlastní integrity a soukromí na internetu.

Mezi časté obavy uživatelů internetu můžeme dále dle Mehraj a kol. (2021) zařadit krádež a zneužití osobních informací, phishing, profilování, podvodný prodej na internetu spojený se ztrátou dat nebo ohrožení vlastní identity a reputace. Mezi další obavy, které mohou mít uživatelé internetu, a především sociálních sítích, může být zařazeno například online zastrašování. Predátoři nyní mají velkou šanci najít svou oběť online. Dříve byla šikana v podstatě pouze tváří v tvář, takže alespoň doma nebo na bezpečných místech mohl mít jedinec svůj bezpečný prostor. Nyní ale může predátor nebo agresor působit i online, čímž narušuje i

tento bezpečný prostor oběti. Zároveň těmto agresorům vyhovuje to, že na internetu mohou být v anonymitě.

Dále fakt, že jsou data uživatelů využívána třetí stranou, například k prodeji či cílené reklamě, může být některým uživatelům nekomfortní. I když je ve většině případů k této práci se sdílenými daty dávají jedinci souhlas, aniž by o tom často věděli (souhlasí s podmínkami využívání stránky, odkliknout cookies apod.). Další zmiňovanou obavou spojenou s užíváním internetu je sociální izolace. Tím, že máme kontakty online může docházet k tomu, že se lidé navzájem izolují v off-line světě. Další výraznou obavou může být právě vznik závislostí na sociálních sítích (Jain, Sahoo & Kaubiyal, 2021).

Obavy o své soukromí na internetu zahrnují také nepříjemné pocity týkající se možného zneužití osobních informací uživatelů. Důsledkem těchto obav by měla být potřeba aktivního ochránění svých osobních údajů před dalšími uživateli (Dienlin & Trepte, 2015). Toto zneužití osobních informací je zmiňováno v mnoha studiích a zároveň se objevilo i ve výsledcích diplomové práce autorky, kdy tento strach či obava byla popsána především v oblasti sociální bezpečnosti na internetu. Stejně jako ve studiích Dienlin & Trepte (2015) nebo Jain, Sahoo & Kaubiyal, (2021) i v diplomové práci respondenti zmiňovali jako velmi nekomfortní to, že jejich data jsou dále využívány třetí stranou a stává se z nich jakási „měna“ na internetu. Ve výzkumu v diplomové práci respondenti také mluvili o strachu z odposlouchávání telefonů, sledování polohy, sledování aktivit na internetu, a to buď vládou nebo nadnárodními (např. reklamními) společnostmi (Kopáňková, 2021).

Jain, Sahoo a Kaubiyal (2021) rozdělují možné hrozby na internetu do tří kategorií, podle toho, co mohou uživatele internetu v současné době prožívat. Tyto tři kategorie jsou:

- Konvenční či běžné hrozby na internetu
- Moderní hrozby na internetu
- Cílené hrozby na internetu

Konvenční nebo běžně se vyskytující hrozby na internetu jsou hrozby, které uživatelé zažívají v podstatě od počátku využívání internetu. Mezi tyto hrozby patří například spam, který se nejběžněji přeposílá skrze e-mail a jedná se o reklamní zprávy s potenciálně nebezpečným či ohrožujícím obsahem. Malwareové útoky zahrnující „nabourání“ se do počítače či zařízení uživatele. Uživatelé mohou kliknout na nebezpečný odkaz přeposlaný e-mailem, v jehož důsledku mohou cizím uživatelům poskytnout přístup ke svému zařízení a ke svým datům, které

mohou být zneužity. Phishing je způsob, kterým hackeři mohou získávat citlivé údaje ostatních uživatelům, jako jsou například hesla či detaily platebních údajů, což může vést ke značné materiální či finanční ztrátě oběti. Poslední kategorií, kterou autoři řadí mezi konvenční hrozby na internetu je krádež identity, kdy jiný uživatel ukradne identitu (profilový obrázek, jméno a další informace) a vystupuje pod tímto ukradeným profilem. Tímto způsobem může docházet ke zneužívání důvěry dalších uživatelů nebo k narušení osobní reputace okradeného jedince.

Mezi moderní hrozby patří například tzv. Cross-site scripting útok. Při tomto útoku může uživatel, který nic netuší kliknout na odkaz, který přepíše vlastnosti stránky, na které se nachází a opět dovolí útočníkovi přístup k zařízení uživatele. Přes takto zašifrované stránky se může následně útočník „schovat" a využít tak zařízení či přihlášení jiného uživatele buď k okradení nebo pro další vystupování na internetu. Další moderní hrozbou je tzv. klonování profilů. Útočník „naklonuje" či duplikuje profil jedince a dále vystupuje pod jeho jménem či profilem za účelem získání důvěry jeho okolí. Tento typ útoku může být využit pro další útoky na internetu jako je kyberšikana, kyberstalking nebo vydírání. Dalšími typy hrozeb může být například útok „Sybil", „Clickjacking" nebo de-anonymizace. Všechny tyto způsoby útoků jsou složitější hackerské práce, které mohou být uživatelům neznámé. Všechny ale mají za cíl zneužít informace ostatních uživatelů, schovat se za jejich zařízení pro páchání mnohdy i trestné činnosti bez vypátrání opravdového viníka, zneužití dat a další. Když tedy respondenti uvádějí, že mají obecně strach ze zneužití dat a z ukradení identity, mohou za tímto označením být „skryté" všechny (a mnohem více) různých hackerských útoků i na profily běžného uživatele internetu.

Mezi cílené hrozby autoři řadí hrozby, které jsou přímo namířené vůči jednomu konkrétnímu jedinci, který je jejich obětí. Mezi tyto hrozby je možné zařadit například kyberšikana, kybergrooming nebo kyberstalking. Kyberšikana je způsob šikany či obtěžování dalšího jedince přes online platformy jako jsou sociální sítě, e-maily, chaty apod. Jako kybergrooming je označována aktivita, kdy se útočník schovává za vymyšlenou identitou a navazuje tak kontakt s potenciální obětí sexuálního zneužívání. Po navázání důvěry s obětí většinou útočník vyláká oběť k osobnímu setkání, kdy může dojít k napadení, sexuálnímu napadení či znásilnění. Zároveň může od oběti získat citlivé informace nebo dokonce intimní fotografie, které může útočník využít k dalšímu vydírání oběti. Obětmi kybergroomingu mohou být děti i dospělí. Kyberstalking je variantou stalkingu, kdy jde o opakované, systematické kontaktování a pronásledování oběti (Jain, Sahoo & Kaubiyal, 2021).

Obavy uživatelů na internetu mohou být jedním z prediktorů jejich dalšího chování a zabezpečení. Jedná se také o jednu z hlavních součástí Protekčně motivační teorie – PMT, která je součástí výzkumu v této práci. V PMT se pracuje především s vnímanou pravděpodobností vzniku potenciální hrozby, s její závažností a se strachem z této hrozby. Nejčastější obavy, které mají uživatelé na internetu mohou být nápomocné při tvorbě intervenčních programů nebo dalším zkoumání tohoto fenoménu.

3.2. *Vnímání bezpečnosti na internetu*

Jak jsem již zmínila v předchozí kapitole "Bezpečnost a chování na internetu", vnímání bezpečnosti na internetu a na to navazující chování je závislé na kontextu a situaci, která se týká konkrétního jedince. Pro někoho může být určitá situace již potenciálně riziková či nepříjemná, někdo jiný ji může vnímat jako pozitivní či neutrální (to může zahrnovat např. posílání intimních fotografií či zpráv). Na druhé straně napadení virem či ukradení profilu či hesla k internetovému bankovnictví si lze těžce představit jako pozitivní či neutrální zkušenost. Předpokládám, že taková situace by pro každého jedince byla přinejmenším nepříjemná. Je tedy otázkou, zda je možné bezpečnost na internetu ještě dále nějakým způsobem dělit, zda jsou různé "druhy" potenciálně rizikových situací a jaký vliv na nás mají různé situace.

Nejčastější obavy, které mohou být spojeny s užíváním internetu je zneužití osobních údajů, které jsou zveřejněny online (Barnes, 2006), dále mohou mít lidé obavy ohledně internetového bankovnictví, ohledně ukradení identity či profilu na internetu, kyberšikany anebo obavy týkající se tzv. chytré domácnosti či monitorovacích či medicínských technologií, které fungují přes internet (Townsend, Knoefel & Goubran, 2011, Alhabash a kol., 2015; Bartsch & Dienlin, 2016;).

K. Raynes-Goldieová (2010) například rozděluje bezpečnost a soukromí na internetu na dva druhy. První je ochrana soukromí **institucionální**, druhá je **sociální**. Toto rozdělení popisuje možné rozdíly v tom, jak je možné vnímat bezpečnost na internetu. Institucionální vnímání bezpečnosti na internetu zahrnuje sběr informací o uživatelích internetu třetí stranou (organizace, reklama apod.); organizace, které mají osobní informace o uživatelích (politické stránky, pojišťovny, firmy nabízející slevy apod.); předávání informací o uživatelích třetím stranám, organizace prodávající informace o uživatelích třetím stranám a přístup vlády k informacím sdílených na internetu.

Institucionální ochrana soukromí by tedy měla být mířena na možný prodej či poskytování informací o uživatelích dalším organizacím či sběr informací vládou.

Mezi sociální stránku bezpečnosti na internetu patří obavy ohledně ztráty kontroly nad svými informacemi, sdílení příliš velkého množství informací nebo odhalení sebe sama. Lidé také nechtějí, aby celý svět věděl všechno: co kdo dělá, kde se nachází, osobní zkušenosti, zážitky apod., zároveň uživatelé nechtějí, aby další lidé věděli příliš osobní informace, které mohou být následně použity k ublížení, ponížení či vydírání dalšího jedince (Quan-Haase & Ho, 2019). S ponížením, ublížením a využíváním informací na internetu souvisí také online disinhibiční efekt. Tento efekt zahrnuje to, že se uživatelé internetu vyjadřují jiným způsobem, v jiné intenzitě a frekvenci, než se vyjadřují v offline světě. Tento efekt může být i pozitivní, kdy lidé ukazují neobvyklou míru přívětivosti. Na druhé straně je tzv. toxická disinhibice, která se pojí s krutostí, negativními až posměšnými komentáři nebo vulgarismy (Suler, 2004). Do sociálních obav je možné zařadit také fenomén FoMO (angl. *Fear Of Missing Out*), což je fenomén strachu z vynechání událostí, zpráv nebo důležitých příspěvků, které se na internetu objevují (Przybylski, Murayam, DeHaan & Gladwell, 2013).

Podobně popisují sociální oblast bezpečnosti a ochranu soukromí na internetu E. Hargittai & A. Marwick (2016), kteří uvádějí především obavy lidí z toho, že jejich informace či příspěvky někdo může zneužít právě k ponížení či vyvolání konfliktu jedince s jeho přáteli, rodinou či partnerem. Další obava je ze stalkingu či sdílení osobních informací, což by mohlo také vést k osobní nepohodě prožívané v souvislosti s užíváním internetu (Lutz & Ranzini, 2017). Institucionální bezpečnost na internetu zahrnuje obavy uživatelů o to, jak a jaké organizace mohou využívat osobní informace nebo zda může vláda sledovat aktivity lidí pomocí informací na internetu (Lutz & Ranzini, 2017).

A. Quan-Haaseová a D. Ho (2019) přidávají ještě třetí možný rozměr vnímání bezpečnosti na internetu. Vedle institucionální a sociální bezpečnosti doplňují ještě **technické pojetí bezpečnosti**. Tento třetí rozměr zahrnuje právě obavy z technických možností napadení počítače či zařízení, které lidé využívají k přístupu na internet. Respondenti uváděli především obavy z hackerského útoky, z napadení viry, ze ztráty dat nebo z ukradení identity, informací k internetovému bankovnictví apod.

Pro přehlednost jsem vytvořila *Tabulku 4. - Rozdílné vnímání bezpečnosti na internetu*, kde jsou rozděleny obavy, které mohou uživatelé internetu mít v rámci každé ze zmíněných

možností, jak na zabezpečení na internetu nahlížet. Na bezpečnost na internetu je tedy možné nahlížet z několika aspektů, stejně tak můžeme nahlížet i na informace, které na internetu sdílíme. M. Taddickenová (2014) například rozděluje informace, které o sobě na internetu můžeme sdělovat na dvě kategorie. První kategorií jsou faktické informace, které zahrnují například příjmení, datum narození, profesi a poštovní adresu. Druhou kategorií jsou citlivé informace, které zahrnují například sdílené fotografie, zážitky, zkušenosti, pocity, myšlenky, obavy a strachy. Pokud tedy spojíme druhy informací, které můžeme na internetu sdílet a možností vnímání bezpečnosti na internetu, každá informace může působit jiné obavy a potřebuje také jiné strategie ochrany.

Obavy týkající se institucionální bezpečnosti	**Obavy týkající se sociální bezpečnosti**	**Obavy týkající se technického zabezpečení zařízení připojeného k internetu**
Organizace shromažďující informace o uživatelých	Ztráta kontroly nad vlastními informacemi	Obavy z napadení systému dalšími lidmi či entitami
Organizace využívající informace o uživatelých v oblasti reklamy, politických či pojišťovacích stránek či služeb	Přílišné sebeodhalení	Obavy z hackerských útoků
Prodej či předání informací o uživatelých třetím stranám	Všichni ostatní mohou vědět, co se děje v životech jiných uživatelů, znají jejich polohu nebo osobní zážitky	Obavy z rozesílání virů, spamů apod.
Sledování uživatelů internetu vládou a dalšími institucemi	Strach z využití osobních informací k ublížení, ponížení či ke konfliktu	Obavy ze ztráty dat, ukradení osobních informací či přístupů k účtům nelegální cestou

Tabulka 4. - Rozdílné vnímání bezpečnosti na internetu

Zároveň poznatky z těchto studií korespondují s výsledky výzkumu v diplomové práci, kde bylo vnímání bezpečnosti na internetu popsáno jako komplexní fenomén s nejméně třemi složkami, dle kterých mohou uživatelé bezpečnost na internetu vnímat. Mezi tyto popsané

složky bezpečnosti na internetu je technická, sociální (osobní) a institucionální. Tyto složky či dimenze korespondují mimo jiné s vlastními či zprostředkovanými zkušenostmi uživatelů na internetu. To znamená, pokud se jedinci nejčastěji setkávali s narušení sociální či osobní složky bezpečnosti (sebeodhalení, zneužití informací, vyvolání konfliktu), považují tuto složku za zásadnější a výraznější. Pokud se častěji setkávali se situací, kdy měli v počítači vir či byli obětí spamů, phishingu apod. byla pro ně tato složka bezpečnosti zásadní a mluvili o ní častěji. Ne všichni respondenti hovořili o institucionální bezpečnosti na internetu, nicméně pokud ano, jednalo se o pro ně velmi zásadní součást diskomfortu a pocitu nebezpečí na internetu. Do této složky řadí respondenti především jejich obavy ohledně sledování telefonických a dalších zařízení vládou, reklamními společnostmi, odposlouchávání, sledování polohy a zneužití jejich digitální stopy.

3.3. Strategie ochrany a zabezpečení na internetu

Na předchozí podkapitolu logicky navazuje další část, ve které jsou popsány možné strategie, které lidé využívají pro svou ochranu na internetu. K samotné bezpečnosti a chování na internetu neodmyslitelně patří také možné nástroje či postupy, které můžeme využít pro to, abychom své soukromí na internetu ochránili.

Pro ochranu osobních informací lidé využívají různé strategie. Strategie ochrany soukromí na internetu jsou chápány jako techniky, které jedinci využívají k ochraně svých informací a ke zmírnění potenciálního narušení svého soukromí. Strategie ochrany soukromí zahrnují především aktivní zapojení uživatelů k ochraně svých informací (Young & Quan-Haase, 2013).

Nejjednodušší forma ochrany dat na internetu je samotné nezveřejňování těchto informací. S touto strategií je ale spojen tzv. *paradox ochrany soukromí* (angl. *The privacy paradox*). Tento paradox popisuje ochotu lidí zveřejňovat své osobní údaje např. na sociální sítích, přičemž na druhé straně vyjadřují vysoké znepokojení ohledně svého soukromí. To znamená, že lidé jsou často znepokojeni tím, že by někdo mohl zneužít jejich osobní informace, ale zároveň tyto informace zveřejňují, nejčastěji na sociálních sítích (Barnes, 2006; Young & Quan-Haase, 2013; Taddicken, 2014).

I když mají uživatelé internetu často obavy o svá data, velké množství uživatelů se ne vždy chová příliš bezpečně. Už v roce 2007 signifikantní množství respondentů ve studii otevíralo e – maily s pochybným obsahem, stahovali malware, používali slabá hesla, klikali na pop-up

(vyskakovací) reklamy, rozklikávali odkazy zaslané v e-mailech od neznámých lidí, stahovali nezabezpečené soubory či se registrovali na pochybných webových stránkách (LaRose & Rifon, 2007). Všechny tyto aktivity jsou rizikové a mohou vést k napadení počítače a dalším potenciálně rizikovým následkům, jako je ukradení dat. Dalším problémem je zveřejňování soukromých informací na internetu. V roce 2013 téměř dvě třetiny respondentů v USA sdílely své soukromé fotografie na sociálních sítích, 50 % uvádělo datum narození, 46 % svou e-mailovou adresu, 44 % svého zaměstnavatele či firmu, ve které pracují a 30 % uvedlo i svou adresu bydliště (Rainie, Kiesler, Kang & Madden, 2013).

Některé starší studie ukazují, že například adolescenti využívají několik strategií, jak své soukromí na internetu, zvlášť na sociálních sítích, ochraňovat, v rámci sociální bezpečnosti na internetu. Mezi tyto aktivní kroky ke své ochraně lze řadit vymazání některých lidí ze seznamu přátel, zablokování některých jedinců a někteří o sobě zveřejňují falešné, vymyšlené informace (Madden a kol., 2013). Další technikou k ochraně údajů může být odznačování sebe samého z fotek nebo příspěvků, které byly zveřejněny. Tato strategie může napomoci k tomu, aby profil jedinců nebyl tak snadno dohledatelný přes profily jiných lidí a přátel (Dhir, Kaur, Linka & Nieminen, 2016).

Jak již bylo několikrát zmíněno, většina studií, která sledují ochranu a bezpečnost na internetu se věnuje právě adolescentům nebo mladým dospělým, kdy jsou data sbírána nejčastěji na studentech vysokých škol. Analýzou 153 starších dospělých ve věku 50-93 let, kteří mají sociální sítě a využívají je, bylo ukázáno, že tato věková kategorie využívá další strategie pro svou ochranu. Tito respondenti využívali například na sociálních sítích místo vlastního jména a příjmení pseudonymy pro udržení určité anonymity. Z celkového výzkumného souboru pouze 6 % uvádělo na svých profilech své křestní jméno a téměř žádný z respondentů na sociálních sítích neuváděl své příjmení. Nejčastěji tedy využívali různé přezdívky nebo křestní jméno s přezdívkou (Maaß, 2011). Tato strategie, kdy na svém profilu nezveřejníme naše celé skutečné jméno zamezí tomu, aby si nás na sociálních sítích mohl kdokoliv vyhledat.

Ve výzkumu A. Quan-Haaseové a D. Ho (2019) se autoři zabývali právě strategiemi, které dospělí využívají pro svou ochranu na internetu. Z výzkumu vyplývá sedm základních strategií, kteří respondenti nejčastěji využívali.

První strategií je **omezení informací, které sdílejí na internetu.** Nejčastěji se tato strategie odrážela v minimalistickém profilu na sociálních sítích. Respondenti nesdíleli především jejich

věk, e-mailovou nebo poštovní adresu, místo bydliště nebo informace o jejich financích. Nejvíce skeptická byla skupina respondentů ohledně sdílení informací na sociálních sítích.

Druhou nejčastější strategií bylo **vyhýbání se využívání některých stránek nebo služeb na internetu.** Toto pravidlo zahrnuje především to, že se respondenti vyhýbali využívání a navštěvování určitých stránek, u kterých měli pocit, že po nich požadují "příliš informací". Jednou z často zmiňovaných služeb bylo internetové bankovnictví, ve kterou měli respondenti malou důvěru.

Další strategií bylo **ignorování nebo vymazání nevyžádaných, neznámých či podezřelých zpráv nebo žádostí.** To zahrnovalo vymazání či ignorování podezřelého e-mailu nebo e-mailu od neznámého uživatele, ignorování podezřelých či neznámých žádostí o přátelství na sociálních sítích nebo návrhy na zapojení se na stránky, které respondenti neznali.

Využívání specifického hardwaru či softwaru bylo další využívanou strategií pro ochranu osobních údajů na internetu. Respondenti například uváděli, že využívají počítače Mac raději než PC, protože mají pocit, že počítače Mac mají lepší zabezpečení před viry a dalšími hackerskými útoky než počítače PC. Zároveň uváděli, že mají svůj počítač zabezpečený speciálním antivirem, takže se nemusí bát napadání viry.

Využívání pseudonym a přezdívek na internetu bylo jako strategie zmíněno i výše ve výsledcích výzkumu W. Maaße (2011). Respondenti využívají buď přezdívky nebo upravují své jméno tak, aby nebylo snadné je na internetu dohledat. Respondenti uváděli, že pseudonymy využívají především v situaci, které je pro ně neznámá nebo nepříjemná.

Předposlední nejčastější strategií bylo **limitování přístupu k soukromému profilu**. Respondenti tedy často uváděli možnosti nastavení soukromí, které mají na sociálních sítích. Nejčastěji tedy limitují přístup ke svému profilu právě pro okruh svých přátel a nechtějí, aby jejich soukromé fotografie, které sdílejí online, mohl vidět i někdo cizí.

Poslední strategií, kterou respondenti uváděli je **používání hesel**. Autoři ale uvádějí, že je poměrně překvapivé, že někteří respondenti uvedli jako strategii ochrany soukromí na internetu právě užívání hesel. I přesto, že respondenti se snaží mít hesla složitá a pravidelně si je mění, většina profilů či služeb, které na internetu využíváme hesla vyžadují. Zároveň jsou tak hesla častým cílem útoků právě kvůli tomu, aby mohl mít cizí uživatel přístup k profilu daného

jedince. Autoři tak uvádějí, že je to možné místo pro intervenci a zvýšení povědomí o tom, že heslo k profilu nemusí znamenat to, že je náš profil imunní vůči útokům jiných uživatelů.

Už jenom ze samé podstaty trvalosti informací na internetu a s ohledem na to, že nad informacemi a údaji, které jsou sdílené na internetu nemusíme mít již dostatečnou kontrolu, je poměrně přirozené, že lidé, kteří internet a technologie využívají mají také obavy a strach o své soukromí. Zároveň jak bylo zmíněno výše, je téměř nemožné se izolovat od využívání internetu. Je tedy potřeba najít balanc mezi tím, co o sobě jedinec na internetu může sdílet a jaké informace mohou být zveřejněny a jaké jsou naopak moc citlivé nebo osobní. Zároveň pro každého uživatele by mělo být zásadní udělat alespoň několik základních kroků k tomu, aby své soukromí na internetu ochránili. Zároveň je nezbytné využívat různé strategie a techniky ochrany v rámci různých aktivit na internetu. Jinou strategii využíváme při používání sociálních sítí, při online seznamování, při používání e-mailu či v internetovém bankovnictví.

Na jedné straně se jedná o technické zabezpečení počítače, což zahrnuje především instalaci antivirového programu a pravidelnou aktualizaci jak systému počítače, tak právě antiviru. Na druhé straně se jedná o to, jak se sami můžeme na internetu chovat, abychom co nejvíce zamezili případnému naplnění obav, které můžeme mít.

Při samotném zamyšlením se nad možnými strategiemi, které vedou k ochraně vlastního soukromí na internetu, každého napadne mnoho rad, pravidel či postupů, jak se ochránit. Mezi prvními strategiemi, které by mohly většinu uživatelů napadnout jsou právě zmíněné techniky technického zabezpečení svého zařízení, přes které se připojujeme na internet. Na druhé straně jsou již vlastní činy všech jednotlivých uživatelů, zahrnující právě sebeodhalení a důvěru v ostatní uživatele, které mohou buď pomoci při ochraně či uškodit při zachování soukromí. Toto je spojeno s poznatky R. Shillairové a kolegů (2015), kteří právě uvádějí osobní zodpovědnost jako důležitý protektivní faktor. Konkrétně na internetu a v dalších zdrojích najdou uživatelé mnoho informací, které se týkají bezpečnosti na internetu a na které se mohou obrátit, pokud si nejsou postupem ochrany jisti. Například Jain, Sahoová a Kaubiyal (2021) nabízí přesný postup pro uživatele sociálních sítí a seznam pravidel, který by měli pro své zabezpečení dodržovat:

- **Využívat silná hesla:** Heslo by mělo být dostatečně dlouhé, neuhodnutelné a mělo by obsahovat číslici a speciální znaky. Uživatelé by měli používat různá hesla k různým účtům.

- **Nesdílet svou polohu s aplikacemi či dalšími lidmi**: Sdílení své polohy je v současné doby trendem a zároveň většina aplikací se uživatelů na jejich polohu ptá nebo dokonce nabízí její sdílení, autoři tedy radí toto sdílení polohy limitovat či úplně zrušit.
- **Být opatrný s přidáváním dalších uživatelů do seznamu přátel:** Ukazuje se, že lidé si přidávají přátele na základě společných přátel, aniž by blíže zkoumali, o koho se jedná, což může být chybou. Před přidáním kohokoliv do seznamu přátel by si uživatelé měli být jistí, že tohoto jedince v seznamu přátel chtějí mít.
- **Být opatrný ohledně sdílených informací:** Uživatelé by před zveřejněním určité informace měli přemýšlet nad tím, co všechno touto informací zveřejní, zda zveřejňují informace pouze o sobě nebo i o dalších lidech ze svého okolí. Zároveň by si měli být vědomi toho, co může sdílení určité informace způsobit.
- **Být opatrný při rozklikávání neznámých odkazů:** Tímto autoři míří právě na posílání virů, malwareové útoky, phishing apod. Každý uživatel internetu by měl přemýšlet nad tím, na jaký odkaz kliká. Pokud do e-mailu přijde zpráva, že vyhráváme milion dolarů a dovolenou, jedná se pravděpodobně o potenciální nebezpečí v podobě viru a dalších.
- **Mít nainstalovaný antivir:** Antivirus může lépe než uživatel zaznamenat potenciální hrozbu, takže může být velmi nápomocný při ochraně. K tomu se samozřejmě pojí také pravidelná aktualizace systému a péče o svá zařízení. (Jain, Sahoo & Kaubiyal, 2021).

Podobných seznamů či návodů, jak se zabezpečit na internetu, existují desítky. Uživatelům radí, jak se chovat bezpečně na sociálních sítích, při užívání internetového bankovnictví, při online seznamování, nakupování, posílání e-mailů či při připojení se k bezdrátové internetové síti. Je ale otázka, zda je možné aplikovat všechna tato pravidla do každodenního života nebo zda opravdu stačí několik základních pravidel a strategií pro ochranu své bezpečnosti na internetu. Toto zamyšlení nad bezpečností na internetu je možné porovnat také s výše zmíněním paradoxem ochrany soukromí – máme sice obavy o vlastní bezpečnost, ale na našem chování na internetu se to nemusí odrážet, protože někdy může být například zvědavost silnější než vědomí potenciálního nebezpečí.

3.4. Vybrané faktory související s chováním a bezpečností na internetu

V následující kapitole autorka popisuje vybrané fenomény, které jsou spojovány s chováním a bezpečností na internetu. Mezi tyto vybrané faktory patří vzdělání, gender, osobnostní rysy nebo styly attachementu. Zároveň je ale důležité zmínit, že chování je ovlivněno nejen těmito měřitelnými faktory, které patří k vlastnostem či dovednostem uživatelů, ale je ovlivněno také okolními faktory, prostředím a dalšími lidmi v něm.

Prvním faktorem je vzdělání a znalosti týkající se zabezpečení na internetu. Znalosti týkající se digitálních technologií a internetu mohou fungovat jako protektivní faktor při ochraně na internetu. S tím dále souvisí otázka, zda samotné vzdělání má nějaký vliv na to, jak se lidé na internetu chrání, zda ovlivňuje jejich přemýšlení, obavy či chování směřující k bezpečnosti na internetu

J. Brands a J. van Wilsem (2019) zkoumali souvislost mezi strachem z okradení či finanční kriminality na internetu a protektivním chováním. Jejich výsledky ukazují, že respondenti s vyšším vzděláním vykazují nižší úroveň strachu z hrozícího finančního napadení (ukradení peněz, přístupu k internetovému bankovnictví apod.) Zároveň se ukazuje, že čím větší strach mají lidé z těchto rizik, tím méně využívají online platby či internetové bankovnictví (Brands & Wilsem, 2019). To může indikovat, že lidé s nižším vzděláním mohou méně využívat nakupování na internetu či internetové bankovnictví. Podobné výsledky ukazuje i studie realizována už v roce 2013 (Roberts, Indermaur & Spiranovic, 2013).

Na rozdíl od výzkumu J. Brandse a J. van Wilsena, výsledky N. Akdemira (2020) ukazují, že lidé s vyšším vzděláním vypovídali o vyšší úrovni strachu z toho, že se stanou obětí kyberkriminality. Zároveň respondenti s vyšším finančním příjmem uváděli vyšší strach z kyberkriminality. Ukázalo se, že sociální status předpovídal vyhýbavé chování na internetu, tzn. že lidé s vyšším vzděláním a vyšším finančním příjmem mají vyšší pravděpodobnost se vyhýbat rizikovým, ohrožujícím či podezřelým situacím, ve kterých by mohlo hrozit, že se stanou obětí kyberkriminality. Další poznatky se týkaly užívání bezpečných hesel. Ukázalo se, že úroveň vzdělání má pozitivní vliv na využívání strategií pro bezpečnější hesla. Je tedy vyšší pravděpodobnost, že lidé s vyšším vzděláním využívají bezpečnější a hůře prolomitelná hesla než lidé s nižší úrovní vzdělání (Akdemir, 2020).

Lidé s vyšším vzděláním a vyšším ročním příjmem v tomto výzkumu reportovali vyšší strach z kriminality či ukradení identity na internetu. Celkově se jako prediktor protektivního a bezpečnostního chování jevil socioekonomický status. U respondentů, kteří uváděli vyšší stupeň vzdělání a vyšší roční příjem je dle výsledků analýzy vyšší pravděpodobnost využívání strategií zabezpečení svých údajů na internetu. Například lidé s vyšším vzdělání mají 3,6krát vyšší pravděpodobnost toho, že vymažou podezřelé e-maily a nebudou na ně reagovat a 3,1krát vyšší pravděpodobnost, že budou stahovat známé soubory z ověřených stránek oproti respondentům, kteří měli nižší vzdělání a nižší kvalifikace (Akdemir, 2020).

Při výzkumu, který sledoval bezpečnostní nastavení na sociálních sítích se ukázalo, že technické znalosti o nastavení soukromí pozitivně korelovaly s tím, zda si uživatelé skutečně upravovali nastavení soukromí na svých profilech. To ukazuje, že technické dovednosti a znalosti mohou být protektivním faktorem na internetu (Boyd & Hargittai, 2010). Gramotnost a s tím spojená důvěra ve vlastní schopnosti spravovat své soukromí mohou ovlivnit to, jak a do jaké míry se uživatelé internetu podílejí na svém bezpečnostním nastavení a na zveřejňování informací o svém životě (Kezer, Sevi, Cemalcilar & Baruh, 2016).

Dalším možným faktorem, který ovlivňuje chování na internetu je gender. V rámci výzkumů komunikace se již ve starších výzkumech ukazuje, že ženy jsou obecně v komunikaci více sdílné a prozrazují o sobě více osobních informací. Míra sdělování informací se samozřejmě odvíjí od kontextu, od toho, jak moc znají danou osobu, které se svěřují. Zároveň mohou více sdílet své pocity (Parker & Parrott, 1995; Dindia & Allen, 1992). V kontextu digitálních technologií se ukazuje, že existují rozdíly ve sdělování osobních informací, konkrétně v případě sociálních sítí.

Ženy více sdílejí osobní informace týkající se jejich oblíbených knih, hudby a jejich náboženství, na druhou stranu méně sdílejí například své osobní telefonní číslo (Tufekci, 2008). Zároveň se ukazuje, že ženy mají častěji, než muži na sociálních sítích nastaven svůj profil jako soukromý. To znamená, že přístup k informacím na jejich profilu mají pouze jejich přátelé, které musí odsouhlasit (Lewis, Kaufman & Christakis, 2008). S tím souvisí také to, že bývají opatrnější než muži v tom, komu na sociální síti povolí přátelství, tzn. koho si přidají do seznamu přátel a umožní tak nahlédnout na jejich profil a získat tak přístup k jejich osobním informacím, které zde zveřejnily (Fogel & Nehmad, 2009). Na druhou stranu, A. Barak a O. Gluck-Ofri (2007) neprokázali ve svém výzkumu žádný signifikantní rozdíl mezi gendery v oblasti sdělování osobních informací na diskuzních fórech.

Novější výzkum T. McGillové a N. Thompsona (2018) naznačuje, že ženy vykazují signifikantně méně bezpečnostního chování a neaplikují tolik bezpečnostních pravidel pro svůj pohyb na internetu jako muži. Dále uvádějí, že individuální percepce bezpečnosti a chování na internetu je variabilní v souvislosti s genderem (McGill & Thompson, 2018). Výzkum M. Gratianové a kolegů (2017) ukazuje, že mezi zabezpečením jsou určité genderové rozdíly. Gender v rámci jejich výzkumu nebyl signifikantní faktor pouze v oblasti zabezpečení vlastní zařízení. Zároveň ale ve třech dalších dimenzích bezpečnosti, kterými jsou generace hesel, povědomí o rizicích a aktualizování systému, byl gender signifikantní. U žen se ukazuje, že nemají tak silná hesla jako muži, nemají tak dobré povědomí o možných rizicích, která na internetu hrozí a zároveň aktualizovaly svá zařízení signifikantně méně než muži (Gratian, Bandi, Cukier, Dykstra & Ginther, 2017).

To ukazuje, že je stále otevřená diskuse mezi tím, zda a jak může gender ovlivňovat chování a bezpečnost na internetu. Některé analýzy ukazují, že statisticky významnými prediktory strachu z internetové kriminality je věk, gender, úroveň vzdělání a příjem uživatelů (Akdemir, 2020), na druhou stranu někteří autoři (např. Roberts, Indermaur & Spiranovic, 2013) uvádějí, že tyto předpokládané prediktory nemají statisticky významný vliv.

Dalšími možnými faktory, které ovlivňují chování na internetu jsou osobnostní faktory. V souvislosti s osobnostními rysy bylo realizováno velké množství studií, sledujících právě vztah mezi rysy osobnosti a zabezpečením na internetu. Na příkladu phishingu se ukázalo, že ženy s vysokým skóre v oblasti neuroticismu mohou mít vyšší pravděpodobnost stát se obětí phishingu. Dále se ukázala korelace mezi otevřeností novým zkušenostem a slabým nastavením vlastního soukromí a bezpečí na internetu (Halevi, Lewis & Memon, 2013). Vysoká extraverze byla například v korelaci se sníženou percepcí možného nebezpečí a rizik při online nakupování (Riquelme & Roman, 2014).

M. Gratianová a kolegové (2017) realizovali výzkum, ve kterém sledovali osobnostní rysy a čtyři faktory, související se zabezpečením na internetu: zabezpečení vlastního zařízení, generace silného hesla, povědomí o rizicích a aktualizace zařízení. Tyto čtyři faktory bezpečnosti na internetu využili autoři po vzoru výzkumu S. Engelmana a E. Peera (2015). Tyto faktory by bylo možné, dle již zmíněných poznatků, zařadit do strategií zajištění technické bezpečnosti na internetu. V oblasti zabezpečení vlastního zařízení se ukazovala jako prediktor například míra extraverze uživatelů. Při generaci hesla, povědomí o rizicích a pro aktualizování

systému se ukázala signifikantní svědomitost (Gratian, Bandi, Cukier, Dykstra & Ginther, 2017).

Styly rozhodování jsou dalším možným faktorem, který ovlivňuje chování na internetu. Styl rozhodování popisuje opakující se vzorce reakcí, které jedinec využívá v rozhodovacím procesu. Styly rozhodování je možné rozdělit do pěti kategorií: racionální, vyhýbavé, závislé, intuitivní a spontánní rozhodování. Při racionálním rozhodování jedinec využívá logické myšlení. Vyhýbavé rozhodování zahrnuje zpoždění či odložení samotného rozhodnutí, závislé rozhodování se odkazuje na pomoc druhých osob. Intuitivní rozhodování je ovlivněno především intuicí a instinkty. Spontánní rozhodování je popisováno jako rychlé rozhodování nezahrnující dlouhé přemýšlení nad následky (Scott & Bruce, 1995). S účinným zabezpečením na internetu negativně koreluje závislé a impulzivní rozhodování (Engelman & Peer, 2015). S výše zmíněnými čtyřmi faktory ochrany na internetu souvisely styly rozhodování následovně: Se zabezpečením vlastního zařízení souvisí racionální rozhodování, s generací silného hesla zase vyhýbavý styl rozhodování, s povědomím o rizicích pozitivně koreluje racionální styl rozhodování a naopak negativně spontánní styl rozhodování, na závěr s aktualizací systému koreluje racionální rozhodování, zatímco spontánní rozhodování koreluje s aktualizacemi negativně (Gratian, Bandi, Cukier, Dykstra & Ginther, 2017). Na rozdíl od výzkumu S. Engelmana a E. Peera (2015) M. Gratianová a kolegové (2017) nenašli korelaci mezi vyhýbavým stylem rozhodování a zabezpečení vlastního zařízení.

Ochota podstupovat rizika (angl. *risk-taking preferences*) popisuje postoj k rizikům a rozhodování při rizikových situacích. Ochotu podstupovat rizika lze rozdělit na pět dimenzí, které jsou sledovány v souvislosti s rizikovým chováním. Je to tedy ochota podstoupit riziko: etické, finanční, ochrany a zdraví, rekreační a sociální (Gratian, Bandi, Cukier, Dykstra & Ginther, 2017). Ochota riskovat je významným faktorem při bezpečnostním chování. Například ochota podstupovat zdravotní / bezpečnostní rizika negativně koreluje s povědomím o rizicích či aktualizací systému (Engelman & Peer, 2015). Ve výzkumu M. Gratianové a kolegů (2017) v souvislosti se zabezpečením vlastního zařízení nekoreloval žádná z uvedených dimenzí ochoty podstupovat rizika. S vytvářením bezpečného hesla a aktualizací systému pozitivně korelovala dimenze ochoty podstupovat zdravotní a bezpečnostní rizika, u povědomí o rizicích se ukázala korelace s ochotou podstupovat etická rizika.

V rámci různých výzkumů bylo dále zjištěno, že na chování na internetu může mít také vliv styl attachementu (vazby či připoutání). V přehledové studii M. Daneta a R. Miljkovithce

(2017) bylo zjištěno, že většina využitých výzkumů potvrzuje, že typ attachementu má určitý vliv na motivaci a způsob užívání internetu. Lidé s jistým attachementem, kteří mají dobré predispozice k navazování sociálních interakcí, využívají sociální sítě jako "prodloužení" svého každodenního života a aplikují své schopnosti z offline do online světa. Lidé s nejistým attachementem mohou virtuální komunikaci využívat jako nástroj kompenzace možných nedostatků a nejistoty při navazování interakcí s dalšími lidmi.

Lidé s nejistým attachementem mají vytvořeny negativní modely či postoje k sobě nebo druhým, což jim může ztížit navazování kontaktu s jinými. Některé výzkumy naznačují, že tito jedinci využívají virtuální komunikaci k získání další podpory. Zároveň se ukazuje, že se liší užívání internetu u různých podtypů nejistého attachementu. Například lidé s vyhýbavým attachementem jsou s interakcí na internetu spokojenější než lidé s jistým attachementem. Na internetu se také lidé s vyhýbavým attachementem mohou zdát méně "vyhýbavými" a odhalují o sobě více osobních informací než v offline konverzaci, internet tak může snižovat jejich obranný přístup ve vztazích.

U lidí s úzkostným attachementem poskytuje internet bezpečný prostor pro navazování vztahů, zároveň tento způsob komunikace využívají častěji, než komunikaci tváří v tvář, zvlášť pokud prožívají negativní emoce (Danet & Miljkovitch, 2017).

Z výše zmíněných výzkumů je možné usuzovat, že bezpečnost a chování na internetu je velmi komplexní fenomén, který může být ovlivněn mnoha proměnnými. Mezi tyto proměnné patří demografické údaje jako je věk, vzdělání či gender, dále může být ovlivněn osobnostními charakteristikami a rysy, vytvořenou vazbou (attachementem), styly rozhodování nebo ochotou podstupovat rizika. Zároveň je bezpečnost na internetu ovlivněna osobními zkušenostmi nebo sociálními normami. Výše zmíněné poznatky tedy představují spíše přehled možných vybraných proměnných, které jsou pro tuto práci i vzhledem k zaměření empirické části zásadní a důležité, ale neznamená to, že jsou to jediné faktory, které na bezpečnost na internetu působí.

4. Protekčně motivační teorie

Zásadním krokem pro zlepšení bezpečnosti na internetu je přijetí osobní zodpovědnosti každým jedincem, který se na internetu pohybuje. V této souvislosti je sledováno, jak směřovat zprávy a intervence, které by mohly motivovat uživatele internetu k lepšímu zabezpečení. Pro vývoj těchto zpráv a intervencí je nezbytné zkoumání teoretických procesů, které ovlivňují to, jak lidé na různé zprávy reagují. V některých výzkumech se tedy zkoumá tzv. *Teorie motivace ochrany* (angl. The protection motivation theory - PMT).

Původně se tato teorie využívala především v oblasti ochrany a péče o zdraví, ale je možné najít určité analogie i v oblasti internetové bezpečnosti. PMT pracuje se třemi klíčovými komponenty, které se objevují při potenciálním ohrožení:

- vnímaná míra škodlivosti nadcházející událost
- vnímaná pravděpodobnost výskytu ohrožující události
- vnímaná účinnost ochranné reakce

Na základě komunikace těchto tří komponent se nastartuje kognitivní reakce a jedinec zaujímá určitý postoj k ohrožující události (Rogers, 1975). Zároveň tato teorie předpokládá, že lidé provádějí dva typy kognitivního zhodnocení situace. V prvním případě je možné situaci vyhodnotit jako ohrožení, v druhém případě je situace brána jedincem jako zvládnutelná jeho copingovými strategiemi. Zároveň se v reakci na situaci mohou objevit dva typy chování: adaptivní nebo maladaptivní. Adaptivní reakce se považuje za účinnou při ochraně před hrozbou. Maladaptivní reakce může vyústit v to, že dané situaci tato reakce nijak nepomůže nebo potenciálně zvyšuje riziko ohrožující situace (Rogers, 1975).

Při posuzování rizikové či ohrožující události lidé hodnotí svou vlastní zranitelnost v dané situaci, závažnost ohrožení, pravděpodobnost výskytu této události, následky ohrožení a své vlastní self- efficacy pro zvládnutí této situace. Záměr zachovat se tak, abychom se ochránili a posouzení efektivity dalšího chování je zároveň ovlivněno odměnami, které jsou s tímto chováním spojené a zároveň posouzení vnímaných nákladů, které je třeba vynaložit při reaktivním chování (Rogers, 1975; Shillair a kol., 2015).

Koncept této teorie je možné aplikovat i na ochranu na internetu a na uživatele, kteří se dostanou do ohrožující situace. Na příkladě otevírání příloh, které jsou přiloženy v e-mailech od

neznámých i známých osob je možné ukázat, jak tuto teorii můžeme aplikovat. Někteří uživatelé mají nainstalované antiviry a ochranu proti spamům a nikdy neotevírají přílohy v e-mailu od neznámých osob. Toto chování je možné označit za adaptivní odpověď. Na druhé straně existují jedinci, kteří otevírají jakoukoliv přílohu v e-mailové poště, nemají nainstalovaný antivir ani ochranu proti spamům, a ještě používají slabá a snadno prolomitelné hesla. Toto chování je naopak maladaptivní. Před otevřením takové přílohy ale lidé zvažují, jakou hrozbu by mohlo samotné otevření přílohy představovat, pravděpodobnost, s jakou je ve zprávě obsažen například vir a jak vážné mohou být následky otevření podezřelé přílohy. Záleží také na tom, jaké má uživatel znalosti a schopnosti rozpoznat bezpečný, a naopak potenciálně nebezpečný e-mail. Zároveň jedinec posuzuje své copingové mechanismy a strategie, jak by se s ohrožením či s následky ohrožení vypořádal a zda je schopný si ochránit svůj počítač či data (Anderson & Agarwal, 2010; Shillair a kol., 2015).

Zároveň vysoké self-efficacy a copingové strategie mohou být pozitivními faktory při zvažování nákladů a zisků, které protektivní chování přináší. Pokud má jedinec vysoce vnímanou vlastní sebe účinnost (self-efficacy) a má vytvořené copingové mechanismy pro zvládnutí ohrožující situace na internetu, bude pro něj vklad do adaptivního chování méně náročný jak časově, tak psychicky. R. Shillairová a kol. (2015) usuzují, že tedy trénink a intervence, které by podporovaly u uživatelů vlastní vnímanou sebeúčinnost by mohly podpořit adaptivní reakce v ochraně na internetu.

4.1. Protekčně motivační teorie a ochrana na internetu

Při aplikaci PMT na rozhodování ohledně ochrany na internetu můžeme pracovat s následujícími faktory:

1. **Vnímání pravděpodobnosti vzniku potenciální hrozby:** Jak lidé vnímají potenciální rizika spojená s užíváním internetu? Jaká je vnímaná pravděpodobnost kybernetického útoku nebo úniku osobních údajů?
2. **Vnímaná závažnost hrozby a strach spojený s hrozbou:** Jak vážně lidé vnímají potenciální důsledky těchto hrozeb, jako je například finanční ztráta nebo narušení jejich osobní integrity či reputace?
3. **Vnímaná zranitelnost:** Jak zranitelní se lidé cítí vůči těmto hrozbám, což může ovlivňovat jejich ochotu přijmout opatření k vlastní ochraně?
4. **Vnímané self-efficacy:** Jak účinně si lidé věří, že ochranná opatření budou při zmírňování hrozeb efektivní, což může ovlivnit jejich motivaci k těmto opatřením.

5. **Náklady spojené s ochrannými opatřeními:** Jaké náklady (čas, peníze, usilí, …) jsou spojeny s přijetím ochranných opatření a jak tyto náklady ovlivňují rozhodnutí je zavést?

V oblasti počítačové a internetové ochrany byl realizován výzkum zkoumající souvislost mezi PMT a používáním antivirového programu. Ukázalo se, že vnímaná zranitelnost, odpověď v chování a copingové self-efficacy predikuje intence k ochraně proti virům. Na druhé straně možné následky a náklady spojené s užíváním antiviru ve výzkumu nevycházejí jako signifikantní prediktory chování. Objevily ale další dva možné prediktory, a to vnímaný zisk, získaný z adaptivní reakce a předchozí zkušenosti s viry (Lee, LaRose & Rifon, 2008). Zároveň se ukazuje, že předchozí znalosti mohou být faktory, predikující zvýšenou ochranu na internetu (Venkatesh, Thong & Xin, 2012). Další zjištění implikují, že významnými prediktory ochrany na internetu jsou v souvislosti s PMT účinnost odezvy a vnímaná sebeúčinnost. Tyto dva prediktory byly významně spojeny se zvyky, které mají jedinci vytvořené v souvislosti s ochranou na internetu (Vance, Siponen & Pahnila, 2012).

Velké množství výzkumů týkající se bezpečnosti na internetu a obecně vnímaní rizik vznikaly během pandemie COVID-19. Tato celosvětová pandemie podněcovala výzkumníky i laickou veřejnost k zájmu o informační technologie. Výzkumy například zkoumají, jak vnímání rizika a potenciální hrozba, zejména během událostí, jako byla pandemie COVID-19, ovlivňuje pocit bezpečí. Studie zjistily, že emocionální a informační vnímání významně ovlivňuje pocit bezpečí lidí, což ukazuje, že vnímaná rizika mohou vést ke zvýšené úzkosti a strachu, a tím ovlivnit to, jak bezpečně se jednotlivci cítí online i off-line (Shi, Qiqi & Guangzhu, 2023).

V roce 2022 byla realizována rozsáhla metaanalýza, která sledovala vztahy mezi konstrukty PMT a bezpečností na internetu. Autoři uvádějí, že i když je PMT jednou z nejvlivnějších teorií, která se využívá v oblasti bezpečnosti na internetu, výsledky studií jsou často nekonzistentní. V rámci metaanalýzy autoři sledovali také další kontextové konstrukty, které nejsou součástí PMT, jako je kolektivismus a individualismus a aplikace poznatků v kontextu pracoviště a osobního života. Z metaanalýzy 92 studií autoři zjistili, že největší průměrný vliv na chování vedoucí k ochraně na internetu má hodnocení zvládání efektivity reakce a vnímané self-efficacy. Teoretické konstrukty PMT byly silnější v osobním kontextu než v kontextu pracoviště, což znamená, že PMT konstrukty lépe predikují to, jak se uživatelé chrání na svém osobním zařízení nežli na pracovním. Zároveň se vnímaná zranitelnost ukazuje smíšené výsledky při predikování výsledného chování, které vede k ochraně na internetu. Žádnou podporu však nemá tvrzení, že náklady vynaložené na reakci mohou být prediktorem chování

uživatelů. Z toho vyplývá, že nejvýznamnější roli z konstruktů PMT má vnímaná efektivita reakce a sebeúčinnost (self-efficacy), dále může predikovat chování vnímaná zranitelnost, ale to, jaký čas, úsilí, finance apod. musí uživatelé vložit do vlastní ochrany na internetu nemá prokazatelný vliv (Mou, Cohen, Bhattacheriee & Kim, 2022).

Zároveň se ukazuje, že přesto, že PMT je často využívanou teorií pro zkoumání chování při zabezpečení na internet, jenom málo studií zkoumá vliv emocí na hodnocení potenciálních hrozeb, online bezpečnosti a reakcí na možné hrozby. Zároveň autoři uvádějí, že je důležité se zaměřovat ve výzkumech i na přidružené emoce, protože PMT naznačuje, že bližší zkoumání informačních hrozeb a emoce spojené s tímto posouzením by mohly ovlivnit samotný proces posuzování hrozeb a schopnosti uživatelů se bránit či se s hrozbami vyrovnat. Některé studie pracují například s mírou úzkosti nebo vzniklým vztekem, který nastává při potenciální hrozbě. Dále se studie zaměřují na potenciálním lítosti, kterou mohou uživatelé cítit po události, která je ohrozila, ale mohli ji ovlivnit svým chováním (Ogbanufe & Baham, 2023).

Například strach z potenciální hrozby může být velmi významným prediktorem určující další chování jedince. Vyvolání pocitu strachu je možné zařadit také do persvazivních technik pro změnu chování. Tyto zprávy mají za cíl "vystrašit" lidi tak, aby změnili své chování k vlastní ochraně (Sobol & Giroux, 2023). Strach je tedy důležitou součástí také toho, jak se lidé na internetu chovají. V rámci PMT se jedná a potenciální emocionální konstrukt, který souvisí vnímaná závažnost hrozby.

Strach z potenciálních hrozeb na internetu skutečně ovlivňuje chování lidí v online prostředí, což potvrzují i odborné studie. Tento strach může vést k různým reakcím, například k omezení online aktivit, zvýšené opatrnosti, a dokonce i k vyhýbání se určitým webovým stránkám nebo službám. Jedna ze studií ukazuje, že strach z kyberhrozeb, jako jsou krádeže dat nebo kyberšikana, může zvýšit opatrnost uživatelů a motivovat je k používání různých bezpečnostních opatření, jako je dvoufaktorová autentizace nebo VPN. Tento strach může také omezit ochotu uživatelů sdílet osobní informace online (Xu a kol., 2022).

Otázkou, jak specifické hrozby ovlivňují motivaci lidí ke změně chování, se zabývá další studie z roku 2023. Ve studii se ukazuje, že čím konkrétnější a osobně relevantní je hrozba, tím větší je pravděpodobnost, že lidé přijmou preventivní opatření, aby se těmto hrozbám vyhnuli (Sobol & Giroux, 2023). Tento strach z online hrozeb může tedy vést k větší opatrnosti a změnám v chování. Celkově lze říci, že strach z potenciálních nebezpečí na internetu může mít významný

vliv na způsob, jakým lidé internet používají, jaké informace sdílejí a jakým způsobem se chovají v digitálním prostředí.

Většina výzkumů, která pracuje s PMT v souvislosti s bezpečností na internetu ukazuje, že zásadními prediktory chování je vnímaná pravděpodobnost vzniku hrozby a vnímané self-efficacy, neboli schopnost si s hrozbou poradit. Vnímání hrozby startuje motivaci k ochraně; pokud jedinec vnímá potenciální hrozbu jako pravděpodobnou, motivuje ho to k zahájení ochranných kroků, aby hrozbě zamezil (Ogbanufe & Baham, 2023). Lidé mají tendenci upravovat své chování na základě toho, jak pravděpodobné považují riziko, kterému mohou čelit. Ukazuje se, že čím významněji respondenti výzkumu vnímají, že hrozba na internetu je reálná a pravděpodobná (např. že mohou být obětí útoku hackera, mohou utrpět nějakou ztrátu nebo krádeže identity), tím větší je pravděpodobnost, že změní své chování, aby se této hrozbě vyhnuli. Tato změna může zahrnovat používání silnějších hesel, pravidelné aktualizace softwaru, vyhýbání se podezřelým stránkám nebo omezení sdílení osobních informací (Xu a kol., 2022).

Dále výzkumy ukazují, že když uživatelé vnímají hrozbu jako velmi pravděpodobnou, mohou následně omezit své aktivity na internetu, především ty, které považují za nejrizikovější. Mezi tyto aktivity mohou být zařazeny nákupy na neprověřených e-shopech nebo používání sociálních sítí. Na druhou stranu, pokud lidé považují hrozbu za nepravděpodobnou nebo vzdálenou, jejich chování se pravděpodobně nezmění nebo se změní jen minimálně (Sobol & Giroux, 2023). Uživatelé internetu také berou v úvahu, jak efektivní jsou opatření, která mohou přijmout. Pokud jedinec věří, že preventivní opatření (např. antivirový software, silná hesla, omezení přístupu ke svému profilu) jsou účinná, může být ochotnější zapojit se do rizikových aktivit, i když vnímají hrozbu jako pravděpodobnou. Naopak, pokud nevěří v efektivitu těchto opatření, mohou se rizikovému chování vyhýbat úplně (Sobol & Giroux, 2023).

Celkově se ale ukazuje, že vnímaná pravděpodobnost hrozby na internetu je jedním z klíčových faktorů, který může ovlivňovat chování na internetu. Uživatelé, kteří vnímají riziko jako vysoké, jsou opatrnější a častěji přijímají preventivní opatření, zatímco ti, kteří riziko vnímají jako nízké, mohou být méně obezřetní.

Na základě PMT by bylo možné nadále koncipovat vzdělávací a intervenční programy pro zlepšení zabezpečení na internetu. Je možné vycházet z výsledků studií a mířit intervenční a výukové programy tak, aby lidé získávali zkušenosti a pocit vlastní sebeúčinnosti při ochraně

na internetu, jelikož vnímaná sebeúčinnost se ukazuje jako protektivní faktor. Zároveň by tyto programy mohly podpořit vlastní znalosti týkající se digitálních technologií, zabezpečení a především znalost postupů a možností, jak ohrožující situaci řešit a jaké postupy jsou nejefektivnější pro vlastní ochranu. Dále by se mělo zapracovat na postupném nahrazení maladaptivních odpovědí adaptivními odpovědi. Důležitá je osobní zodpovědnost a aplikace kroků a postupů, které mohou každého jedince ochránit před co nejvíce potenciálními hrozbami.

Empirická část

Empirická část rigorózní práce navazuje na realizovaný výzkum v diplomové práci autorky, který se zaměřoval na vnímání bezpečnosti na internetu u dospělých ve věku 35-60 let s dokončeným maximálně základním vzděláním.

Na základě výsledků diplomové práce bylo realizováno dotazníkové šetření s reprezentativním souborem respondentů (n = 700) ve věku mezi 35-60 lety. Výzkum probíhal za podpory programu Specifického vysokoškolského výzkumu „Adaptace aktérů a institucí na vývoj současné společnosti“ (SVV-Adakin) 2022. Pro dotazníkové šetření bylo upuštěno od původního kritéria pro výběr týkající se výše maximálního stupně vzdělání. To znamená, že v současném výzkumu jsou zahrnuti respondenti všech skupin dosaženého stupně vzdělání, aby bylo možné výsledky aplikovat na populaci střední dospělosti.

5. Výchozí kvalitativní výzkum

Výzkum v rigorózní práci navazuje na kvalitativní výzkum, který byl proveden v rámci diplomové práce autorky. Při výzkumu byly použity polostrukturované rozhovory a prezentace obrazových materiálů pro prohloubení diskuse s respondenty. Sběr dat probíhal během pandemie COVID-19, takže všechny rozhovory byly realizovány online. Rozhovory byly nahrávány na diktafon, následně přepsány a kódovány pomocí zakotvené teorie v programu MAXQDA 2021.

Výzkum pro diplomovou práci probíhal ve větším výzkumu, který sledoval znalosti uživatelů internetu se základním vzdělání ve všech věkových kategoriích. Pro diplomovou práci byly vybrány rozhovory s respondenty, kteří splňovali podmínku věku (35-60 let). Celkem bylo zrealizováno 16 hloubkových rozhovorů s respondenty ve věku 35-60 let, kteří měli dokončené maximálně základní vzdělání. Každý rozhovor trval cca 90 minut. Rozhovory probíhaly na platformách ZOOM nebo Skype, dle preference respondenta. Z rozhovorů nebyl pořizován obrazový, pouze zvukový záznam.

Cílem výzkumu bylo zmapovat vnímání online bezpečnosti a strategie online bezpečnosti u dospělých ve věku 35-60 let s maximálně základním vzděláním. Pro výběr do výzkumného souboru museli respondenti splňovat tři kritéria: věk mezi 35-60 lety, dokončené maximálně základní vzdělání a alespoň základní dovednosti práce na internetu.

Výzkumný soubor tvořilo 16 respondentů, osm žen a osm mužů. Průměrný věk respondentů byl 48,7 let (M = 48,7; SD = 7,47).

Výzkumné otázky byly zvoleny následující:

1. Jak respondenti vnímají bezpečnost na internetu?
2. Jaké strategie ochrany online respondenti používají?
3. Jak respondenti dospěli k těmto individuálním strategiím ochrany na internetu?

Rozhovor se skládal ze šesti otázek, osmi podotázek a obrazových materiálů. Jako obrazové materiály byly využity tři fotografie z filmu *Jak vytrhnout velrybě stoličku* a respondenti byli u jednotlivých fotografií dotazování, zda by podobnou fotografii sdíleli či nesdíleli na internetu. Následně byla respondentům prezentována účelně vytvořená konverzace mezi dvěma neznámými lidmi, nad kterou byla s respondenty vedena diskuse. Posledním prezentovaným podnětem k diskusi byl příklad e-mailového phishingu, nad kterým byla vedena debata. Obrazový materiál podpořil plynulost rozhovoru a bylo docíleno hlubší debaty nad jednotlivými tématy.

K analýze výsledků byla využita metoda zakotvené teorie. K. Charmazová (2014) pojímá zakotvenou teorii jako metodu, která nabízí systematické, ale přitom flexibilní postupy pro analýzu kvalitativních dat a následné vynoření teorie z dat. Zakotvená teorie je tedy metoda, která napomáhá nahlédnout do struktury získaných dat a hledat tak teorie, které se vynořují v samotných datech. Analýza dat pomocí zakotvené teorie zahrnuje neustálé porovnávání dat, takže se jedná o interaktivní metodu, která nás neustále udržuje v kontaktu s daty a s vytvořenými kódy. Dle výsledků výzkumu lze vnímání online bezpečnosti v rámci vybrané skupiny považovat za komplexní jev, který lze rozdělit minimálně do tří složek:

1. **Sociální (osobní) bezpečnost na internetu**:

Sociální (osobní) bezpečnost zahrnovala především rizika spojená s narušením či poškozením vlastní osobní integrita či identita uživatele, jeho soukromí a osobní pohody. Může zde být zahrnuto například riziko zneužití údajů k zesměšňování, vydírání nebo kyberšikaně, vystavení nepříjemným, urážlivým nebo krutým komentářům.

- ID0037 (Žena, 46 let): *"A oni tam začnou bejt hnusný, začnou mi škaredě nadávat, že se mám vrátit zpátky do školy a kdesi cosi. Já si je bloknu, odstraním komentáře a vypnu je, protože mě to obtěžuje a uráží mě to... pak mám zkaženej celej den, tak to radši vypnu a neřeším to. Chtějí jenom ubližovat lidem, aby se oni zviditelnili a byli zajímavý a toho druhýho aby potopili."*

- *ID0029 (Muž, 53 let): Stala se mi taková nepříjemná zkušenost. Každý chlap si píše s holkama, to je normální. Měl jsem uložených pár holek a každá vlastně viděla, koho mám v přátelích. Jedna měla takovou odvahu, spíš teda drzost, že si začala s těma mejma kontaktama psát, zjišťovat o mně informace a ptát se, jestli s nima nechodím a takový, to je jako by mi četla dopisy. A když se tohle stalo, tak mi kamarád poradil a přímo naučil, jak to mám dělat, že člověk pak uvidí jenom to, co já mu povolím. To je vlastně moje zkušenost, že mě mezi sebou ty holky pomlouvaly, a to je příčina, proč jsem si musel ty sociální sítě trochu zabezpečit.*

2. Technická bezpečnost na internetu

V rámci technické bezpečnosti na internetu se respondenti nejčastěji obávají materiální ztráty či poškození. Jsou zde zahrnuty například virové útoky, ztráta osobních údajů, hackerské útoky, ztráta peněz při používání internetového bankovnictví a online plateb, spam, podvodné e-maily, phishing atd.

- ID0025 (žena, 45 let): *"Tak mám obavy třeba z nějakých virů, který se mi tam můžou dostat a můžu přijít o data a o fotky, taky třeba z nějakýho až jako hackerskýho útoky jako... vybrakování bankovního účtu a něco takovýho."*

- *ID0030 (Muž, 44 let): "No obávám se třeba, že když dělám bankovnictví, tak má člověk strach, aby nepřišel o prachy. Nebo abych se nesplet, když někam posílám prachy. Tak toho se obávám, protože ty e-shopy a všechno, člověk, jak už je starší, tak nemá tu jistotu, o tom to je."*

3. Institucionální bezpečnost na internetu

Hlavním znakem této kategorie jsou obavy ze zásahu do soukromí vyššími institucemi, prodej dat třetím stranám, sledování aktivity na internetu, zavedení cenzury a omezení svobody slova na internetu, dále například ztráta anonymity vlivem vyšších institucí. Institucionální složka bezpečnosti na internetu nebyla při hloubkových rozhovorech (na rozdíl od sociální či technické složky) zmiňována všemi respondenty. Když ale byla v rozhovoru zmíněna, tak tvořila hlavní část celého rozhovoru a v kontextu výzkumu se ukazovala jako důležitá pro další práce.

- ID0027 (Muž, 49 let): *"Teď jsem zmoudřel, ale zamlada jsem žil divokým životem. Když budu chtít vidět kamarády, kteří tímhle životem stále žijí, tak abych se ubránil tomu, že mi někdo bude prošťourávat telefon, protože jsme permanentně hlídaní, tak jim nenapíšu, že přijedu. Jednoduše tam dojedu, telefon nechám v autě, podívám se, kde ten asi bydlí nebo mu dám jinak najevo, že tam jsem. Snažím se neřešit některý věci přes telefon." ... "Pořád nás sleduje "velký bratr", to vím z vlastní zkušenosti, podvodníčkům a malým hackerům se ubráníte, ale bezpečnostním složkám a podobnejm se neubráníte, ty jsou tak 10-20 let napřed."*

- ID0032 (Muž, 37 let): *"To je facebook, sociální sítě, twitter, instagram. Zde lidi řeknou věci, za které můžou pykat v rámci trestního řízení nebo přestupku. Sociální sítě jsou obrovský problém, tam si lidé už zas musej dávat pozor na to, co řeknou. Lidi nejsou opatrný tam, kde hrozí ztráta práv a svobod, ale to je pro mě důležitý." ... "Není to pravidlo, ale je to trend, kterej jde z vyšší společnosti. Tam mají určitou moc, snaží se to zprivatizovat bez konzultace s veřejností. Mám obavy, že internet přestane být anonymní."*

Dále byl předchozí výzkum zaměřen na využívané strategie ochrany na internetu. Na základě odpovědí respondentů byl zjištěn rozdílný přístup k aplikaci ochranných strategií na různé složky bezpečnosti. To odráží také jaké mají respondenti vlastní zkušenosti, dovednosti a postoj k jednotlivým složkám bezpečnosti na internetu. Pokud jde o technickou a institucionální bezpečnost, existují soubory pravidel a strategií, které mohou všichni uživatelé uplatňovat stejným způsobem a je možné je najít v obecných „tutoriálech" či radách, jak se chránit na internetu (bezpečné heslo, dvojitá ochrana, nepřipojování se k nezabezpečeným sítím, neotevírání e-mailů od neznámého odesílatele apod.) Na druhé straně strategie pro ochranu v rámci sociální bezpečnosti odrážejí vlastní i zprostředkované zkušenosti a dovednosti jednotlivých uživatelů. V této oblasti se liší nastavené hranice jednotlivých respondentů toho, co vnímají jako potenciálně nebezpečné či ohrožující.

V rámci zjišťování ochranných strategií na internetu byly zmiňované aspekty jako je například vlastní zkušenost s hrozbami na internetu, vnímané self-efficacy a vnímání pravděpodobnosti výskytu hrozby. Z těchto důvodů jsou v tomto výzkumu zahrnuty také prvky protekčně motivační teorie.

Vzhledem k zjištěním byl výzkum pro rigorózní práci koncipován tak, aby byly v dotazníku zahrnuty všechny zjištěné dimenze bezpečnosti na internetu. Pro další výzkum považuje autorka za nezbytné reflektovat možnost, že respondenti mohou odpovídat mírně odlišně v závislosti na tom, kterou dimenzi považují v danou chvíli za nejdůležitější. Je tedy důležité vědět, co si respondenti pod spojením „bezpečnost na internetu“ představují a co pro ně tento fenomén znamená. Otázky pro dotazníkové šetření jsou kategorizovány podle tří dimenzí bezpečnosti na internetu. Tyto dimenze považuje autorka za důležité i během výzkumných rozhovorů, při plánování vzdělávacích kurzů nebo při pomoci lidem překonat strach z pohybu na internetu a zvládání stresu spojeného s digitálními technologiemi.

6. Cíle výzkumu

Cílem výzkumu je blíže prozkoumat vnímání bezpečnosti na internetu u dospělých mezi 35-60 lety. Ve výzkumu je pracováno s členěním bezpečnosti na internetu na tři základní zkoumané složky, a to složku sociální, technickou a institucionální. Zároveň jsou ve výzkumu využity prvky protekčně motivační teorie, konkrétně vnímaný strach spojený s potenciální hrozbou na internetu, vnímaná pravděpodobnost výskytu hrozby na internetu a vnímané self-efficacy respondentů v oblasti ochrany na internetu.

Strach z vnímané hrozby byl vybrán pro bližší zkoumání především proto, že se jedná o emocionální složku vnímané závažnosti potenciální hrozby. Dle některých výzkumů je právě strach důležitou složkou při zkoumání ochranného chování. PMT využitá v této práci se zaměřuje především na to, jak lidé reagují na potenciální hrozby. Tato teorie také předpokládá, že jedinci jsou motivováni k vlastní ochraně, pokud vnímají nějakou hrozbu a věří, že jsou schopni podniknout kroky k vlastní ochraně. Proto byl zařazen strach jako emocionální faktor. Strach a obavy z potenciální hrozby byly blíže popsány v podkapitole *3.1. Obavy uživatelů internetu*. Předpokladem je, že pokud budou respondenti uvádět vyšší skóre v oblasti strachu potenciální hrozby, budou více motivováni k vlastní ochraně na internetu.

Vnímaná pravděpodobnost potenciální hrozby byla zařazena proto, že může působit jako prediktor pro ochranu na internetu. Základním předpokladem je, že pokud respondenti budou mít pocit, že je vysoká pravděpodobnost výskytu hrozby, budou se také více snažit této hrozbě zamezit. Pokud mají respondenti pocit, že „se to nemůže stát“ můžeme předpokládat, že se chránit nebudou.

Dále bylo vybráno právě self-efficacy, které určuje, zda mají uživatelé pocit, že jsou schopni efektivně se potenciálním hrozbám postavit a zamezit jim. Předpokladem je, že pokud mají pocit vysoké sebe účinnosti v zabránění potenciální hrozbě, budou motivováni k vlastní ochraně.

Tyto složky PMT byly blíže sledovány v souvislosti s vnímanou bezpečností na internetu a jednotlivými složkami tohoto fenoménu. **Cílem výzkumu tedy je zjistit vliv zvolených prvků protekčně motivační teorie na vnímání třech složek bezpečnosti na internetu u dospělých**

ve střední dospělosti (35-60 let). Dále je cílem prozkoumat souvislost genderu a vzdělání s vnímáním bezpečnosti na internetu u dospělých ve střední dospělosti (35-60 let).

6.1. Výzkumné otázky a hypotézy

Vzhledem k cílům výzkumu byly zvoleny následující otázky a hypotézy:

1. **Existuje závislost mezi sociální (osobní) bezpečností na internetu a strachem z vnímané hrozby?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:
   H_0: Mezi skóre sociální složky bezpečnosti a skóre strachu z vnímané hrozby není závislost.
   H_A: Mezi skóre sociální složky bezpečnosti a skóre strachu z vnímané hrozby je závislost.

2. **Existuje závislost mezi sociální (osobní) bezpečností a vnímanou pravděpodobností vzniku hrozby na internetu?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:
   H_0: Mezi skóre sociální složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby není závislost.
   H_A: Mezi skóre sociální složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby je závislost.
3. **Existuje závislost mezi sociální (osobní) bezpečností a vnímaném self-efficacy?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:
   H_0: Mezi skóre sociální složky bezpečnosti a skóre vnímaného self-efficacy není závislost.
   H_A: Mezi skóre osobní složky bezpečnosti a skóre vnímaného self-efficacy je závislost.
4. **Existuje závislost mezi technickou bezpečností na internetu a strachem z vnímané hrozby?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:
   H_0: Mezi skóre technické složky bezpečnosti a skóre strachu z vnímané hrozby není závislost.
   H_A: Mezi skóre technické složky bezpečnosti a skóre strachu z vnímané hrozby je závislost.
5. **Existuje závislost mezi technickou bezpečností a vnímanou pravděpodobností vzniku hrozby na internetu?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:
   H_0: Mezi skóre technické složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby není závislost.
   H_A: Mezi skóre technické složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby je závislost.
6. **Existuje závislost mezi technickou bezpečností a vnímaném self-efficacy?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

H_0: Mezi skóre technické složky bezpečnosti a skóre vnímaného self-efficacy není závislost.

H_A: Mezi skóre technické složky bezpečnosti a skóre vnímaného self-efficacy je závislost.

7. **Existuje závislost mezi institucionální bezpečností na internetu a strachem z vnímané hrozby?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

   H_0: Mezi skóre institucionální složky bezpečnosti a skóre strachu z vnímané hrozby není závislost.

   H_A: Mezi skóre institucionální složky bezpečnosti a skóre strachu z vnímané hrozby je závislost.

8. **Existuje závislost mezi institucionální bezpečností a vnímanou pravděpodobností vzniku hrozby na internetu?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

   H_0: Mezi skóre institucionální složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby není závislost.

   H_A: Mezi skóre institucionální složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby je závislost.

9. **Existuje závislost mezi institucionální bezpečností a vnímaném self-efficacy?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

   H_0: Mezi skóre institucionální složky bezpečnosti a skóre vnímaného self-efficacy není závislost.

   H_A: Mezi skóre institucionální složky bezpečnosti a skóre vnímaného self-efficacy je závislost.

10. **Existuje závislost mezi vnímanou závažností sociální (osobní) složky bezpečnosti na internetu a pohlavím?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

    H_0: Pořadí, které respondenti přisuzují osobní složce bezpečnosti, nezávisí na pohlaví.

    H_A: Pořadí, které respondenti přisuzují osobní složce bezpečnosti, závisí na pohlaví.

11. **Existuje závislost mezi vnímanou závažností technické složky bezpečnosti na internetu a pohlavím?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

    H_0: Pořadí, které respondenti přisuzují technické složce bezpečnosti, nezávisí na pohlaví.

    H_A: Pořadí, které respondenti přisuzují technické složce bezpečnosti, závisí na pohlaví.

12. **Existuje závislost mezi vnímanou závažností institucionální složky bezpečnosti na internetu a pohlavím?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

    H_0: Pořadí, které respondenti přisuzují technické složce bezpečnosti, nezávisí na pohlaví.

    H_A: Pořadí, které respondenti přisuzují technické složce bezpečnosti, závisí na pohlaví.

13. **Existuje závislost mezi vnímanou závažností jednotlivých složek bezpečnosti na internetu a vzděláním?** Pro tuto výzkumnou otázku byly zvoleny tyto hypotézy:

    H_0: Pořadí, které respondenti přisuzují jednotlivým složkám bezpečnosti, nezávisí na vzdělání.

    H_A: Pořadí, které respondenti přisuzují jednotlivým složkám bezpečnosti, závisí na vzdělání.

7. Metodika

7.1. Výzkumný soubor

Výzkumný soubor je tvořen 700 respondenty, celkem 362 muži a 338 ženami. Ve skupině mezi 35-44 lety je 278 respondentů, od 45-60 let celkem 422 respondentů. Průměrný věk respondentů je

M = 47, 3 (SD = 6,7). Jedná se o obecnou populaci mezi 35-60 lety. Respondenti byli dále dotazováni, kolik času tráví na internetu ve volném čase a v rámci zaměstnání. Průměrný čas trávený na internetu v rámci volného času je 2,1 hodiny (SD = 1,5; Min = 0; Max = 10) a v zaměstnání je průměrný čas na internetu 2,6 hodiny (SD = 3; Min = 0; Max = 14). Od respondentů byly dále zjišťovány informace ohledně vzdělání, rodinného statusu, pracovního zaměření a hodnocení jejich dovedností na internetu.

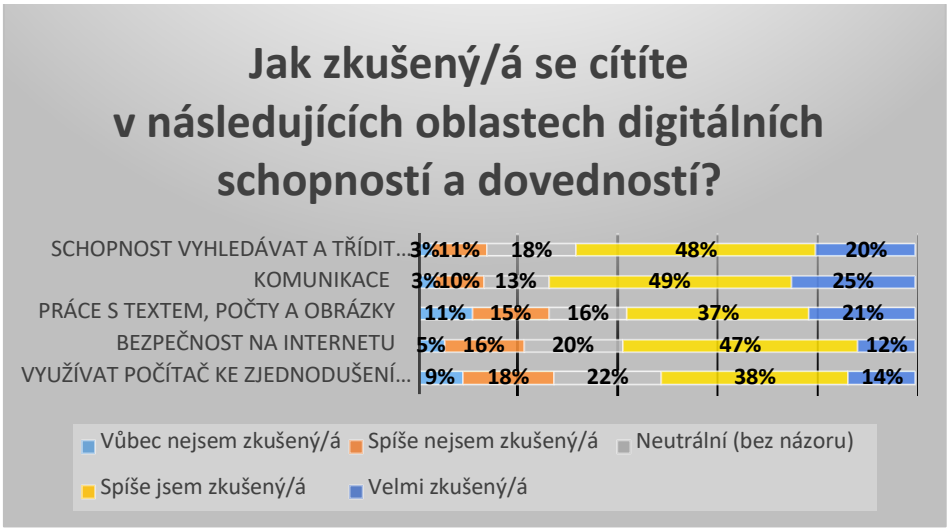
V následující tabulce jsou blíže popsány proměnné pohlaví, věková kategorie, vzdělání a rodinný status respondentů, včetně absolutních a relativních četností u jednotlivých kategorií.

Proměnná/varianta	Absolutní četnost	Relativní četnost
Pohlaví		
Muž	362	51,7 %
Žena	338	48,3 %
Věková kategorie		
35-44 let	278	39,7 %
45-54 let	289	41,3 %
55 let a více	133	19,0 %
Nejvyšší ukončené vzdělání?		
ZŠ nebo neukončené	16	2,3 %

Vyučen/a bez maturity	261	37,3 %
Středoškolské s maturitou	262	37,4 %
Vysokoškolské	161	23,0 %
Rodinný status		
Svobodný, svobodná	159	22,7 %
Ženatý, vdaná	404	57,7 %
Rozvedený, rozvedená	127	18,1 %
Vdovec, vdova	10	1,4 %

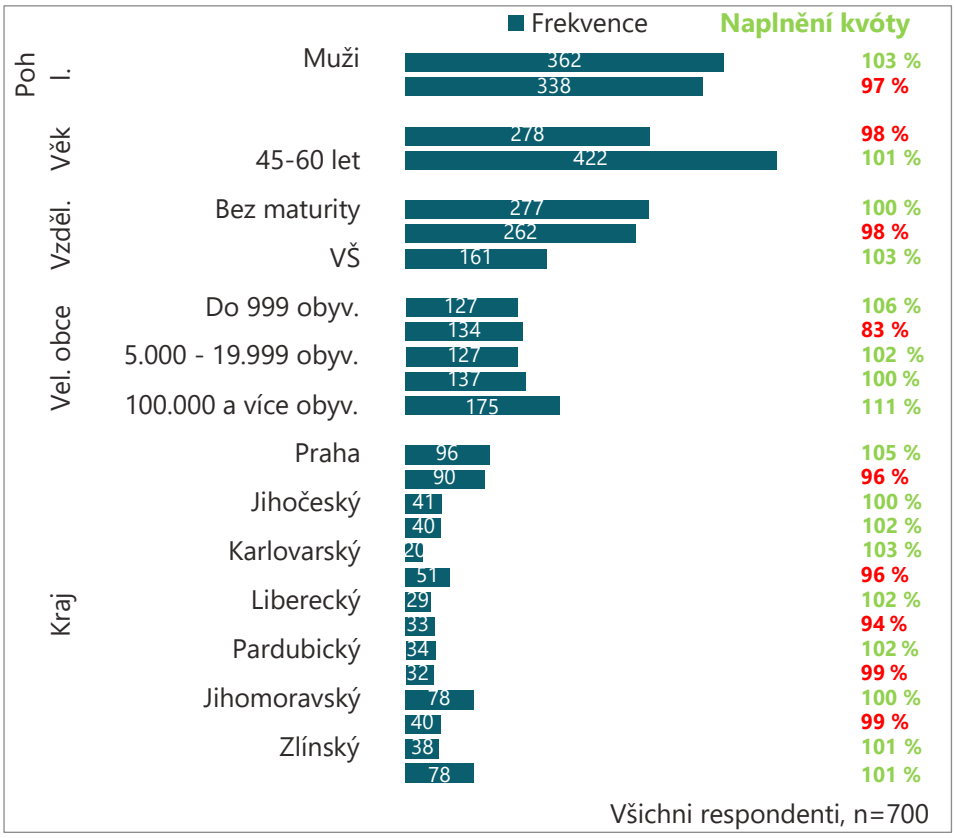
Tabulka 5. – Popis výzkumného souboru

Respondenti byli dále dotazováni na jejich sebehodnocení pěti základních dovedností na internetu dle EU (Vuorikari et al., 2022) mezi které jsou řazeny: schopnost vyhledávat a třídit informace, komunikace na internetu, práce s textem, počty a obrázky, bezpečnost na internetu a využívání počítače ke zjednodušení práce. Otázka zněla „Jak zkušený/á se cítíte v následujících oblastech digitálních schopností a dovedností?“ a hodnocení probíhalo na pětibodové Likertovo škále od Vůbec nejsem zkušený/á po Velmi zkušený/á. Respondenti se ve všech pěti oblastech nejčastěji hodnotí jako „Spíše jsem zkušený/á“. Výsledky jsou shrnuty v následujícím grafu:



Graf 1. – Sebehodnocení digitálních schopností a dovedností

Výběr výzkumného souboru je kvótní, reprezentativní dle demografických podmínek. V následujícím grafu jsou popsány další charakteristiky výzkumného souboru, včetně naplnění jednotlivých kvót:



Graf 2. – Výzkumný soubor – kvóty

7.2. Výzkumný dotazník

Pro účely tohoto výzkumu byl vytvořen vlastní dotazník s celkem 17 testovými otázkami s využitím pětibodové Likertovy škály. Dále bylo zařazeno sedm sociodemografických a identifikačních otázek. Otázky byly vytvořeny dle výsledků kvalitativního výzkumu z diplomové práce tak, aby kopírovaly jednotlivé složky vnímání bezpečnosti na internetu: sociální, technickou a institucionální. Pro formulaci otázek byly využity především předchozí odpovědi z hloubkových rozhovorů. Znění otázek a podoba škál prošla několika revizemi, které byly konzultovány s Mgr. Terezou Hannemann a PhDr. Jiřím Vinopalem, Ph.D. Dále byly otázky hodnoceny v rámci pilotních rozhovorů, po kterých se finalizovalo znění otázek a využitých škál. Pro zjištění reliability testu bylo vypočítáno Cronbachovo alfa, které vychází 0,711, tudíž považujeme test za dostatečně reliabilní pro výzkumné využití.

Pro složku sociální bezpečnosti na internetu byly využity tyto otázky:

1. Do jaké míry Vám vadí sdílet fotografie na sociálních sítích?
2. Jak moc by Vám bylo nepříjemné, kdyby na Vás byli ostatní uživatelé na internetu vulgární a uráželi Vás (např. na sociálních sítích, v diskuzích apod.)?
3. Míváte někdy pocit, že na internetu ztrácíte soukromí?

Pro složku technické bezpečnosti na internetu byly zvoleny tyto otázky:

1. Je pro Vás důležité mít internetové účty zabezpečené silným heslem?
2. Otevíráte přílohy v e-mailu i od odesílatelů, které neznáte?
3. Stalo se Vám v minulosti, že Vám kvůli napadení viry nefungoval počítač?

Pro institucionální složku bezpečnosti na internetu byly zvoleny tyto otázky:

1. Myslíte, že Vaše aktivity na internetu mohou být sledovány vládou?
2. Měl/a jste v minulosti pocit, že Váš telefon může být odposloucháván reklamními agenturami?
3. Povolujete v internetových aplikacích sledování Vaší polohy?

Pro sledování vnímané závažnosti jednotlivých složek bezpečnosti na internetu byla zařazena následující otázka:

Seřaďte dle závažnosti, jak vy osobně vnímáte následující tři „typy“ nebezpečí na internetu (1 - nejzávažnější, 3 - nejméně závažné):

- **Technické:** Zavirování počítače a ztráta dat v počítači
- **Sociální (osobní):** Zneužití osobních údajů, narušení soukromí a osobní útoky či zesměšnění od dalších uživatelů na internetu
- **Institucionální:** Sledování aktivit na internetu vládou či reklamními agenturami, odposlouchávání telefonů a sledování polohy

Dále byly sledovány proměnné vycházející z protekčně motivační teorie (PMT): vnímaný strach z výskytu určité hrozby, vnímaná pravděpodobnost vzniku hrozby na internetu a vnímané self-efficacy v rámci zvládnutí hrozby na internetu:

1 Bojíte se, že Vám někdo může přes internet ukrást peníze z Vašeho bankovního účtu?
2 Bojíte se, že na internetu může někdo zneužít Vaše osobní údaje (např. jméno, rodné číslo, adresu, telefonní číslo) ve svůj prospěch?
3 Jak velká je podle Vás šance, že budete podvedeni nepoctivým prodejcem na internetu?
4 Jak velká je podle Vás šance, že by někdo mohl využít Vaše soukromé informace k zesměšnění, vydírání nebo dalšímu zneužití?
5 Věříte, že jste schopný/á se chránit před zavirováním počítače?
6 Věříte, že se umíte vyhnout osobním útokům (vydírání, zesměšnění či šikana) od ostatních uživatelů na internetu?
7 Věříte, že dokážete posoudit důvěryhodnost stránek, na kterých se běžně pohybujete (e-shopy, diskuze, sociální sítě apod.)?

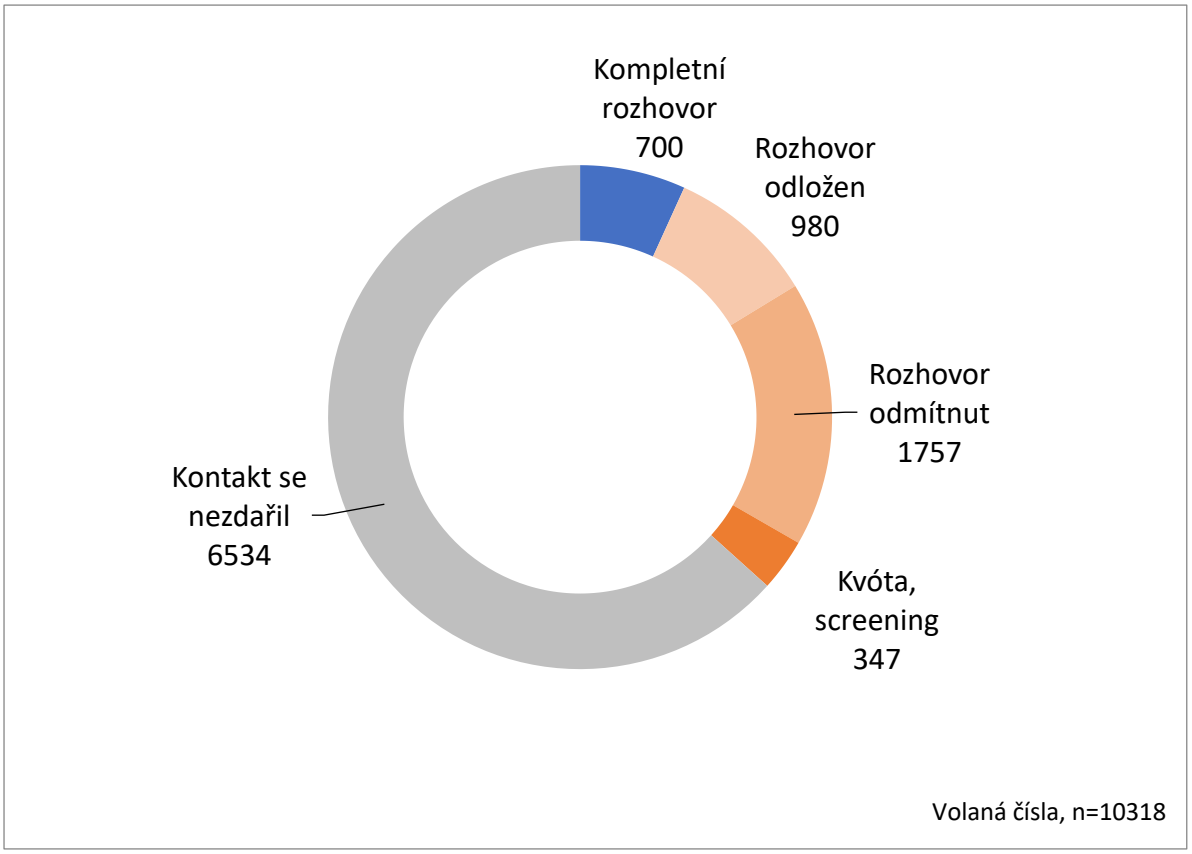
Přesné znění dotazníku, včetně využitých škál, je uvedeno *v příloze I – Výzkumný dotazník.*

7.3. Sběr dat

Jak již bylo zmíněno, výzkum probíhal za podpory programu Specifického vysokoškolského výzkumu „Adaptace aktérů a institucí na vývoj současné společnosti“ (SVV-Adakin) 2022. Po vyhovění žádosti o podporu byl vytvořen dotazník, který byl schválen pro testování. Pro dotazníkové šetření bylo zvoleno telefonické dotazování ve spolupráci s agenturou STEM/MARK, a.s. Před samotným testováním bylo provedeno zhodnocení srozumitelnosti dotazníku pěti samostatnými hovory, které měly za cíl zjistit, zda respondenti rozumí otázkám. Na základě získaných odpovědí bylo znění některých otázek nebo škál upraveno. Následně proběhlo dvacet pilotních telefonických rozhovorů, ve kterých byla znovu zkoumána srozumitelnost zadávaných otázek, zda jsou v datech správní respondenti, zda jsou v datech požadované proměnné, zda jsou tyto proměnné ve správném formátu, jestli správně funguje filtr pro výběr respondentů a zda jsou připojeny všechny dodatečné proměnné. Tato kontrola nevykázala žádné nedostatky v datovém souboru. Také bylo zjištěno, že průměrná délka hovoru činila cca 15 minut, což se následně potvrdilo i v průběhu dotazování.

Sběr dat probíhal od 18.8.-15.8. 2022. V průběhu dotazování bylo vytočeno 10 318 unikátních telefonních čísel, z toho třetina opakovaně. Ve dvou třetinách případů se vůbec nepodařilo

respondenta kontaktovat (nezvedá telefon, obsazeno, záznamník apod.). Celkem 1 757 osob odmítlo poskytnout rozhovor, dalších 980 hovorů bylo odloženo na pozdější dobu a následně neuskutečněno. Úspěšnost z volaných čísel tak byla na úrovni cca 7 %. Celkem bylo zrealizováno 700 rozhovorů.



Graf 3. – Průběh telefonického dotazování

7.4. Statistická analýza

Pro kategoriální proměnné byly vypočteny absolutní a relativní četnosti. Pro kvantitativní proměnné byly vypočteny průměr, směrodatná odchylka, medián, minimum a maximum. Testování hypotéz bylo provedeno pomocí testu nezávislosti založeném na Pearsonově korelačním koeficientu, chí-kvadrát testu nezávislosti v kontingenční tabulce a testu nezávislosti založeném na Spearmanově korelačním koeficientu. Výpočty byly provedeny pomocí programu TIBCO STATISTICA a JAMOVI, hladina významnosti pro rozhodnutí o nulové hypotéze činila 5 %.

Výpočet reliability testu byl využit výpočet Cronbachovo alfa, který vychází 0,627, kdy následně byly dvě položky převráceny. Výsledná reliabilita dotazníku má hodnotu 0,711, což je v rámci výzkumu považováno za dostatečně vysokou reliabilitu. Výzkumný dotazník bude využit pouze pro účely tohoto výzkumy a není v plánu dotazník využívat pro další měření, kdy by byla vyžadována vyšší hodnota reliability. Za tímto účelem by musela být hodnota reliability vyšší.

Skóre sociální (osobní) složky bezpečnosti bylo pro každého respondenta vypočteno jako součet kódů dle následující tabulky:

Otázka	Varianta odpovědi	Kód
1, Do jaké míry Vám vadí sdílet fotografie na sociálních sítích?	Vůbec mi nevadí Spíše mi nevadí Ani vadí/ani nevadí Spíše mi vadí Velmi mi vadí	1 2 3 4 5
2, Jak moc by Vám bylo nepříjemné, kdyby na Vás byli ostatní uživatelé na internetu vulgární a uráželi Vás?	Vůbec by mi to nebylo nepříjemné Spíše by mi to nebylo nepříjemné Ani nepříjemné/ani příjemné Spíše by mi to bylo nepříjemné Bylo by mi to velmi nepříjemné	1 2 3 4 5
3, Míváte někdy pocit, že na internetu ztrácíte soukromí?	Nikdy Výjimečně Občas Často Neustále	1 2 3 4 5

Tabulka 6. – Skóry sociální (osobní) bezpečnosti na internetu

Skóre sociální (osobní) složky bezpečnosti se mohlo pohybovat mezi 3 a 15, přičemž kódy byly zvoleny tak, aby s vyšším skóre byl spojen větší důraz na osobní bezpečnost na internetu. To znamená, pokud respondentovi vadí sdílet fotky, vadí mu urážení a vulgarity a má pocit, že ztrácí soukromí, předpokládáme, že klade na osobní bezpečnost větší důraz než respondent, kterému tyto věci nevadí.

Skóre technické složky bezpečnosti bylo pro každého respondenta vypočteno jako součet kódů dle následující tabulky:

Otázka	Varianta odpovědi	Kód
	Není to vůbec důležité Spíše to není důležité	1 2

4, Je pro Vás důležité mít internetové účty zabezpečené silným heslem?	Ani důležité/ani nedůležité Spíše je to důležité Je to velmi důležité	3 4 5
5, Otevíráte přílohy v e-mailu i od odesílatelů, které neznáte?	Nikdy Výjimečně Občas Často Pokaždé	5 4 3 2 1
6, Stalo se Vám v minulosti, že Vám kvůli napadení viry nefungoval počítač?	Nestalo se nikdy Už se mi to stalo jednou Už se mi to stalo vícekrát Děje se mi to neustále	4 3 2 1

Tabulka 7. – Skóre technické bezpečnosti na internetu

Skóre technické složky bezpečnosti se mohlo pohybovat mezi 3 a 14, přičemž kódy byly zvoleny tak, aby s vyšším skóre byl spojen větší důraz na technickou bezpečnost na internetu, podobně jako v případě sociální (osobní) složky.

Skóre institucionální složky bezpečnosti bylo pro každého respondenta vypočteno jako součet kódů dle následující tabulky:

Otázka	Varianta odpovědi	Kód
7, Myslíte, že Vaše aktivity na internetu mohou být sledovány vládou?	Nesouhlasím Spíše nesouhlasím Ani souhlas/ani nesouhlas Spíše souhlasím Souhlasím	1 2 3 4 5
8, Měl/a jste v minulosti pocit, že Váš telefon může být odposloucháván reklamními agenturami?	Nikdy jsem tento pocit neměl/a Už jsem měl/a pocit jednou Už jsem měl/a pocit vícekrát Mám tento pocit neustále	1 2 3 4
9, Povolujete v internetových aplikacích sledování Vaší polohy?	Nikdy Výjimečně Občas Často Vždy	5 4 3 2 1

Tabulka 8. – Skóre institucionální bezpečnosti na internetu

Skóre institucionální složky bezpečnosti se mohlo pohybovat mezi 3 a 14, přičemž kódy byly zvoleny tak, aby s vyšším skóre byl spojen větší důraz na institucionální bezpečnost na internetu, stejně jako v předchozích případech.

Skóre strachu z vnímané hrozby bylo pro každého respondenta vypočteno jako součet kódů dle následující tabulky:

Otázka	Varianta odpovědi	Kód
15, *Bojíte se, že Vám někdo může přes internet ukrást peníze z Vašeho bankovního účtu?*	Vůbec se nebojím Spíše se nebojím Neutrální (bez názoru) Spíše se bojím Velmi se bojím	1 2 3 4 5
16, *Bojíte se, že na internetu může někdo zneužít Vaše osobní údaje (např. jméno, rodné číslo, adresu, telefonní číslo) ve svůj prospěch?*	Vůbec se nebojím Spíše se nebojím Neutrální (bez názoru) Spíše se bojím Velmi se bojím	1 2 3 4 5

Tabulka 9. – Skóre strachu z vnímané hrozby

Skóre strachu z vnímané hrozby se mohlo pohybovat mezi 2 a 10, přičemž kódy byly zvoleny tak, aby s vyšším skóre byl spojen větší strach z vnímané hrozby.

Skóre vnímané pravděpodobnosti hrozby bylo pro každého respondenta vypočteno jako součet kódů dle následující tabulky:

Otázka	Varianta odpovědi	Kód
17, *Jak velká je podle Vás šance, že budete podvedeni nepoctivým prodejcem na internetu?*	Žádná šance Spíše žádná šance Neutrální (bez názoru) Spíše je šance Velká šance	1 2 3 4 5
18, *Jak velká je podle Vás šance, že by někdo mohl využít Vaše soukromé informace k zesměšnění, vydírání nebo dalšímu zneužití?*	Žádná šance Spíše žádná šance Neutrální (bez názoru) Spíše je šance Velká šance	1 2 3 4 5

Tabulka 10. – Skóre vnímané pravděpodobnosti hrozby

Skóre vnímané pravděpodobnosti hrozby se mohlo pohybovat mezi 2 a 10, přičemž kódy byly zvoleny tak, aby s vyšším skóre byla spojena větší vnímaná pravděpodobnost hrozby.

Skóre vnímaného self-efficacy bylo pro každého respondenta vypočteno jako součet kódů dle následující tabulky:

Otázka	Varianta odpovědi	Kód
19, *Věříte, že jste schopný/á se chránit před zavirováním počítače?*	Rozhodně nejsem schopný/á Spíše nejsem schopný/á Neutrální (bez názoru) Spíše jsem schopný/á Rozhodně jsem schopný/á	1 2 3 4 5
20, *Věříte, že se umíte vyhnout osobním útokům od ostatních uživatelů na internetu?*	Rozhodně neumím Spíše neumím Neutrální (bez názoru) Spíše umím Rozhodně umím	1 2 3 4 5
21, *Věříte, že dokážete posoudit důvěryhodnost stránek, na kterých se běžně pohybujete?*	Rozhodně nedokáži Spíše nedokáži Neutrální (bez názoru) Spíše dokáži Rozhodně dokáži	1 2 3 4 5

Tabulka 11. - Skóre vnímaného self-efficacy

Skóre vnímaného self-efficacy se mohlo pohybovat mezi 3 a 15, přičemž kódy byly zvoleny tak, aby s vyšším skóre bylo spojeno lepší vnímání své self-efficacy.

7.5. Etika výzkumu

Sběr dat probíhal formou telefonického dotazování, které bylo realizováno agenturou STEM/MARK, a.s. Výběr respondentů probíhal kvótní dle zadání (věk mezi 35-60 lety, reprezentativní soubor), přičemž další postup a generace telefonních čísel probíhala dle procedur agentury, do kterých autorka neměla přístup. V úvodu rozhovoru byl respondentům vždy krátce představen výzkum a jeho účel. Dále byli respondenti obeznámeni s tím, že jejich odpovědi jsou anonymní a účast dobrovolná. Dále bylo respondentům řečeno, že mohou kdykoliv hovor ukončit a svou účast v rozhovoru tak přerušit. Zároveň vždy po seznámení s průběhem rozhovoru byli respondenti dotázáni, zda souhlasí s pokračováním hovoru, čímž zároveň udělili souhlas se sběrem dat. V dotazníku nebyly obsaženy citlivé otázky a netýkají se citlivého tématu. Telefonický rozhovor nenesl vyšší rizika než běžný hovor průzkumu veřejného mínění.

Data byla po sběru dat přeposlána autorce v anonymizované formě, kdy není možné spojit jednotlivé odpovědi s určitým respondentem. Autorka neměla přístup k žádnému telefonnímu číslu ani ke způsobu generace telefonních čísel. Data má v současné době k dispozici pouze autorka práce.

8. Výsledky

V následující kapitole je věnována pozornost interpretaci výsledků dotazníkové šetření v rámci jednotlivých výzkumných otázek.

Existuje závislost mezi sociální (osobní) bezpečností na internetu a strachem z vnímané hrozby?

V této otázce se autorka zaměřuje na to, zda existuje závislost mezi vnímanou závažností sociální bezpečnosti na internetu a strachem z vnímané hrozby na internetu obecně.

H_0: Mezi skóre sociální (osobní) složky bezpečnosti a skóre strachu z vnímané hrozby není závislost.

H_A: Mezi skóre sociální (osobní) složky bezpečnosti a skóre strachu z vnímané hrozby je závislost.

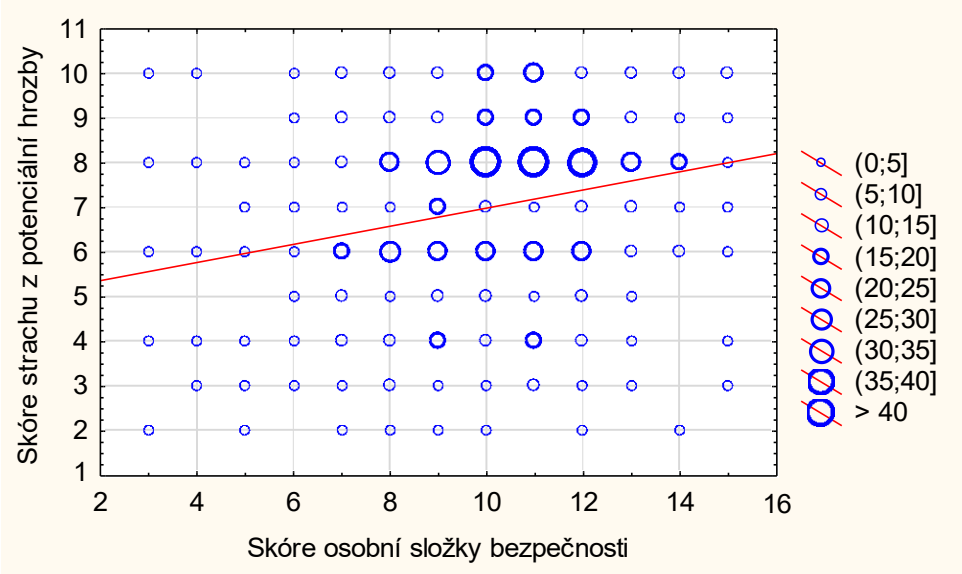
Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
0,24	0,000	zamítáme	ano

Tabulka 12. – Sociální (osobní) bezpečnost a strach z vnímané hrozby

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,000, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost mezi skóre osobní složky bezpečnosti a skóre strachu z vnímané hrozby. Vzhledem ke kladné hodnotě korelačního koeficientu, která je mezi 0,1 a 0,3, se jedná o přímou závislost o slabé intenzitě. S rostoucím skóre sociální (osobní) složky bezpečnosti je ve slabé intenzitě závislosti spojeno rostoucí skóre strachu z vnímané hrozby. Slabou rostoucí tendenci je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou. S rostoucí důležitostí a významností sociální (osobní) složky rostla u respondentů také míra vnímaného strachu či obav z potenciální hrozby na internetu.

Graf 4. - Sociální (osobní) bezpečnost a strach z vnímané hrozby



Existuje závislost mezi sociální (osobní) bezpečností a vnímanou pravděpodobností vzniku hrozby na internetu?

H_0: Mezi skóre sociální (osobní) složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby není závislost.

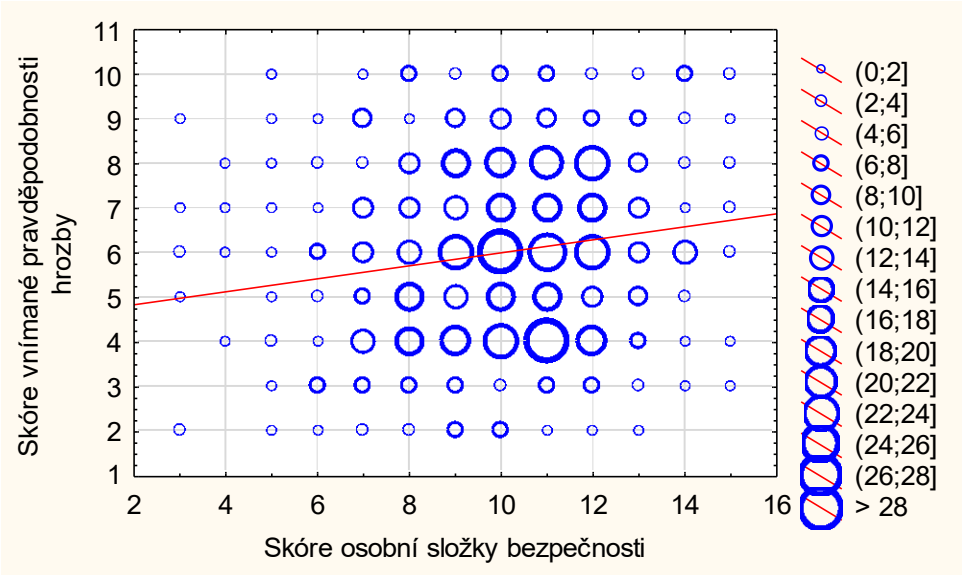
H_A: Mezi skóre sociální (osobní) složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
0,17	0,000	zamítáme	ano

Tabulka 13. – Sociální (osobní) bezpečnost a vnímaná pravděpodobnost hrozby

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,000, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost mezi skóre sociální (osobní) složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby. Vzhledem ke kladné hodnotě korelačního koeficientu, která je mezi 0,1 a 0,3, se jedná o přímou závislost o slabé intenzitě. S rostoucím skóre sociální (osobní) složky bezpečnosti je ve slabé intenzitě závislosti spojeno rostoucí skóre vnímané pravděpodobnosti hrozby. Slabou rostoucí tendenci je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.



Graf 5. – Sociální (osobní) bezpečnost a vnímaná pravděpodobnost hrozby

Existuje závislost mezi sociální (osobní) bezpečností a vnímaném self-efficacy?

H_0: Mezi skóre sociální (osobní) složky bezpečnosti a skóre vnímaného self-efficacy není závislost.

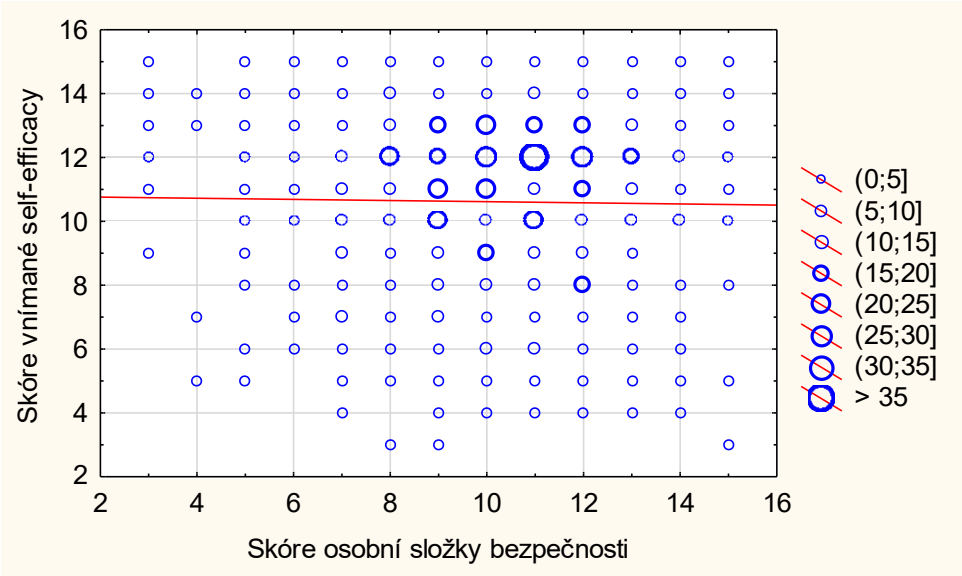
H_A: Mezi skóre sociální (osobní) složky bezpečnosti a skóre vnímaného self-efficacy je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
-0,02	0,648	nezamítáme	ne

Tabulka 14. – Sociální (osobní) bezpečnost a self-efficacy

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,648, tj. vyšší než zvolená hladina významnosti 0,05. Nulová hypotéza nebyla zamítnuta. Na hladině významnosti 0,05 nebyla prokázána závislost mezi skóre sociální (osobní) složky bezpečnosti a skóre vnímaného self-efficacy. Absenci výraznější závislosti je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.



Graf 6. - Sociální (osobní) bezpečnost a self-efficacy

Existuje závislost mezi technickou bezpečností na internetu a strachem z vnímané hrozby?

H_0: Mezi skóre technické složky bezpečnosti a skóre strachu z vnímané hrozby není závislost.

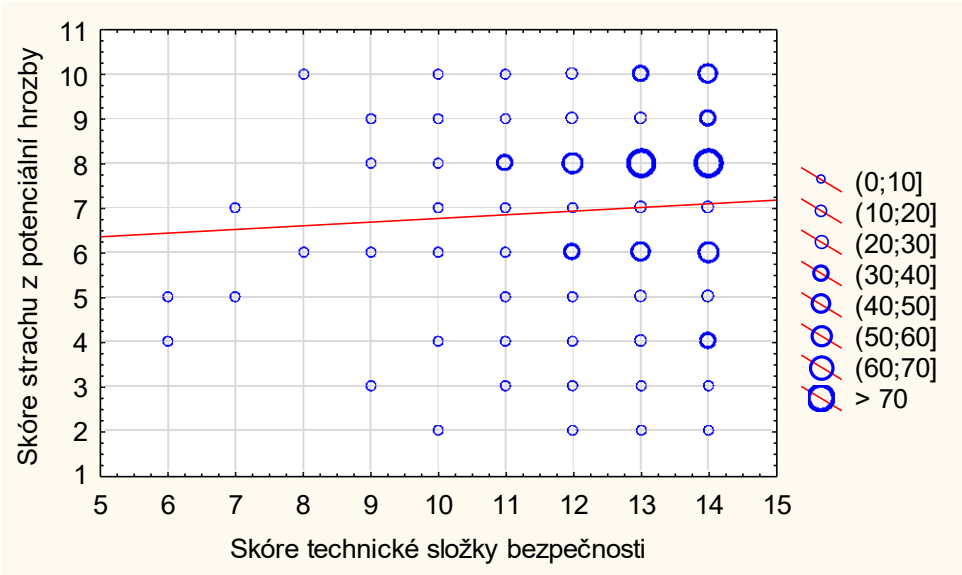
H_A: Mezi skóre technické složky bezpečnosti a skóre strachu z vnímané hrozby je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
0,05	0,165	nezamítáme	ne

Tabulka 15. – Technická bezpečnost a strach z hrozby

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,165, tj. vyšší než zvolená hladina významnosti 0,05. Nulová hypotéza nebyla zamítnuta. Na hladině významnosti 0,05 nebyla prokázána závislost mezi skóre technické složky bezpečnosti a skóre strachu z vnímané hrozby. Absenci výraznější závislosti je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.



Graf 7. - Technická bezpečnost a strach z hrozby

Existuje závislost mezi technickou bezpečností a vnímanou pravděpodobností vzniku hrozby na internetu?

H_0: Mezi skóre technické složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby není závislost.

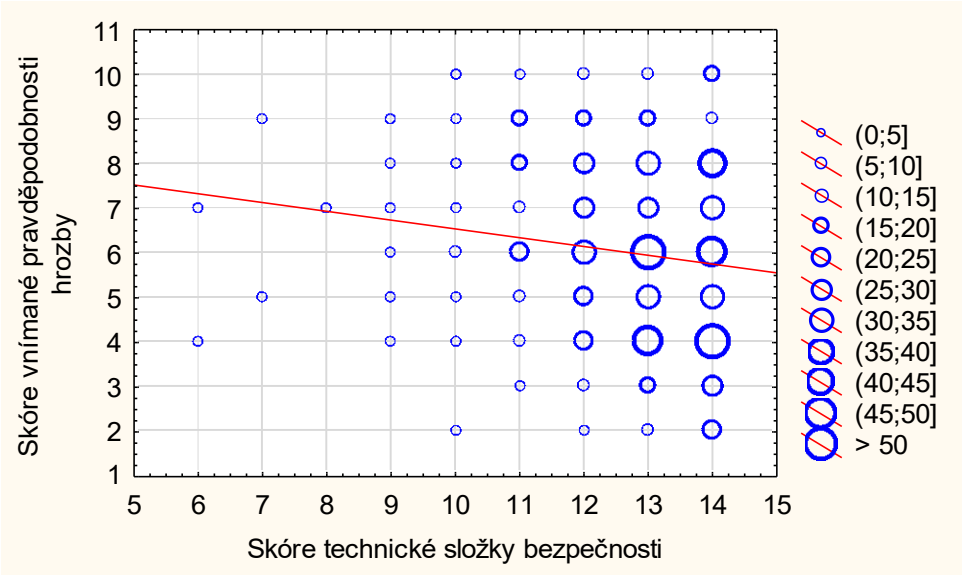
H_A: Mezi skóre technické složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
-0,13	0,001	zamítáme	ano

Tabulka 16. – Technická bezpečnost a pravděpodobnost hrozby

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,001, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost mezi skóre technické složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby. Vzhledem k záporné hodnotě korelačního koeficientu, která je mezi -0,1 a -0,3, se jedná o nepřímou závislost o slabé intenzitě. S rostoucím skóre technické složky bezpečnosti je ve slabé intenzitě závislosti spojeno klesající skóre vnímané pravděpodobnosti hrozby. Slabou klesající tendenci je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.



Graf 8. - Technická bezpečnost a pravděpodobnost hrozby

Existuje závislost mezi technickou bezpečností a vnímaném self-efficacy?

H_0: Mezi skóre technické složky bezpečnosti a skóre vnímaného self-efficacy není závislost.

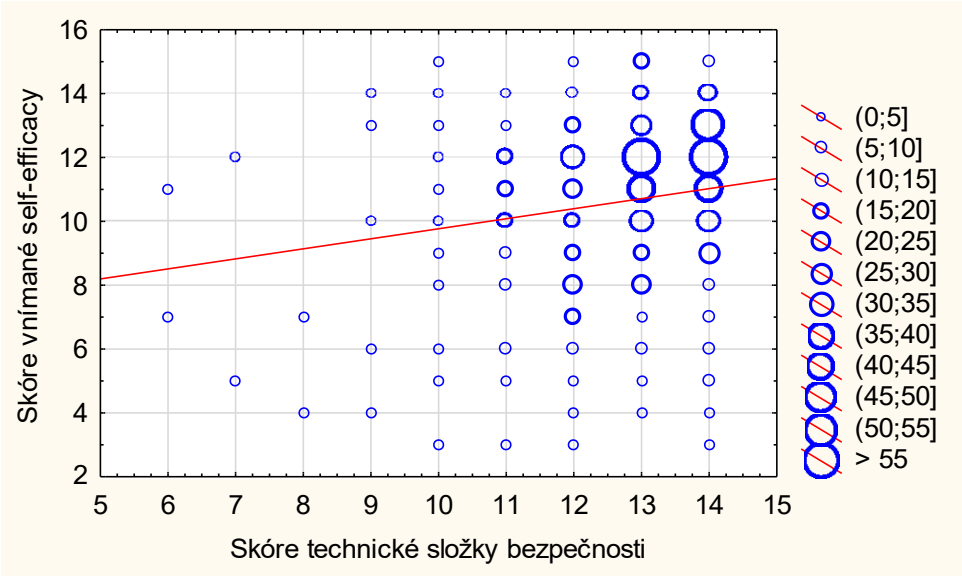
H_A: Mezi skóre technické složky bezpečnosti a skóre vnímaného self-efficacy je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
0,16	0,000	zamítáme	ano

Tabulka 17. – Technická bezpečnost a self-efficacy

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,000, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost mezi skóre technické složky bezpečnosti a skóre vnímaného self-efficacy. Vzhledem ke kladné hodnotě korelačního koeficientu, která je mezi 0,1 a 0,3, se jedná o přímou závislost o slabé intenzitě. S rostoucím skóre technické složky bezpečnosti je ve slabé intenzitě závislosti spojeno rostoucí skóre vnímaného self-efficacy. Slabou rostoucí tendenci je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.



Graf 9. - Technická bezpečnost a self-efficacy

Existuje závislost mezi institucionální bezpečností na internetu a strachem z vnímané hrozby?

H_0: Mezi skóre institucionální složky bezpečnosti a skóre strachu z vnímané hrozby není závislost.

H_A: Mezi skóre institucionální složky bezpečnosti a skóre strachu z vnímané hrozby je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
0,15	0,000	zamítáme	ano

Tabulka 18. – Institucionální bezpečnost a strach z hrozby

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,000, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost mezi skóre institucionální složky bezpečnosti a skóre strachu z vnímané hrozby. Vzhledem ke kladné hodnotě korelačního koeficientu, která je mezi 0,1 a 0,3, se jedná o přímou závislost o slabé intenzitě. S rostoucím skóre institucionální složky bezpečnosti je ve slabé intenzitě závislosti spojeno rostoucí skóre strachu z vnímané hrozby. Slabou rostoucí tendenci je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.

Graf 10. - Institucionální bezpečnost a strach z hrozby

Existuje závislost mezi institucionální bezpečností a vnímanou pravděpodobností vzniku hrozby na internetu?

H_0: Mezi skóre institucionální složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby není závislost.

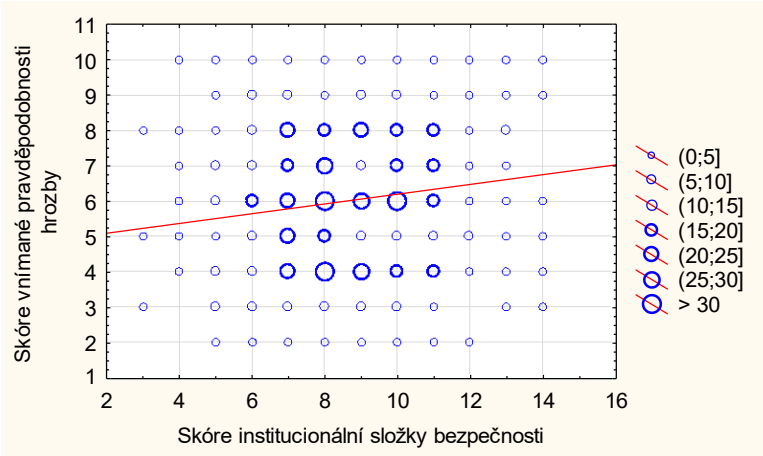
H_A: Mezi skóre institucionální složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
0,15	0,000	zamítáme	ano

Tabulka 19. – Institucionální bezpečnost a pravděpodobnost hrozby

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,000, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost mezi skóre institucionální složky bezpečnosti a skóre vnímané pravděpodobnosti hrozby. Vzhledem ke kladné hodnotě korelačního koeficientu, která je mezi 0,1 a 0,3, se jedná o přímou závislost o slabé intenzitě. S rostoucím skóre institucionální složky bezpečnosti je ve slabé intenzitě závislosti spojeno rostoucí skóre vnímané pravděpodobnosti hrozby. Slabou rostoucí tendenci je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.



Graf 11. - Institucionální bezpečnost a pravděpodobnost hrozby

Existuje závislost mezi institucionální bezpečností a vnímaném self-efficacy?

H_0: Mezi skóre institucionální složky bezpečnosti a skóre vnímaného self-efficacy není závislost.

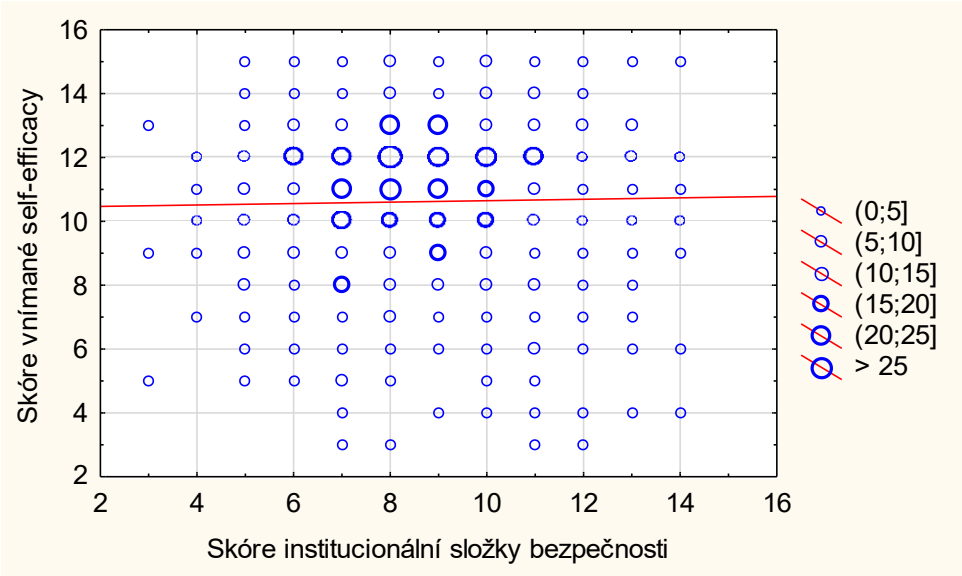
H_A: Mezi skóre institucionální složky bezpečnosti a skóre vnímaného self-efficacy je závislost.

Pearsonův korelační koeficient a test nezávislosti

hodnota R	p-hodnota	rozhodnutí o H0	závislost prokázána
0,02	0,607	nezamítáme	ne

Tabulka 20. – Instutucionální bezpečnost a self-efficacy

P-hodnota testu nezávislosti založeném na Pearsonově korelačním koeficientu vyšla s ohledem na 3 desetinná místa 0,607, tj. vyšší než zvolená hladina významnosti 0,05. Nulová hypotéza nebyla zamítnuta. Na hladině významnosti 0,05 nebyla prokázána závislost mezi skóre institucionální složky bezpečnosti a skóre vnímaného self-efficacy. Absenci výraznější závislosti je možné pozorovat na základě bodového četnostního grafu orientačně proloženého regresní přímkou.



Graf 12. - Instutucionální bezpečnost a self-efficacy

Existuje závislost mezi vnímanou závažností sociální složky bezpečnosti na internetu a pohlavím?

H_0: Pořadí, které respondenti přisuzují osobní složce bezpečnosti, nezávisí na pohlaví.

H_A: Pořadí, které respondenti přisuzují osobní složce bezpečnosti, závisí na pohlaví.

Kontingenční tabulka a chí-kvadrát test

Chí-kvadrát test p-hodnota: 0,003	Pořadí osobní (dle otázky 10)						
	První		Druhé		Třetí		celkem
Pohlaví	n	%	n	%	n	%	
Muž	144	39,8	146	40,3	72	19,9	362
Žena	178	52,7	105	31,1	55	16,3	338
Celkem	322		251		127		700

Tabulka 21. – Sociální (osobní) bezpečnost a pohlaví

P-hodnota chí-kvadrát testu nezávislosti v kontingenční tabulce vyšla s ohledem na 3 desetinná místa 0,003, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost pořadí, které respondenti přisuzují osobní složce bezpečnosti, na pohlaví. Dle relativních četností uvedených v tabulce lze interpretovat, že ženy umístily sociální (osobní) složku bezpečnosti výše než muži. Tento výsledek koresponduje také s předpoklady, které vycházely z původního kvalitativního výzkumu v diplomové práci. Při hloubkových rozhovorech se

ukazovala mírná tendence rozdílné důležitosti vnímání sociální (osobní) složky v rámci genderu. Tato skutečnost ale nebyla součástí výzkumných otázek v původním výzkumu.

Existuje závislost mezi vnímanou závažností technické složky bezpečnosti na internetu a pohlavím?

H_0: Pořadí, které respondenti přisuzují technické složce bezpečnosti, nezávisí na pohlaví.

H_A: Pořadí, které respondenti přisuzují technické složce bezpečnosti, závisí na pohlaví.

Kontingenční tabulka a chí-kvadrát test

Chí-kvadrát test p-hodnota: 0,011	Pořadí technické						
	První		Druhé		Třetí		celkem
Pohlaví	n	%	n	%	n	%	
Muž	115	31,8	111	30,7	136	37,6	362
Žena	80	23,7	137	40,5	121	35,8	338
Celkem	195		248		257		700

Tabulka 22. – Technická bezpečnost a pohlaví

P-hodnota chí-kvadrát testu nezávislosti v kontingenční tabulce vyšla s ohledem na 3 desetinná místa 0,011, tj. nižší než zvolená hladina významnosti 0,05. Nulová hypotéza byla zamítnuta ve prospěch alternativní hypotézy. Na hladině významnosti 0,05 byla prokázána závislost pořadí, které respondenti přisuzují technické složce bezpečnosti, na pohlaví. Dle relativních četností uvedených v tabulce lze interpretovat, že muži umístili technickou složku bezpečnosti výše než ženy.

Existuje závislost mezi vnímanou závažností institucionální složky bezpečnosti na internetu a pohlavím?

H_0: Pořadí, které respondenti přisuzují technické složce bezpečnosti, nezávisí na pohlaví.

H_A: Pořadí, které respondenti přisuzují technické složce bezpečnosti, závisí na pohlaví.

Kontingenční tabulka a chí-kvadrát test

Chí-kvadrát test p-hodnota: 0,262	Pořadí institucionální						
	První		Druhé		Třetí		celkem
Pohlaví	n	%	n	%	n	%	
Muž	103	28,5	105	29,0	154	42,5	362
Žena	80	23,7	96	28,4	162	47,9	338
Celkem	183		201		316		700

Tabulka 23. – Institucionální bezpečnost a pohlaví

P-hodnota chí-kvadrát testu nezávislosti v kontingenční tabulce vyšla s ohledem na 3 desetinná místa 0,262, tj. vyšší než zvolená hladina významnosti 0,05. Nulová hypotéza nebyla zamítnuta. Na hladině významnosti 0,05 nebyla prokázána závislost pořadí, které respondenti přisuzují institucionální složce bezpečnosti, na pohlaví. **Existuje závislost mezi vnímanou závažností jednotlivých složek bezpečnosti na internetu a vzděláním?**

H_0: Pořadí, které respondenti přisuzují jednotlivým složkám bezpečnosti, nezávisí na vzdělání.

H_A: Pořadí, které respondenti přisuzují jednotlivým složkám bezpečnosti, závisí na vzdělání.

Spearmanův korelační koeficient a test nezávislosti

Složka	hodnota R	p-hodnota	závislost prokázána
Osobní	-0,04	0,239	ne
Technická	-0,04	0,351	ne
Institucionální	0,08	0,038	ano

Tabulka 24. – Závažnost jednotlivých složek bezpečnosti a vzdělání

Dle testu nezávislosti založeném na Spearmanově korelačním koeficientu byla na hladině významnosti 0,05 prokázána závislost mezi stupněm dosaženého vzdělání a institucionální složkou bezpečnosti. Jednalo se však o zanedbatelnou míru závislosti, neboť hodnota korelačního koeficientu byla nižší než 0,1. Pro osobní a technickou složku bezpečnosti nebyla závislosti prokázána.

8.1. Shrnutí výsledků

V rámci výzkumu bylo sledováno, zda jednotlivé složky bezpečnosti na internetu (sociální, technická a institucionální) souvisí se strachem z potenciální online hrozby, s vnímanou pravděpodobností vzniku hrozby a s vnímaným self-efficacy v oblasti efektivní ochrany na internetu. Další výzkumnou otázkou je, zda vnímání závažnosti jednotlivých složek bezpečnosti na internetu souvisí s genderem a vzděláním respondentů.

Sociální (osobní) bezpečnost na internetu **pozitivně koreluje se skóre vnímaného strachu z potenciální hrozby (r = 0,24), dle hodnoty r se jedná o slabou přímou závislost**. Tento výsledek naznačuje, že čím významněji je vnímána sociální (osobní) bezpečnost na internetu, tím vyšší je skóre strachu z potenciální hrozby. To může ukazovat, že respondenti v oblasti sociální (osobní) bezpečnosti na internetu pociťují vyšší míru strachu z této hrozby, protože se přímo dotýká jejich integrity či jejich osobnosti na internetu. Dále sociální (osobní) bezpečnost pozitivně koreluje s vnímanou pravděpodobností vzniku hrozby (r = 0,17), kdy se opět jedná o slabou přímou korelaci. **Čím významněji je vnímána sociální (osobní) bezpečnost na internetu, tím více pravděpodobná se může hrozba respondentům zdát. V otázce vnímaného self-efficacy a vnímanou závažností sociální (osobní) bezpečnosti na internetu se neprokázala závislost (r= -0,02, p hodnota = 0,648).**

V oblasti technické bezpečnosti na internetu **nebyla prokázána korelace mezi vnímanou závažností technické bezpečnosti a vnímaným strachem z potenciální hrozby** (r = 0,05, p hodnota = 0,165). **Na druhou stranu byla prokázána slabá nepřímá závislost mezi technickou bezpečnosti a vnímanou pravděpodobností vzniku hrozby na internetu**, tzn. Čím vyšší skóre respondenti mají v rámci technické bezpečnosti, tím nižší je skóre vnímané pravděpodobnosti. Tato zjištění ukazují, že čím závažnější je dle respondentů technická bezpečnost na internetu, tím menší mají pocit, že se může potenciální hrozba objevit. To může korespondovat s tím, že v této oblasti mají jisté strategie ochrany, což by mohl potvrdit i následující závěr, kdy **byla prokázána slabá přímá závislost mezi vnímanou technickou bezpečností na internetu a vnímaným self-efficacy**, na rozdíl od sociální (osobní) bezpečnosti na internetu. Respondenti tedy pociťují větší self-efficacy v oblasti technické bezpečnosti.

Čím vyšší skóre uvádějí respondenti v oblasti institucionální bezpečnosti na internetu, tím vyšší mají skóre v oblasti strachu z vnímané hrozby. V tomto případě byla prokázána přímá závislost o slabé intenzitě (r = 0,15). Zde můžeme tedy říct, že existuje slabá závislost mezi tím, jak vysoko respondenti hodnotí institucionální bezpečnost a vnímaným strachem z potenciální hrozby. Dále podobně **vychází institucionální bezpečnost a vnímaná pravděpodobnost hrozby. I mezi těmito dvěma faktory byla prokázána přímá závislost o slabé intenzitě (r = 0,15). Naopak mezi institucionální bezpečností a vnímaným self-efficacy respondentů nebyla prokázána závislost.**

Další část dotazníku se zaměřovala právě na vnímání závažnosti jednotlivých složek bezpečnosti na internetu. Celkově byla nejzávažněji vnímána sociální (osobní) složka bezpečnosti na internetu mezi všemi respondenty. Za využití chí kvadrát testu nezávislosti byl sledován rozdíl mezi genderem a vnímáním závažnosti jednotlivých složek. **Z výsledků vychází, že ženy hodnotí sociální (osobní) složku bezpečnosti na internetu výše než muži. Naopak muži uvádějí signifikantně výše právě technickou složku bezpečnosti na internetu.** Na základě těchto výsledku je tedy možné říct, že ženy ve střední dospělosti vnímají sociální (osobní) složku bezpečnosti na internetu závažněji než muži, kdy na druhé straně muži ve střední dospělosti jako závažnější vnímají technickou bezpečnost na internetu. **V oblasti institucionální bezpečnosti nebyl prokázán signifikantní rozdíl ve vnímané závažnosti mezi muži a ženami.**

Dále byla sledována závislost mezi vnímanou závažností jednotlivých složek bezpečnosti na internetu a stupněm nejvyššího dosaženého vzdělání. **V případě technické a sociální bezpečnosti na internetu nebyla prokázána závislost mezi vnímanou závažností těchto složek a vzděláním. V případě institucionální složky byla prokázána přímá závislost mezi vnímanou závažností této složky a stupněm vzdělání, ale jedná se o zanedbatelnou závislost, kdy hodnota r = 0,08, tudíž je považována za zanedbatelnou.**

9. Diskuse

Využití technologií se zapojuje do stále více aktivit každodenního života jako je komunikace, navazování přátelských i partnerských vztahů, zasahuje do stále většího množství pracovních pozic, v průběhu vzdělávání je téměř nezbytné využívat internet. Dále se rozvíjí volnočasové aktivity spojené s internetem – internetové televize, streamovací služby, poslech hudby, rychlá dostupnost informací, online mapy, online jízdní řády, online nákupy či online bankovnictví. Téměř ke všemu máme v dnešní době vytvořenou aplikaci, která nám pomáhá při sportu, vaření, při kontrole vlastního zdraví apod. Na tento "nával" digitálních technologií je nutné reagovat i v rámci výzkumů a vědeckého poznání.

V teoretické části se autorka věnuje několika tématům, které souvisí s vybraným zaměřením práce. V první kapitole se zaměřuje především na generaci střední dospělosti, na tradiční i moderní vývojové teorie, na charakteristiku uživatelů internetu v tomto věkovém rozmezí a na mezigenerační srovnání chování na internetu. V rámci výzkumu v diplomové i rigorózní práci se autorka zaměřuje na generaci střední dospělosti, kterou vymezuje dle syntézy vybraných vývojových teorií věkem 35 – 60 let. Toto věkové rozmezí se v rámci různých teorií či výzkumů liší a není zcela jednotné. Autorka zvolila toto rozmezí také z toho důvodu, že se v ČR jedná většinou o generaci v produktivním věku, kteří se s digitálními technologiemi setkávají na každodenní bázi, ať už se jedná o jejich osobní či pracovní život. Při dotazování respondentů na jejich čas trávený na internetu se objevili i respondenti, kteří uvedli, že na internetu tráví méně než hodinu denně jak v osobním, tak pracovním životě. Průměrný čas trávený na internetu však činil 2,1 (SD = 1,5) hodiny ve volném čase a průměrně 2,6 (SD = 3) hodiny v pracovní době. Maximální hodnota času tráveného na internetu byla 10 hodin ve volném čase a 14 hodin v pracovní době. Průměrně by se tedy dalo říct, že respondenti (n = 700) uvádějí, že během dne tráví na internetu celkem cca 4-5 hodin. Z tohoto je možné vyvodit, že se respondenti setkávají s hrozbami, které plynou z užívání na internetu, a bezpečnost na internetu by pro ně měla být tématem, se kterým se běžně setkávají.

Generaci střední dospělosti není věnováno tolik prostoru v oblasti výzkumů bezpečnosti na internetu, i když i tato skutečnost se v současné době mění (White, Gummerum, Wood & Hanoch, 2017). Autoři dále uvádějí, že považují za důležité se této generaci na internetu blíže věnovat.

V předložené práci je kladen důraz na popis vybraných psychologických fenoménu, které jsou spojeny s využíváním internetu. Mezi tyto fenomény je možné zařadit například sociální inhibici na internetu, neustále připojení, internetový trolling, sociální srovnávání na internetu nebo FOMO. Tyto fenomény mohou působit, že přímo nesouvisí s bezpečností na internetu. Z hloubkových rozhovorů, které byly realizovány v diplomové práci, ale vychází najevo, že právě tyto fenomény mohou uživatelům internetu narušovat jejich osobní pocit bezpečí, mohou mít vliv na prožívání jedinců, na jejich pozornost, sebehodnocení či osobní pohodu neboli well-being (např. Ward, Duke, Gneezy & Bos, 2017; Akhtar & Morrison, 2019; Russo, Ollier-Malaterre & Morandin, 2019; Harkin & Kuss, 2021). Některými respondenty byl v diplomové práci zmiňován fenomén FoMO, neboli strach ze zameškání nějaké události jako faktor, kvůli kterému se připojili na sociální sítě. Dále bylo všemi respondenty zmíněno, že jako hlavní výhodu internetu vnímají dostupnost informací. To by bylo možné dále zkoumat z pohledu kognitivní psychologie a zmíněného Google efektu.

Tyto psychologické fenomény jsou tedy v rigorózní práci popsány a je jim věnována značná pozornost. Jak již bylo řečeno, bezpečnost na internetu je důležité vnímat jako komplexní fenomén a mohou do něj tedy zasahovat i další dílčí fenomény.

V dalších kapitolách je věnována pozornost především konkrétně bezpečnosti na internetu, jak je vnímána uživateli internetu, jaké jsou možné strategie ochrany na internetu a jaké jsou nejčastější obavy uživatelů internetu. Tyto kapitoly v celkové práci nastiňují již konkrétně fenomén bezpečnosti na internetu. Stejně jako v diplomové práci, kde se z analýzy dat ukazovalo dělení bezpečnosti na internetu na jednotlivé složky: sociální (osobní), technickou a institucionální, i v dalších výzkumech je možné sledovat jisté dělení (Raynes-Goldie, 2010; Jain, Sahoo & Kaubiyal, 2021). .

Další kapitolou je popis Protekčně motivační teorie – PMT. Tato teorie je považována za jeden z nejsilnějších teoretických konstruktů pro sledování bezpečnosti na internetu a chování uživatelů. Jak bylo zmíněno v teoretické části, PMT byla původně aplikována v oblasti zdraví, ale v dnešní době je hojně využívána ve výzkumech týkajících se digitálních technologií. PMT byla pro tento výzkum vybrána proto, že některé konstrukty PMT byly zmiňovány i v kvalitativním výzkumu v diplomové práci autorky. Mezi těmito zmiňovanými prvky byla především vnímaná pravděpodobnost potenciální hrozby a vnímané self-efficacy uživatelů. Pokud měli uživatelé pocit, že se s potenciální hrozbou dovedou vypořádat, dokázali si i určit své vlastní strategie ochrany a byli motivovaní k vlastní ochraně. Výsledky předchozího

kvalitativního výzkumu však nebylo možné, vzhledem k povaze výzkumu, generalizovat. Z toho důvodu byl také realizován kvantitativní výzkum, který je popsán v této rigorózní práci. Vybrané výzkumné otázky a cíle výzkumu přímo navazují na zjištění kvalitativního výzkumu, který byl inspirací pro sestavení dotazníkového šetření.

Porovnání výsledků výzkumu s dalšími studiemi

Cílem výzkumu je blíže zkoumat vnímání bezpečnosti na internetu u dospělých mezi 35-60 lety. Ve výzkumu je využito členění bezpečnosti na internetu na tři základní zkoumané složky, a to složku sociální, technickou a institucionální. Ve výzkumu využity prvky PMT, konkrétně vnímaný strach spojený s potenciální hrozbou na internetu, vnímaná pravděpodobnost výskytu hrozby na internetu a vnímané self-efficacy respondentů v oblasti ochrany na internetu. Cílem výzkumu je zjistit vliv zvolených prvků protekčně motivační teorie na vnímání třech složek bezpečnosti na internetu u dospělých ve střední dospělosti (35-60 let). Dále je cílem prozkoumat souvislost genderu a vzdělání s vnímáním bezpečnosti na internetu u dospělých ve střední dospělosti (35-60 let).

Rozdělení bezpečnosti, které se ukázalo ve výzkumné části podporuje rozdělení bezpečnosti na internetu dle K. Raynes-Goldieové (2010). K. Raynes-Goldieová rozdělila bezpečnost na institucionální a na sociální. V předchozím výzkumu nebylo vnímání institucionální bezpečnosti tak výrazné, i když se zde také ukazuje. Na druhou stranu se velmi výrazně objevuje právě oblast technické bezpečnosti na internetu, kterou přidávají také A. Quan-Hasseová a D. Ho (2019).

V rámci výzkumu se ukázalo, že mezi vnímanou závažností technické bezpečnosti na internetu a vnímaným self-efficacy existuje přímá slabá závislost ($r = 0{,}16$). Tyto výsledky korespondují s výsledky staršího výzkumu, který sleduje PMT a využití antivirů, které je možné řadit mezi strategie ochrany v rámci technické bezpečnosti na internetu. V tomto výzkumu se vnímané self-efficacy ukazuje jako významný prediktor pro vlastní ochranu (Lee, LaRose & Rifon, 2008). Stejné výsledky ukazují i další novější studie (Vance, Siponen & Pahnila, 2012; Mou, Cohen, Bhattacheriee & Kim, 2022; Ogbanufe & Baham, 2023). Tyto výsledky se však prokázaly pouze v oblasti technické bezpečnosti na internetu. V případě vnímané závažnosti u sociální (osobní) a technické bezpečnosti na internetu nebyl prokázán vztah s vnímaným selff-efficacy. Tyto výsledky mohou naznačovat, že mají tendence vytvářet či znát strategie, které mohou využít v případě technické bezpečnosti na internetu, ale v oblasti sociální (osobní) a

institucionální nemají vytvořené strategie ochrany a necítí tak vysokou sebe účinnost v těchto oblastech. Tato zjištění korespondují také s výsledky z diplomové práce. V hloubkových rozhovorech respondenti uváděli, že v oblasti technické bezpečnosti na internetu mají alespoň nějaký přehled o tom, jaká pravidla mají dodržovat (silné heslo, nainstalovaný antivir, aktualizace systému apod.). Pro sociální (osobní) bezpečnost se ukazovala tendence, že nejsou přesné postupy k vlastní ochraně, protože každý uživatel v této oblasti vnímá i své vlastní hranice pro narušení osobní integrity jinak. Pro oblast institucionální bezpečnosti na internetu respondenti uváděli, že mají pocit, že neexistuje efektivní způsob, jak se chránit a jejich self-efficacy v této oblasti může být pravděpodobně nízké.

Ukazuje se, že právě důvěra ve vlastní schopnosti může být dalším faktorem, který pozitivně ovlivňuje efektivní ochranu na internetu (Kezer, Sevi, Cemalcilar & Baruh, 2016). Ve výsledcích bylo mimo jiné zahrnuto dotazování týkající se pěti základních digitálních dovedností respondentů. Toto hodnocení prováděli respondenti na základě sebehodnocení vlastních dovedností. Ukazuje se, že v oblasti bezpečnosti na internetu se 47 % respondentů považuje za spíše zkušené, 12 % za velmi zkušené. Na druhou stranu 20 % respondentů uedlo neutrální postoj, 16 % se považuje za spíše nezkušené a 5 % respondentů má pocit, že jsou v oblasti bezpečnosti na internetu velmi nezkušení. I tato zjištění mohou být zajímavá pro další výzkum. Pokud tedy přihlédneme k faktu, že se ukazuje, že právě důvěra ve vlastní schopnosti může pozitivně ovlivnit efektivní ochranu na internetu, tak mezi dospělými ve střední dospělosti je až 41 % jedinců, kteří si v této oblasti nejsou zcela jisti.

Některé studie uvádějí, že se v oblasti výzkumu sledující PMT a bezpečnost na internetu málo pracuje s přidruženými emocemi (Ogbanufe & Baham, 2023). V této souvislosti autorka zvolila jako jeden z konstruktů strach, který respondenti pociťují s potenciální hrozbou na internetu. Strach je možné zařadit pod vnímanou závažnost potenciální hrozby, což je prvek PMT. Pokud budou respondenti pociťovat strach z potenciální hrozby, mohou tak vnímat potenciální hrozbu jako závažnější.

Ve výsledcích můžeme vidět, že vnímaný strach z potenciální hrozby na internetu pozitivně koreluje se složkou sociální (osobní) a institucionální bezpečnosti na internetu. To znamená, čím vyšší významnost přikládají respondenti složkám sociální (osobní) a institucionální, tím vyšší mají skóre v oblasti strachu. Mezi vnímaným strachem a technickou bezpečností nebyla prokázána souvislost. Jak ukazují zmíněné studie (Xu a kol., 2022; Sobol & Giroux, 2023),

strach je jedním z důležitých prediktorů chování, který může motivovat uživatele k ochranným opatřením.

Další zkoumanou proměnnou je vnímaná pravděpodobnost výskytu hrozby na internetu. Tato proměnná je jedním z významných faktorů, které mohou ovlivňovat chování na internetu. Často je e výzkumech spojována s behaviorální reakcí jedinců a s účinností ochranné reakce. Pokud jedinci věří, že jsou jejich ochranná opatření účinná, tak se stejně mohou pustit do rizikových aktivit, i když vnímají hrozbu jako pravděpodobnou (Sobol & Giroux, 2023). nímaná pravděpodobnost hrozby pozitivně koreluje se sociální (osobní) složkou bezpečnosti na internetu, zatímco negativně koreluje s technickou složkou bezpečnosti na internetu. Toto zjištění může opět korespondovat s tím, že v oblasti technické bezpečnosti mají obecně uživatele více možností, jak se chránit a mohou tedy více důvěřovat svým bezpečnostním strategiím (do technické bezpečnosti je možné zařadit ochranu pomocí antiviru a dalších softwarových nastavení). To v případě sociální (osobní) a institucionální aplikovat nemůžou, tam se musí spoléhat na sebe, na své hranice a částečně i na své okolí a lidi, které si pustí do svého online osobního prostoru. Toto zjištění může vyvolávat otázku, zda jedinci na internetu více důvěřují nainstalovaným programům nebo sobě.

Výzkumy ukazují, že je možné sledovat rozdíl v chování na internetu a zabezpečením na internetu i v souvislosti s genderem. Například se ukazuje, že ženy využívají méně protektivních strategií ochrany (McGill & Thompson, 2018). Ženy dle výzkumu nevyužívají silná hesla a neaktualizují své zařízení tak často jako muži (Gratian, Bandi, Cukier, Dykstra & Ginther, 2017). V rigorózní práci byl sledován vztah mezi genderem a vnímanou závažností jednotlivých složek bezpečnosti na internetu. Tato otázka vznikla již při realizaci diplomové práce, kde vznikl první předpoklad, že by mezi vnímáním mužů a žen v oblasti bezpečnosti na internetu mohl být rozdíl. V rámci hloubkových rozhovorů se objevovala tendence žen hodnotit některé obrazové materiály jako více potenciálně nebezpečné než muži. V diskuzi diplomové práce byl tento fakt nastíněn, ale vzhledem k malému výzkumnému vzorku a kvalitativní povaze výzkumu nebylo možné tuto domněnku ve výsledcích prezentovat. V tomto výzkumu byl na otázku genderu naopak kladen důraz. Ukazuje se, že ženy signifikantně závažněji hodnotí sociální (osobní) bezpečnost oproti mužům. Na druhé straně muži jako závažnější vnímají technickou bezpečnost na internetu. Tato zjištění korespondují s výsledky výše zmíněných studií. I když některé studie uvádějí, že v chování není rozdíl v rámci genderu (např. Barak & Gluck-Ori, 2007), v tomto výzkumu se rozdíl ukazuje. Vysvětlením může být, že ženy

jsou citlivější v případě sociální (osobní) bezpečnosti na internetu, která zahrnuje možné obavy ohledně využití osobních informací k pomluvě, vyvolání konfliktu, zneužití např. intimních fotografií, veřejné vysmívání, urážlivé komentáře apod. Zatímco na druhou stranu muži mohou být více citliví v oblasti technické bezpečnosti, které zahrnuje např. materiální ztrátu, zavirování osobního zařízení, viry, spamy, ztráta dat, nabourání bankovního účtu apod. Toto rozdílné vnímání závažnosti jednotlivých složek může také souviset s tím, jaká ochranná opatření na internetu zástupci každého genderu zvolí.

Některé studie uvádějí (Roberts, Indermaur & Spiranovic, 2013; nebo Brands & Wilsem, 2019), že lidé s nižším vzděláním mohou mít větší strach z finančních rizik na internetu, a tak méně využívají internetové bankovnictví a platby přes internet. Zároveň některé studie ukazují, že gramotnost a znalosti týkající se zabezpečení na internetu mohou být protektivním faktorem na internetu. Zároveň mohou být lidé, kteří jsou gramotnější v oblasti technologií, efektivnější ve vlastní ochraně (Kezer, Sevi, Cemalcilar & Baruh, 2016). Tyto výsledky naznačují, že vzdělání může souviset s chováním na internetu, které vede k vlastnímu zabezpečení. V předloženém výzkumu bylo vzdělání sledováno v souvislosti s vnímanou závažností jednotlivých složek bezpečnosti na internetu. Ve výzkumu však nebyla prokázána žádná souvislost mezi tím, jaký mají uživatelé ve střední dospělosti dosažený stupeň vzděláním a vnímanou závažností zmíněných složek bezpečnosti na internetu. Z výsledků tedy vidíme, že vzdělání pravděpodobně neovlivňuje vnímání závažnosti jednotlivých složek, ale dle zmíněných studií může být považován za prediktor chování v oblasti ochrany na internetu.

Limity výzkumu

Sběr dat probíhal telefonickým dotazováním ve spolupráci s agenturou STEM/MARK, a.s. za podpory programu Specifického vysokoškolského výzkumu „Adaptace aktérů a institucí na vývoj současné společnosti“ (SVV-Adakin) 2022. Díky této spolupráci bylo možné realizovat výzkum za poměrně krátký čas. Zároveň pro tuto práci byly poskytnuty finanční prostředky pro zaplacení dotazníkového šetření. V rámci této spolupráce byl, vzhledem k poskytnutým finančním prostředkům, předem daný počet proměnných, které je možné do dotazníku zařadit. Při vytváření výzkumného dotazníku tedy byla částečně limitující horní hranice počtu otázek, která byla naplněna.

Dotazník procházel několika revizemi tak, aby obsahoval alespoň dvě otázky týkající se každé sledované proměnné. Je možné, že právě tento omezený počet otázek, které mohou pokrýt

určitý sledovaný konstrukt mohl ovlivnit výsledné hodnoty. Otázky byly vytvářeny především z rozsáhlé analýzy 16 hloubkových rozhovorů, kdy na základě častých a významných odpovědí respondentů byly zařazeny výsledné otázky. Znění otázek bylo konzultováno s konzultantkou diplomové práce Mgr. Terezou Hannemann a s PhDr. Jiřím Vinopalem, Ph.D. Následně bylo znění otázek i škál podrobeno pilotnímu testování, po kterém byly některé položky dále upřesněny či bylo pozměněno jejich znění. Žádná položka však nebyla po pilotních rozhovorech vyřazena.

Autorka práce dále nebyla účastna samotnému sběru dat. Sběr dat probíhal plně v zastoupení agenturou STEM/MARK, a.s., což bylo součástí získání této podpory. S agenturou byl předem konzultován záměr výzkumu, pracovníci agentury byli seznámeni s postupy, které jsou potřeba dodržovat při realizaci vysokoškolského výzkumu. Jednalo se především o dodržení etických pravidel. Mezi tato pravidla patřila především anonymita účastníků, jejich dobrovolná účast, možnost hovor kdykoliv ukončit a také poučení o tom, že pokud respondent z jakéhokoliv důvodu nebude chtít na otázku odpovědět, tak nemusí. Všechna tato etická pravidla byla během sběru dat dodržena.

Pro sběr dat byla zvolena metoda CATI neboli telefonické dotazování. Tato varianta byla zvolena i s ohledem na menší velikost výsledného výzkumného souboru. Vzhledem k charakteru otázek byla zvolena tato metoda právě proto, že některé položky mohly být respondentům dovysvětleny či zopakovány.

Spolupráce s agenturou STEM/MARK, a.s. bylo možné získat přesný výběr dotazovaného vzorku, který byl kvótní. Naplnily se tak všechny požadavky pro splnění reprezentativního výzkumného souboru. Sběr dat touto formou poskytnul značnou časovou variabilitu a rychlost při sběru dat, který byl realizován během jednoho týdne. Je nutné podotknout, že by nebylo v silách autorky takto rychle a efektivně realizovat sběr dat. Jako limit je možné vnímat to, že autorka nebyla přítomna sběru dat a nemohla tak v průběhu již do způsobu sběru dat zasahovat. Na druhou stranu sběr dat byl provázen objektivní osobou, která měla přesně daný postup od autorky práce, jasné znění otázek a nemohla tak příliš zasahovat do odpovědí respondentů podle záměrů výzkumu.

Sběr dat probíhal v srpnu 2022, zatímco samotná analýza a sepsání rigorózní práce probíhalo během roku 2024. Toto odložení zpracování dat nastalo vzhledem k mateřské dovolené autorky. Tato prodleva mezi realizací sběru dat a jeho následným zpracováním má také značné

limity pro práci. Časová prodleva mohla například změnit i samotné vnímání využitých otázek autorkou. Dalším limitem této prodlevy je, že data mohla ztratit na své aktuálnosti a jejich interpretace tak přichází se zpožděním a současné odpovědi respondentů by se mohly lišit. Na výsledky výzkumu by v současné době mohl mít vliv také další rozvoj digitálních technologií, zapojení umělé inteligence do zabezpečení na internetu a do dalších aktivit. Během posledních dvou let se mohly objevit nové hrozby a respondenti mají nové zkušenosti a znalosti. V kapitole *7.3. Sběr dat* je tato skutečnost zmíněna, včetně přesného datumu sběru dat, tudíž je důležité tento fakt také zohlednit při čtení výsledků a závěrů výzkumu.

Návrhy pro další výzkumy a aplikace do praxe

V dalších výzkumech je možné více aplikovat navrhnuté dělení bezpečnosti na internetu. Zároveň jak jsem již zmiňovala, obor digitálních technologií je velmi dynamický a rychle se rozvíjející obor, proto je potřeba reagovat i souvisejícími výzkumy. V tomto případě je možné zařadit několik replikačních studií, které budou sledovat to, co již bylo sledováno předchozími výzkumy. To, co je vyzkoumáno může být během několika let neplatné nebo úplně jiné.

Dále by bylo možné zařadit také experimentální studie, která by sledovala nejen korelaci, ale také kauzalitu některých vztahů týkajících se bezpečnosti na internetu. V teoretické části je navrhnuto mnoho podtémat, které je možné v rámci kyberpsychologie sledovat, např. vliv sociální disinhibice, dopad fenoménu FOMO, internetový trolling nebo se více věnovat rozvinutí PMT v kontextu bezpečnosti na internetu i o emocionální složky. Dále jsou v práci popsány mnohé faktory, které mohou s chováním na internetu souviset a mohou být dále zkoumány.

V současné době přichází také velmi důležitý prvek související s bezpečností na internetu, a to je umělá inteligence. Umělá inteligence má kolem sebe spoustu otázek a je možné, že pro odbornou i pro laickou veřejnost může mít často negativní konotace. V dalších výzkumech je možné sledovat vnímání umělé inteligence, vliv umělé inteligence na chování na internetu, zda uživatelé internetu rozpoznají, kdy pracují s umělou inteligencí apod.

Výsledky ukazují, že prvky PMT souvisí s chováním a bezpečností na internetu. Zároveň se ukazuje, že dělení bezpečnosti na internetu by mohlo být efektivní a přínosné pro další výzkumy i aplikaci v intervenčních či edukativních programech, jelikož výsledky se v jednotlivých složkách mírně liší, což ukazuje na rozdílnost a důležitost tohoto dělení.

10. Závěr

Předložená rigorózní práce se věnuje vnímání bezpečnosti na internetu u generace střední dospělosti. Práce popisuje generaci střední dospělosti z pohledu moderních i tradičních vývojových teorií a podává ucelený přehled možných psychologických fenoménů, které se pojí s bezpečností na internetu. Zároveň je v práci popsána bezpečnost na internetu, její vnímání, možné dělení a s bezpečností spojené obavy uživatelů internetu. Práce dále rozpracovává PMT v kontextu digitálních technologií.

Výzkumná část popisuje realizovanou korelační studii sledující vnímaní bezpečnosti na internetu u respondentů ve střední dospělosti v souvislosti s vybranými konstrukty PMT. Výzkum probíhal formou telefonického dotazování reprezentativního souboru respondentů (n = 700). Bylo zvoleno celkem 13 výzkumných otázek a k tomu zvolených hypotéz. Realizovaný výzkum vychází z diplomové práce a navazuje na výsledky předchozího výzkumu, ve kterém byla bezpečnost rozdělena na tři základní složky: sociální (osobní), technickou a institucionální. Každá složka bezpečnosti na internetu byla v rámci analýzy dat sledována samostatně a výsledky se liší u každé vyjmenované složky. Tento fakt ukazuje, že navrhnuté dělení bezpečnosti na internetu je možné aplikovat do praxe, jelikož každá složka nese jiné konotace. Například v případě sociální (osobní) a institucionální bezpečnosti na internetu se ukázala přímá slabá korelace mezi těmito složkami a vnímaným strachem z potenciální hrozby, zatímco v případě technické bezpečnosti tato korelace nebyla prokázána. V případě vnímané pravděpodobnosti hrozby byla prokázána slabá přímá korelace se sociální (osobní) a institucionální složkou, zatímco s technickou složkou se ukazuje naopak nepřímá korelace. Vnímané self-efficacy přímo koreluje s technickou bezpečností na internetu, ale nebyla prokázána korelace se sociální (osobní) a institucionální složkou. Výsledky také naznačují, že gender může mít vliv na vnímanou závažnost jednotlivých složek bezpečnosti na internetu, kdy ženy hodnotí jako závažnější sociální (osobní) složku a muži naopak technickou. Stupeň dosaženého vzdělání v prezentované studii nekoreluje s žádnou složkou bezpečnosti na internetu.

Výsledky práce mohou přispět k lepšímu pochopení fenoménu bezpečnosti na internetu a předkládají nový pohled na možné dělení a další výzkumnou či intervenční práci v oblasti bezpečnosti na internetu u dospělých ve věku 35-60 let.

Reference

Akdemir, N. (2020). Examining the impact of fear of cybercrime on internet users' behavioral adaptations, privacy calculus and security intentions. *International Journal of Eurasia Social Sciences, 11(40)*, 606-648.

Akhtar, S. & Morrison, C.M. (2019). The prevalence and impact of online trolling of UK members of parliament. *Computers in Human Behavior,* 99, 322–7.

Alhabash, S., Jiang, M., Brooks, B., Rifon, N. J., Larose, R., & Cotten, S. R. (2015). Online banking for the ages. *Communication and information technologies annual studies in media and communications, 10*, 145–171.

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. New York: Holt, Rinehart, & Winston.

Anderson, C.L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly, 34(3)*, 613-643.

APA (2020). *Publication Manual of the American Psychological Association* (7th Ed.). American Psychological Association.

Baltes, P. B., Staudinger, U. M., & Lindenberger, U. (1998). Life-span theory in developmental psychology. W. Damon. & R.M. Lerner. *Handbook of child psychology: Vol. 1. Theoretical models of human development* (5. vyd.,1029 – 1143). New York: Wiley.

Barak, A., & Gluck-Ofri, O. (2007). Degree and reciprocity of self-disclosure in online forums. *CyberPsychology & Behavior*, *10(3)*, 407–417.

Barnes, S.B. (2006). ‚A privacy paradox: social networking in the United States'. *First Monday, (11)9*. Dostupné z: https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312

Bartsch, M., & Dienlin, T. (2016). Control your Facebook. *Computers in Human Behavior, 56(3)*, 147–154.

Baruh, L., & Cemalcılar, Z. (2014). It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences, 70*, 165-170.

Betina, A. & Megha, M. (2021). Fake news during Covid-19 outbreak: Differentiating audience's age regarding prior exposure, emotion, susceptibility, practise, and forward behaviour. *Media Watch, 12(2)*, 251-264.

Binns, A. (2012). DON'T FEED THE TROLLS! Managing troublemakers in magazines' online communities. *Journalism Practice*, *6*(4), 547-562.

Blatný, M. (ed.). (2017). *Psychologie celoživotního vývoje*. Praha: Karolinum.

Bolton, R. N., Parasuraman, A., Hoefnagels, A., Kabadayi, S., Gruber, T., Loureiro, Y. K., ... & Solnet, D. (2013). Understanding Generation Y and their use of social media: A review and research agenda. *Journal of Service Management, 24(3)*, 245–267.

Boyd, D. (2008). *Taken out of context. American teen sociality in networked publics*. Ph.D. Dissertation, University of California, Berkeley. Dostupné z: http://www.danah.org/papers/ TakenOutOfContext.pdf

Brands, J. & Van Wilsem, J. (2019). "Connected and Fearful? Exploring Fear of Online Financial Crime, Internet Behaviour and Their Relationship". *European Journal of Criminology, 40(1)*, 1-22.

Brauer, K., Sendatzki, R., & Proyer, R.T. (2022). Localizing gelotophobia, gelotophilia, and katagelasticism in domains and facets of maladaptive personality traits: A multi-study report using self- and informant ratings. *Journal of Research in Personality, 98*, 1-13.

Bronfenbrenner, U. (2005). The bioecological theory of human development (2001). U. Bronfenbrenner. *Making human beings human: Bioecological perspectives on human development* (3 – 15). Thousand Oaks: Sage Publications.

Craker, M. & March, E. (2016). The dark side of Facebook®: The dark tetrad, negative social potency, and trolling behaviors. *Personality and Individual Differences, 102*, 79-84.

Danet, M., & Miljkovitch, R. (2017). Monde virtuel : enjeux et risques liés à l'attachement. *Psychologie Française, 62(1)*, 57–83.

Day, A., Barber, L., & Tonet, J. (2019). *Information communication technology and employee well-being: Understanding the "iParadox Triad" at work.* Landers., R.N. (2019). *The Cambridge handbook of technology and employee behavior,* (580–607). Cambridge: Cambridge University Press.

Dhir, A., Kaur, P., Lonka, K., & Nieminen, M. (2016). Why do adolescents untag photos on Facebook?. *Computers in Human Behavior, 55(2),* 1106–1115.

Dindia, K., & Allen, M. (1992). Sex differences in self-disclosure: A meta-analysis. *Psychological Bulletin, 112(1)*, 106–124.

Duggan, M. (2017). Online harassment 2017. *Pew Research Center*. Dostupné z: www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Egelman, S., & Peer, E. (2015). Scaling the Security Wall. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 2873-2882.

Elder G.H. Jr. & Giele, J.Z. (2009). Life course studies: An evolving field. G.H. Elder, Jr. & J.Z. Giele. (2009). *The craft of life course research*. New York: Guilford Publications.

Erikson, E. (1997). *Životní cyklus rozšířený a dokončení.* Praha: Nakladatelství Lidové Noviny.

Festinger, L. (1954). A theory of social comparison processes. *Human Relations, 7*, 117–140.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25(1)*, 153–160.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security, 2008(4),* 6–9.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2017). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345–358.

Grinberg, N., Kalyanaraman, S., Adamic, L. A., & Naaman, M. (2017). Understanding feedback expectations on facebook. In C.-M. E. Yau, & T. Williams (Eds.). *Hong Kong neo-noir* (726–739). Edinburgh: Edinburgh University Press.

Halevi, T., Lewis, J. & Memon, N. (2013). *A pilot study of cyber security and privacy related behavior and personality traits.* Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro, 737-744.

Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. *Journal of Politeness Research, 6*, 215–242.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" explaining the privacy paradox with online apathy. *International Journal of Communication, 10,* 3737–3757.

Harkin, L.J. & Kuss, D. (2021). "My Smartphone Is an Extension of Myself": A Holistic Qualitative Exploration of the Impact of Using a Smartphone. *Psychology of Popular Media, 10(1)*, 28-38.

Havighurst, R. J. (1972). *Developmental tasks and education.* New York: David McKay.

Hayes, R. A., Carr, C. T., & Wohn, D. Y. (2016). One click, many meanings: Interpreting paralinguistic digital affordances in social media. *Journal of Broadcasting & Electronic Media, 60*(1), 171–187.

Hermans, H. J., & Oles, P. K. (1999). Midlife Crisis in Men: Affective Organization of Personal Meanings. *Human Relations, 52(11),* 1403–1426.

Holmes, T. H., & Rahe, R. H. (1967). The social readjustment rating scale. *Journal of Psychosomatic Research, 11(2)*, 213-218.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media. *Decision Support Systems, 55(4)*, 948–956.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media. *Decision Support Systems, 55(4)*, 948–956.

Charmaz, K. (2014). *Constructing Grounded Theory, 2.vyd*. Los Angeles: SAGE.

Chen, Y. (2018). “Being a butt while on the internet”: Perceptions of what is and isn't internet trolling. *Proceedings of the Association for Information Science and Technology*, *55*(1), 76-85
Jain, S., Sahoo, S.R. & Kaubiyal, J. (2021). Online Social Networks Security and Privacy: Comprehensive Review and Analysis. *Complex & Intelligent Systems,* 7, 2157-2177.

Kail, R. V., & Cavanaugh, J. (2017). *Human development: A life-span view.* 8. vyd. Mason, OH: CENGAGE Learning Custom Publishing.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(1),* 1-20.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(1),* 1-20.

Kopáňková, N. (2021). *Bezpečnost a chování na internetu u dospělých se základním vzděláním*. Diplomová práce. Univerzita Karlova. Filozofická fakulta.

Kopecký, K., Szotkowski, R., Kožíšek, M. & Kasáčková, J. (2018). *Starci na internetu (výzkumná zpráva)*. Centrum prevence rizikové virtuální komunikace.

Kunst A. Opinions on internet trolling in the U.S. 2017. Statista 2019. Dostupné online 30.8.2024 z: https://www.statista.com/statistics/380047/agree-disagree-internet-trolling/

LaRose, R., & Rifon, N. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs, 41(1)*, 127–149.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour and Information Technology, 27(5),* 445–454.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14(1),* 79–100.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2013). *In their own words: What bothers childrenonline? With the EU Kids Online Network. EU Kids Online, LSE.*

Lutz, C., & Ranzini, G. (2017). Where dating meets data. *Social Media + Society, 3(1)*, 1–12.

Maaß, W. (2011). *The elderly and the internet.* S. Trepte & L. Reinecke. (2011). Privacy online (235–249). Heidelberg, Germany: Springer.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). *Teens, social media, and privacy.* Pew Research Center, Internet & Technology. Dostupné z: https:// www.pewresearch.org/internet/2013/05/21/teens- social-media-and-privacy/

March, E., & Steele, G. (2020). High esteem and hurting others online: Trait sadism moderates the relationship between self-esteem and internet trolling. Cyberpsychology Behavior and Social Networking, 23, 441–446.

Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13(1)*, 114–133.

Masui, K. (2019). Loneliness moderates the relationship between Dark Tetrad personality traits and internet trolling. *Personality and Individual Differences*, 150, 1-5.

Mazmanian, M., Orlikowski, W.J. & Yates, J. (2013). The Autonomy Paradox: The implications of mobile email devices for knowledge professionals. *Organization Science, 24(5)*, 1337-1357.

McGill, T.J. & Thompson, N. (2018). Gender Differences in Information Security Perceptions and Behaviour. *Australasian Conference on Information Systems 2018.*

Mehraj, H., Jayadevappa, D., Haleem, S.L.A., Parveen, R., Madduri, A., Ayyagari, M.R. & Dhabliya, D. (2021). Protection Motivation theory using multi-factor authentication for providing security over social networking sites. *Patter Recognition Letters, 152*, 218-224.

Merriam, S., & Mullins, L. (1981). Havinghurst's adult development tasks. *Activities, Adaptation & Aging, 1(3),* 9–22.

Millová, K. (2017). *Střední dospělost*. Blatný, M. (2017). Psychologie celoživotního vývoje. Praha: Karolinum.

Miniwatts Marketing group. (2020). *Internet Users Distribution in the World - 2021.* Online.

Mou, J., Cohen, J.F., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach, *Journal of the Association for Information Systems*, 23(1), 196-236.

Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D.A. & Nielsen, R.K. (2017). *Reuters Institute Digital News Report 2017*. Dostupné z (25.6.2024): https:// reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report %202017%20web_0.pdf

Ngyuen, M.H. (2021). Managing Social Media Use in an "Always On" Society: Exploring Digital Wellbeing Strategies That People Use to Disconnest. *Mass Communication and Society, 24(6),* 795-817.

Norton, A. M., & Baptist, J. (2014). Couple boundaries for social networking in middle adulthood: Associations of trust and satisfaction. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8(4)*, 1-15.

Ogbanufe, O. M., & Baham, C. (2023). Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. *Information systems frontiers*, *25*(2), 897-916

Papacharissi, Z., & Gibson, P. L. (2011). *15 minutes of privacy: Privacy, sociality, and publicity on social network sites.* In S. Trepte, & L. Reinecke (Eds.): Privacy online: Perspectives on privacy and self-disclosure in the social web (75–89). Heidelberg and New York: Springer. *Organization Studies, 32(7), 941–961.*

Parker, R.G. & Parrott, R. (1995). Patterns of Self-Disclosure across Scoial Support Netvworks: Elderly, Middle-Aged, and Young Adults. *International Journal of Aging & Human Development, 41(4)*, 281-297.

Parris, L., Varjas, K., Meyers, J., & Cutts, H. (2012). Highschool students' perceptions of coping withcyberbullying. *Youth & Society, 44(2),* 284–306.

Petronio, S. (2002): *Boundaries of privacy.* Dialectics of disclosure. Albany, NY: SUNY Press.

Pfattheicher, S., Lazarevic, L.B., Westgate, E.C. & Schindler, S. (2021). On the Relation of Boredom and Sadistic Aggression. *Journal of Personality and Social Psychology*, *121(3),* 573-600.

Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers In Human Behavior, 29(4)*, 1841-1848.

Příhoda, V. (1977). *Ontogeneze lidské psychiky*. 4. vyd. Praha: Státní pedagogické nakladatelství.

Quan-Haase, A. & Ho, D. (2019). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of Information Science and Technology, 71(9),* 997-10001.

Ragnedda. M. (2018). Conceptualizing digital capital. *Telematics and Informatics, 35(8),* 2366 2375.

Rainie, L., Kiesler, S., Kang, R. & Madden, M. (2013). *Anonymity, Privacy, and Security Online.* Washington DC: Pew Research Center's Internet & American Life Project. Dostupné z (30.6.2024): https:// www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

Raynes-Goldie, K. (2010) 'Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook', First Monday, (15)1, Dostupné z (dne 26.6.2024): http://firstmonday.org/htbin/cgiwrap/ bin/ojs/index.php/fm/article/ view/2775/2432.

Riquelme, I. & Roman, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers?. *Electronic Markets, 24(2),* 135-49.

Roberts, L. D., Indermaur, D. & Spiranovic, C. (2013). "Fear of Cyber-Identity Theft and Related Fraudulent Activity". *Psychiatry, Psychology and Law, 20(3),* 315-328.

Rogers, W.R. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91(1),* 93-114.

Rosenthal-on der Pütten, A.M., Hastall, M.R., Köcher, S., Meske, Chr., Heinrich, T., Labrenz, F. & Ocklenburg, S. (2019). „Likes“ as social rewards: Their role in online social comparison and decisions to like other People’s selfies. *Computers in Human Behavior*, *92*,76-86.

Rubin, V.L., Chen, Y., & Conroy, N.J. (2016). Deception detection for news: Three types of fakes. *Proceedings of the Association for Information Science and Technology, 51(1)*, 1–4.

Russo, M., Ollier-Malaterre, A. & Morandin, G. (2019). Breaking out from constant connectivity: Agentic regulation of smartphone use. *Computers in Human Behavior, 98(4)*, 11-19.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation. *American Psychologist, 55(1)*, 68–78.

Říčan, P. (2006). *Cesta životem. 2. přeprac. vyd.* Praha: Portál.

Scott, S.G. & Bruce, R.A. (1995). Decision-Making Style: The Development and Assessment of a New Measure. *Educational and Psychological Measurement, 55(5),* 818-831.

Shachaf, P. & Hara, N. (2010). Beyond vandalism: Wikipedia trolls. Journal of Information Science, 36(3), 357–70.

Shi, R., Qiqi, L., & Guangzhu Wu. (2023). Risk Perception and Sense of Public Health Safety: The Mediating Role of Emotional Perception. *Sustainability,* 15(21), 1-17.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior, 48,* 199–207.

Schaik, P., Jeske, D., Onibokun., J., Coventry, L., Jansen, J. & Kusev, P. (2021). Risk perception of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75, 547-559.

Schulz, R., & Heckhausen, J. (1996). A lifespan model of successful aging. *American Psychologist, 51(7),* 702–714.

Sobol, K. & Giroux, M. (2023). Threat specifity in fear appeals: examination of fear response and motivated behavior, *Journal of Consumer Marketing*, *40(4),* 470-480.

Sparrow, B., Liu, J., & Wegner, D. M. (2011). Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips. *Science, 333(6043)*, 776-778.

Statista. Share of teenage individuals who have been bullied or trolled online in the United Kingdom (UK) as of January 2016, by platform 2016. Dostupné (30.8.2024) z: https://www-statista-com.zu.idm.oclc.org/statistics/547974/experience-of-online-bullying-and-trolling-on-social-media-by-teens-in-the-uk/.

Suler, J.R. (1999). To get what you need: healthy and pathological internet use. *CyberPsychology & Behavior, 2(5),* 385–394.

Suler, J.R. (2002). Identity Management in Cyberspace. *Journal of Applied Psychoanalytic Studies, 4(4),* 455-460.

Suler, J.R. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior, 7(3),* 321–326.

Šmahel, D., & Wright, M.F. (2014). *Meaning of online problematic situations for children: Results of qualitative cross-cultural investigation in nine European countries.* EU Kids Online, LSE.

Šmahel, D., Macháčková, H., Mascheroni, G., Dědková, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries. EU Kids Online.*

Taddicken, M. (2014). The "Privacy Paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19(2)*, 248–273.

ten Brummelhuis, L.L., ter Hoeven, C.L. & Toniolo-Barrios, M. (2021). Staying in the loop: Is constant connectivity to work good or bad for work performance?. Journal of Vocational Behavior, 128, 1-17.

Thornton, B., Faires, A., Robbins,R. & Rollins, E. (2014). "The Mere Presence of a Cell Phone May Be Distracting: Implications for Attention and Task Performance". *Social Psychology, 45(6),* 479– 88.

Townsend, D., Knoefel, F., & Goubran, R. (2011). *Privacy versus autonomy.* Engineering in medicine and biology society, EMBC (2011) annual international conference of the IEEE (4749– 4752).

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28(1)*, 20–36.

Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media+ Society, 1(2),* 1-11.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49(3–4)*, 190–198.

Venkatesh, V., Thong, J. Y., & Xin, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36(1),* 157–178.

Vogel, E., Rose, J., Roberts, L. & Eckles, K. (2014). Social Comparison, Social Media, and Self-Esteem. *Psychology of Popular Media Culture*. 3, 206-222.

Volkmer, S.A, Gaube, S., Raue, M,. & Lermer, E. (2023) Troll story: The dark tetrad and online trolling revisited with a glance at humor. *PLoS ONE, 18(3).*

Vuorikari, R., Kluzer, S. & Punie, Y. (2022). *Dig Comp 2.2: The Digital Competence Framework for Citizens-With new examples of knowledge, skills and attitudes*. Publications Office of the European Union, Luxembourg.

Wajcman, J., & Rose, E. (2011). Constant Connectivity: Rethinking Interruptions at Work. *Organization Studies*, *32*(7), 941-961.

Ward, A. F., Duke, K., Gneezy, A., & Bos, M. W. (2017). Brain Drain: The Mere Presence of One's Own Smartphone Reduces Available Cognitive Capacity. *Journal Of The Association For Consumer Research, 2(2),* 140-154

Westin, A. F. (1967). *Privacy and freedom.* New York: Atheneum.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2(4),* 338–346.

White, C.M., Gumerumm, M., Wood, S. & Hanoch, Y. (2017). Internet Safety and the Silver Surfer: The Relationship Between Gist Reasoning and Adults‘ Risky Online Behavior. *Journal of Behavioral Desicion Making, 30(4)*, 819-827.

Willis S.L., & Martin, M.. (2005). *Middle Adulthood : A Lifespan Perspective*. SAGE Publications, Inc.

Wohn, D. Y., Carr, C. T., & Hayes, R. A. (2016). How affective is a like? The effect of paralinguistic digital affordances on perceived social support. *Cyberpsychology, Behavior and Social Networking, 19*(9), 562–566

Wrzus, C., Hänel, M., Wagner, J., & Neyer, F. J. (2013). Social network changes and life events across the life span: A meta-analysis. *Psychological Bulletin, 139*, 53-80.

Xu, Y., Pace, S., Kim, J., Iachini, A., King, L.B., Dehart, D., … &Simone, M. (2022). Threats to Online Sureys: Recognizing, Detecting and Preventing Survey Bots, *Social Work Research, 46(4),* 343-350.

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies of Facebook. Information, *Communication & Society, 16(4),* 479–500.

Seznam tabulek

Seznam grafů

Seznam příloh

Přílohy

Příloha 1 – Využitý dotazník

- Do jaké míry Vám vadí sdílet fotografie na sociálních sítích? (OSOBNÍ)

Vůbec mi nevadí
Spíše mi nevadí
Ani vadí/ani nevadí
Spíše mi vadí
Velmi mi vadí

- Jak moc by Vám bylo nepříjemné, kdyby na Vás byli ostatní uživatelé na internetu vulgární a uráželi Vás (např. na sociálních sítích, v diskuzích apod.)? (OSOBNÍ)

Vůbec by mi to nebylo nepříjemné
Spíše by mi to nebylo nepříjemné
Ani nepříjemné/ani příjemné
Spíše by mi to bylo nepříjemné
Bylo by mi to velmi nepříjemné

- Míváte někdy pocit, že na internetu ztrácíte soukromí? (OSOBNÍ)

Nikdy
Výjimečně
Občas
Často
Neustále

- Je pro Vás důležité mít internetové účty zabezpečené silným heslem? (TECHNICKÁ)

Není to vůbec důležité
Spíše to není důležité
Ani důležité/ani nedůležité
Spíše je to důležité
Je to velmi důležité

- Otevíráte přílohy v e-mailu i od odesílatelů, které neznáte? (TECHNICKÁ)

Nikdy

Výjimečně

Občas

Často

Pokaždé

- Stalo se Vám v minulosti, že Vám kvůli napadení viry nefungoval počítač? (TECHNICKÁ)

Nestalo se nikdy

Už se mi to stalo jednou

Už se mi to stalo vícekrát

Děje se mi to neustále

- Myslíte, že Vaše aktivity na internetu mohou být sledovány vládou? (INSTITUCIONÁLNÍ)

Nesouhlasím

Spíše nesouhlasím

Ani souhlas/ani nesouhlas

Spíše souhlasím

Souhlasím

- Měl/a jste v minulosti pocit, že Váš telefon může být odposloucháván reklamními agenturami? (INSTITUCIONÁLNÍ)

Nikdy jsem tento pocit neměl/a

Už jsem měl/a pocit jednou

Už jsem měl/a pocit vícekrát

Mám tento pocit neustále

- Povolujete v internetových aplikacích sledování Vaší polohy? (INSTITUCIONÁLNÍ)

Nikdy

Výjimečně

Občas

Často

Vždy

- **Seřaďte dle závažnosti, jak vy osobně vnímáte následující tři „typy“ nebezpečí na internetu (1 - nejzávažnější, 3 - nejméně závažné):**

  - Technické: Zavirování počítače a ztráta dat v počítači
  - Osobní: Zneužití osobních údajů, narušení soukromí a osobní útoky či zesměšnění od dalších uživatelů na internetu
  - Institucionální: Sledování aktivit na internetu vládou či reklamními agenturami, odposlouchávání telefonů a sledování polohy

- Bojíte se, že Vám někdo může přes internet ukrást peníze z Vašeho bankovního účtu? (STRACH Z VNÍMANÉ HROZBY)

Vůbec se nebojím
Spíše se nebojím
Neutrální (bez názoru)
Spíše se bojím
Velmi se bojím

- Bojíte se, že na internetu může někdo zneužít Vaše osobní údaje (např. jméno, rodné číslo, adresu, telefonní číslo) ve svůj prospěch? (STRACH Z VNÍMANÉ HROZBY)

Vůbec se nebojím
Spíše se nebojím
Neutrální (bez názoru)
Spíše se bojím
Velmi se bojím

- Jak velká je podle Vás šance, že budete podvedeni nepoctivým prodejcem na internetu? (PRAVDĚPODOBNOST HROZBY)

Žádná šance
Spíše žádná šance
Neutrální (bez názoru)
Spíše je šance
Velká šance

- Jak velká je podle Vás šance, že by někdo mohl využít Vaše soukromé informace k zesměšnění, vydírání nebo dalšímu zneužití? (PRAVDĚPODOBNOST HROZBY)

Žádná šance

Spíše žádná šance

Neutrální (bez názoru)

Spíše je šance

Velká šance

- Věříte, že jste schopný/á se chránit před zavirováním počítače? (VNÍMANÉ SELF-EFFICACY)

Rozhodně nejsem schopný/á

Spíše nejsem schopný/á

Neutrální (bez názoru)

Spíše jsem schopný/á

Rozhodně jsem schopný/á

- Věříte, že se umíte vyhnout osobním útokům (vydírání, zesměšnění či šikana) od ostatních uživatelů na internetu? (VNÍMANÉ SELF-EFFICACY)

Rozhodně neumím

Spíše neumím

Neutrální (bez názoru)

Spíše umím

Rozhodně umím

- Věříte, že dokážete posoudit důvěryhodnost stránek, na kterých se běžně pohybujete (e-shopy, diskuze, sociální sítě apod.)? (VNÍMANÉ SELF-EFFICACY)

Rozhodně nedokáži

Spíše nedokáži

Neutrální (bez názoru)

Spíše dokáži

Rozhodně dokáži

- Jak zkušený/á se cítíte v následujících oblastech digitálních schopností a dovedností?

Pokyn: *Přečíst vždy i závorku (zhodnocení vlastních dovedností)*

	Vůbec nejsem zkušený/á	Spíše nejsem zkušený/á	Neutrální (bez názoru)	Spíše jsem zkušený/á	Velmi zkušený/á

Schopnost vyhledávat a třídit informace (posoudit jejich pravdivost a užitečnost)					
Komunikace (komunikace a spolupráce s lidmi a organizacemi, využívání e-mailu, chatů, sdílených dokumentů apod.)					
Práce s textem, počty a obrázky (příprava a úprava dokumentů – práce s textem, tabulkami, úprava obrázků apod.)					
Bezpečnost na internetu (schopnost chránit svůj počítač, osobní údaje a soukromí.)					
Využívat počítač ke zjednodušení práce (znalost technologických trendů a postupů)					

Sociodemografické a identifikační otázky (21 proměnných)

Jste?

1. Muž.
2. Žena.

Kolik je Vám let?

Jaké je Vaše nejvyšší ukončené vzdělání?

1. Základní nebo neukončené základní
2. Vyučen/a bez maturity
3. Středoškolské s maturitou
4. Vysokoškolské

Jste:

1. svobodný, svobodná,
2. ženatý, vdaná (příp. žijete v registrovaném partnerství),
3. rozvedený, rozvedená,
4. vdovec, vdova.

Uveďte, do které skupiny v současnosti spadáte:

1. Student, učeň
2. Důchodce
3. Nezaměstnaný
4. V domácnosti/na mateřské/rodičovské dovolené
5. Podnikatel se zaměstnanci
6. Samostatně činný bez zaměstnanců
7. Vyšší odborný pracovník nebo řídící pracovník (specialisté, manažeři)
8. Nižší odborný pracovník
9. Řadový úředník, provozní pracovník ve službách a prodeji
10. Dělník vyučený v oboru práce, řemeslník, opravář
11. Obsluha strojů, montér, nekvalifikovaný nebo pomocný dělník, zemědělec

FILTR: pouze ekonomicky aktivní a pracující

V jakém odvětví pracujete?

1. Zemědělství, myslivost, lesní hospodářství.
2. Rybolov, chov ryb.
3. Těžba nerostných surovin.
4. Zpracovatelský průmysl (potravinářský, textilní, papírenský, chemický průmysl, kovovýroba, vydavatelství, výroba strojů, přístrojů, vozidel, nábytku...).
5. Výroba a rozvod elektřiny, plynu a vody.
6. Stavebnictví.
7. Obchod; opravy motorových vozidel a spotřebního zboží.
8. Ubytování a stravování.
9. Doprava, skladování, pošty a telekomunikace.
10. Bankovnictví, pojišťovnictví, finanční zprostředkování.
11. Činnosti v oblasti nemovitostí; pronájem strojů a přístrojů; výzkum a vývoj; výpočetní technika; právní, účetní, architektonické a inženýrské poradenství; reklama; ochrana objektů...
12. Veřejná správa, obrana, povinné sociální zabezpečení.
13. Vzdělávání, školství.

14. Zdravotní a sociální péče, veterinární činnosti.
15. Ostatní veřejné, sociální a osobní služby (odpady, odpadní vody, čištění měst; rekreace, kultura, sport; odbory, profesní a podobné organizace; herny; čistírny; kadeřnictví...).
16. Domácnosti zaměstnávající personál.
17. Mezinárodní organizace a instituce.
18. JINÉ (vypsat)

OKRES. V jakém okrese bydlíte?

Kolik hodin denně průměrně trávíte na internetu ve svém volném čase (vyjma pracovní doby)? (otevřená na číslici)

Kolik hodin denně průměrně trávíte na internetu ve své pracovní době? (otevřená na číslici)