VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

INFORMOVANOST VEŘEJNOSTI O KYBERNETICKÝCH HROZBÁCH JAKO NÁSTROJ PREVENCE KRIMINALITY

Autor práce: Tomáš Provazník, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Tomáš Provazník, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Informovanost veřejnosti o kybernetických hrozbách jako nástroj prevence kriminality

Název bakalářské práce v anglickém jazyce: Public Awareness of Cyber Threats as a Tool for Crime Prevention

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): Listopad, 2025

Cíl bakalářské práce:
Cílem bakalářské práce je vymezit úroveň informovanosti veřejnosti o kybernetických hrozbách v České republice, identifikovat nejčastější nedostatky v osvětě a navrhnout efektivní preventivní opatření, která by mohla přispět ke snížení výskytu kybernetické kriminality.

Student: Tomáš Provazník, DiS.	15.11.2025	Provazník
Vedoucí práce: RNDr. Růžena Ferebauerová	15. 11. 2025	Ferebauerová

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	8. 11. 025	
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11.12.2025	
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20.12.2025	

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí(mu) bakalářské práce doktorce Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

PROVAZNÍK, T. *Informovanost veřejnosti o kybernetických hrozbách jako nástroj prevence kriminality: bakalářská práce.* Příbram: Vysoká škola evropských a regionálních studií, 2026. 71 s. Vedoucí práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kybernetické hrozby, phishing, malware, kyberšikana, informovanost veřejnosti, prevence kriminality

Bakalářská práce se zabývá tím, jak je veřejnost informována o kybernetických hrozbách a jakou roli hraje v prevenci trestné činnosti. S rostoucím používáním internetu a digitálních technologií se kybernetické hrozby stávají téměř běžnou součástí našeho každodenního života a mohou mít vážné následky jak pro jednotlivce, tak pro celou společnost. Často právě nedostatek informací o nebezpečí v online světě vede k tomu, že jsou uživatelé více zranitelní a kybernetickým zločincům se tak mnohé umožňuje.

V teoretické části práce je nejprve vymezeno, co znamená pojem kybernetická hrozba, jak se charakterizují nejčastější druhy kybernetických hrozeb např. phishing, malware nebo kyberšikana a co mohou tyto hrozby způsobit. Současně je zde pak kybernetická informovanost chápána jako prostředek prevence kriminality a je přiblížen základní rámec právních předpisů a strategií v oblasti kybernetické bezpečnosti v ČR. Cílem práce je zhodnotit, že kybernetická informovanost veřejnosti je jedním z důležitých činitelů v prevenci proti trestné činnosti.

ABSTRACT

PROVAZNÍK, T. *Public Awareness of Cyber Threats as a Tool for Crime Prevention: bachelor's thesis.* Příbram: College of European and Regional Studies, 2026. 71 p. Supervisor: RNDr. Růžena Ferebauerová.

Key words: cyber threats, phishing, malware, cyberbullying, public awareness, crime prevention

This bachelor's thesis examines how the public is informed about cyber threats and what role it plays in crime prevention. With the growing use of the internet and digital technologies, cyber threats are becoming an almost commonplace part of our daily lives and can have serious consequences for both individuals and society as a whole. Often, it is precisely the lack of information about the dangers of the online world that makes users more vulnerable and thus enables cybercriminals to act with impunity.

The theoretical section of the thesis first defines the concept of a cyber threat, describes the most common types of cyber threats—such as phishing, malware, and cyberbullying—and explains the potential consequences of these threats. At the same time, cyber awareness is understood here as a means of crime prevention, and the basic framework of legal regulations and strategies in the field of cybersecurity in the Czech Republic is outlined. The aim of this thesis is to demonstrate that public cyber awareness is one of the key factors in crime prevention.

Obsah

Úvod

Internet a digitální technologie dnes využívá většina obyvatel České republiky prakticky denně. Slouží ke komunikaci, práci, studiu i zábavě a staly se neoddělitelnou součástí moderní společnosti. Spolu s jejich rozvojem se však stále častěji objevují také rizika, která jsou s online prostředím spojena. Kybernetické hrozby již dávno nepředstavují problém pouze pro odborníky v oblasti informačních technologií, ale stále častěji se dotýkají běžných uživatelů internetu.

Z vlastní zkušenosti i z mediálních výstupů lze pozorovat, že mnoho lidí si rizika spojená s používáním internetu buď plně neuvědomuje, nebo jim nepřikládá dostatečnou pozornost. Často chybí základní povědomí o bezpečném chování v online prostředí a o možnostech, jak rozpoznat potenciální hrozby. Tento nedostatek informací může vést k tomu, že se uživatelé stávají snadným cílem kybernetické trestné činnosti, zejména v podobě internetových podvodů, zneužití osobních údajů či neoprávněných finančních transakcí.

Významnou roli v ochraně před kybernetickými hrozbami proto hraje informovanost veřejnosti. Lidé, kteří mají k dispozici srozumitelné a aktuální informace, jsou schopni lépe reagovat na rizikové situace a snížit pravděpodobnost, že se stanou obětí kybernetické kriminality. Prevence v oblasti kybernetické bezpečnosti tak nespočívá pouze v technických opatřeních, ale také v systematické osvětě a vzdělávání veřejnosti.

Cílem této bakalářské práce je proto zaměřit se na problematiku informovanosti veřejnosti o kybernetických hrozbách a posoudit její význam jako nástroje prevence kybernetické kriminality. Práce se snaží propojit teoretická východiska s praktickým pohledem běžných uživatelů internetu a prostřednictvím dotazníkového šetření zjistit, jaké jsou jejich znalosti, zkušenosti a postoje k bezpečnému chování v online prostředí.

1 Cíl a metodika bakalářské práce

Internet a digitální technologie dnes představují běžnou součást každodenního života většiny obyvatel České republiky. Jsou využívány nejen ke komunikaci a zábavě, ale také k práci, studiu či vyřizování úředních záležitostí. S rostoucí mírou digitalizace společnosti však dochází i k nárůstu rizik spojených s online prostředím, zejména v oblasti kybernetické bezpečnosti. Kybernetické hrozby se tak stále častěji netýkají pouze odborníků v oblasti informačních technologií, ale zasahují i běžné uživatele internetu.

Bakalářská práce je rozdělena na teoretickou a praktickou část. Teoretická část vychází z odborné literatury, právních předpisů a dostupných studií a zaměřuje se na vymezení pojmu kybernetická hrozba, její základní typologii a právní rámec kybernetické bezpečnosti v České republice. Cílem této části je vytvořit teoretický základ pro pochopení souvislostí mezi kybernetickými hrozbami a prevencí kriminality.

Praktická část práce je založena na dotazníkovém šetření, jehož cílem je zjistit, do jaké míry jsou respondenti schopni rozpoznat kybernetické hrozby v online prostředí a jaký mají přístup k bezpečnému chování na internetu. Získaná data budou statisticky vyhodnocena a využita k formulaci závěrů a doporučení směřujících ke zlepšení informovanosti veřejnosti v oblasti kybernetické bezpečnosti.

2 Kybernetické hrozby v kontextu současné společnosti

2.1 Digitalizace společnosti a vznik kybernetických hrozeb

Proces digitalizace společnosti je dlouhodobě spojován s nárůstem kybernetických hrozeb, neboť stále větší množství činností je realizováno prostřednictvím informačních a komunikačních technologií. Tento vývoj vytváří širší prostor pro útoky zaměřené na informační systémy, data i samotné uživatele. Odborné instituce zabývající se kybernetickou bezpečností dlouhodobě upozorňují na skutečnost, že s rostoucím využíváním digitálních technologií roste také sofistikovanost a četnost kybernetických útoků, a to jak vůči jednotlivcům, tak vůči organizacím.[1]

S rozvojem moderních technologií, jako jsou umělá inteligence, sociální sítě nebo další digitální služby, se také zvyšuje složitost a rozmanitost kybernetických hrozeb.[2] Velmi významná část těchto hrozeb souvisí především s využíváním informačních a komunikačních technologií, může být zaměřena na firmy, organizace i jednotlivce. Motivací útočníků je nejčastěji finanční zisk nebo snaha získat cenné informace, jako jsou osobní či jiné citlivé údaje, které mohou být následně zneužity například k vydírání.

Uživatelé, kteří nemají dostatek informací o možných kybernetických hrozbách, rizicích a bezpečnostních opatřeních, bývají vůči těmto útokům výrazně zranitelnější. Mezi nejčastější kybernetické hrozby patří útoky typu phishing, šíření škodlivého softwaru (malware) a další různé formy útoků v online prostředí. Tyto hrozby mohou také vést k úniku citlivých dat a finančním ztrátám.[3]

Vznik a šíření kybernetických hrozeb je tedy úzce spojeno s procesem digitalizace. S rostoucím počtem digitálních technologií a jejich využíváním roste i potřeba bezpečného chování v online prostředí a zvyšování informovanosti uživatelů o možných rizicích. Informovanost veřejnosti tak představuje jeden z důležitých

[1] BRESNAHAN, E. How Digital Transformation Impacts IT And Cyber Risk Programs [online]. CyberSaint Security, [cit. 4. 1. 2026]. Dostupné z: https://www.cybersaint.io/blog/managing-risk-in-digital-transformation

[2] BRESNAHAN, E. How Digital Transformation Impacts IT And Cyber Risk Programs [online]. CyberSaint Security, [cit. 4. 1. 2026]. Dostupné z: https://www.cybersaint.io/blog/managing-risk-in-digital-transformation

[3] KRÁLOVÁ, M. Kybernetické hrozby a jak se před nimi chránit [online]. CDC Data, 27. 3. 2023 [cit. 4. 1. 2026]. Dostupné z: https://www.cdc.cz/cs/kybernetricke-hrozby-a-jak-se-pred-nimi-chranit/

předpokladů pro omezení dopadů kybernetických hrozeb a posílení prevence kybernetické kriminality.[4]

2.2 Vymezení pojmu kybernetická hrozba

2.2.1 Odborná definice pojmu

Kybernetickou hrozbu lze obecně chápat jako faktor nebo situaci, která představuje riziko narušení fungování informačních systémů, ochrany dat nebo práv jednotlivců v digitálním prostředí. Nejde přitom pouze o již uskutečněné útoky, ale také o potenciální jednání, u něhož existuje reálná možnost vzniku negativních následků. Důležitým aspektem posuzování kybernetické hrozby je tedy samotná existence rizika, a to bez ohledu na to, zda již došlo k jeho faktické realizaci.[5][6]

2.2.2 Rozdíl mezi pojmy hrozba, riziko, útok

Podle Ministerstva vnitra České republiky se za hrozbu považuje: *„jakýkoliv fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností, čili rizikem) možného uplatnění této hrozby.“*[7]

Vlastní pojem hrozba je definován jako *„potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.“*[8]

Na obecný pojem hrozby úzce navazuje také pojem bezpečnostní hrozba. Tu můžeme chápat jako okolnost nebo faktor, který může směřovat ke vzniku nežádoucí události a způsobit poškození systému nebo jeho aktiv. Takové poškození se může projevit například zničením nebo změnou dat, jejich neoprávněným zpřístupněním nebo omezením dostupnosti poskytovaných služeb.[9]

---

[4] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA Threat Landscape 2025 [online]. 1. October 2025 [cit. 4. 1. 2026]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[5] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. s. 74. ISBN 978-80-88168-31-7.

[6] SAK, Petr. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. Petrklíč, 2018. s. 14. ISBN 978-80-7229-793-1.

[7] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. s. 74. ISBN 978-80-88168-31-7.

[8] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. s. 74. ISBN 978-80-88168-31-7.

[9] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. s. 74. ISBN 978-80-88168-31-7.

2.2.3 Kybernetické hrozby jako součást kybernetické kriminality

Kybernetické hrozby jsou v odborné literatuře nejčastěji spojovány s narušením fungování informací a informačních systémů. Může jít například o únik citlivých údajů, jejich neoprávněnou změnu nebo poškození, případně o situace, kdy dojde k omezení či úplnému výpadku dostupnosti služeb. Za kybernetickou hrozbu je možné považovat také neoprávněné nebo nelegitimní využívání informací. K tomu může docházet jak ze strany externích útočníků, tak i osob, které mají k systémům určitý přístup, avšak tento přístup využívají v rozporu s nastavenými pravidly.[10]

Část autorů zároveň upozorňuje na skutečnost, že nejde o zcela samostatný druh kriminality, ale spíše o běžnou trestnou činnost, která je páchána s využitím informačních a komunikačních technologií. V tomto smyslu lze kybernetické hrozby chápat jako určitý předstupeň nebo prostředek kybernetické kriminality, přičemž k samotné trestné činnosti dochází až v případě jejich skutečné realizace.[11]

2.3 Dopady kybernetických hrozeb na společnost

Dopady kybernetických hrozeb se neomezují pouze na technickou rovinu, ale významně zasahují také jednotlivce a celou společnost. V případě úspěšných útoků může docházet k přímým finančním ztrátám, zneužití osobních údajů nebo narušení soukromí obětí. Tyto následky často vyžadují další časové i finanční náklady spojené s obnovou účtů, zabezpečením dat či řešením vzniklých škod.[12]

Vedle ekonomických dopadů nelze opomenout ani negativní vliv na psychickou pohodu obětí. Kybernetické útoky mohou vyvolávat stres, pocity nejistoty či obavy z opakování podobné situace. Dlouhodobě se tak může snižovat důvěra veřejnosti v digitální prostředí a online služby, což má dopad nejen na jednotlivce, ale i na fungování digitální společnosti jako celku.[13]

Důsledky kybernetických hrozeb dopadají na společnost jako celek. Když se útoky často objevují v médiích nebo když lidé kolem nás přijdou o peníze či data, důvěra v digitální prostředí klesá. Lidé pak méně ochotně sdílejí osobní údaje, váhají používat

[10] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. s. 76-77. ISBN 978-80-88168-31-7.
[11] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 31. ISBN 978-80-88168-15-7.
[12] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Kybernetická bezpečnost, kybernetická kriminalita a AI [online]. 9. 4. 2025 [cit. 12. 1. 2026]. Dostupné z: https://www.kybersoutez.cz/finale2025/MV.pdf
[13] BADA, M. a JASON R. C. Nurse. The Social and Psychological Impact of Cyber-Attacks [online]. 29 9 2019 [cit. 12. 1. 2026]. Dostupné z: https://arxiv.org/pdf/1909.13256.pdf

online služby nebo se méně zapojují do digitální ekonomiky. To může zpomalovat technologický rozvoj a bránit tomu, aby společnost naplno využila výhody moderních technologií.[14]

Na tato rizika reaguje i česká legislativa. Ochranu osobních údajů upravuje zákon č. 110/2019 Sb. o zpracování osobních údajů, který navazuje na evropské nařízení GDPR. Stanovuje základní pravidla pro to, jak mohou být osobní údaje zpracovány, a zároveň chrání práva lidí v digitálním prostředí.

Zákon zdůrazňuje, že osobní údaje lze zpracovávat jen tehdy, když existuje právní důvod – například splnění zákonné povinnosti, výkon veřejné moci nebo ochrana oprávněného zájmu. Cílem je omezit rizika spojená s úniky a zneužíváním dat a posílit důvěru veřejnosti v to, že jejich údaje jsou v online světě v bezpečí.[15]

2.3.1 Komunikační sítě

Bezpečnost komunikačních sítí představuje důležitý prvek ochrany digitálního prostředí, neboť zajišťuje bezpečný přenos informací mezi jednotlivými systémy a uživateli. Odborné zdroje zdůrazňují význam technických a organizačních opatření, jako je segmentace sítí, řízení přístupů a využívání kryptografických prostředků, jejichž cílem je ochrana důvěrnosti, integrity a dostupnosti přenášených dat. Tyto požadavky jsou zároveň zakotveny v právní úpravě, která ukládá provozovatelům komunikačních sítí povinnost přijímat odpovídající bezpečnostní opatření.[16]

[14] DONNELLY, M. Social Impacts of Cyber Crime [online]. 2023 [cit. 12. 1. 2026]. Dostupné z: https://www.ebsco.com/research-starters/computer-science/social-impacts-cyber-crime

[15] *Zpracování osobních údajů: nový zákon o zpracování osobních údajů a další právní předpisy. GDPR : obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů : redakční uzávěrka 1.5.2019*. ÚZ : úplné znění. Ostrava: Sagit, [2019]. s. 4. ISBN 978-80-7488-353-8.

[16] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. s. 167-171. ISBN 978-80-7380-765-8.

3 Typologie kybernetických hrozeb ohrožujících veřejnost

Po vymezení samotného pojmu kybernetické hrozby a nastínění toho, jak mohou ovlivnit jednotlivce i celou společnost, je vhodné se zaměřit na konkrétní druhy rizik, se kterými se lidé na internetu setkávají. Tato kapitola představuje základní přehled vybraných kybernetických hrozeb, jež mohou být obzvlášť nebezpečné pro běžné uživatele. V jednotlivých podkapitolách je popsán jejich princip, nejčastější podoby i možné následky pro oběti. Cílem je přiblížit tato rizika srozumitelně a ukázat, proč je důležité věnovat jim pozornost v rámci prevence kyberkriminality.

3.1 Sociální inženýrství

Sociální inženýrství představuje soubor technik, jejichž cílem je ovlivnit nebo zmanipulovat člověka, aby útočník získal informace či přiměl poškozeného k jednání, do kterého by se za normálních okolností nepustil. Nejčastěji jde o využití lidské důvěry, nepozornosti nebo snahy vyhovět než o technické útoky na zabezpečení. Útočník vytváří situaci, která v oběti vzbudí dojem, že postupuje správně či bezpečně, a ta útočníkovi sama poskytne to, co potřebuje.

Základní myšlenka sociálního inženýrství vychází z toho, že člověk bývá slabším článkem jakéhokoliv bezpečnostního systému. Útočníci nejčastěji sáhnou po manipulaci, která je pro ně jednodušší než složité technické útoky. Tyto metody mohou mířit na jednotlivce i celé organizace a získané informace slouží k dalším, mnohem závažnějším formám kyberkriminality.[17]

Útočníci využívající principy sociálního inženýrství jsou označováni jako sociální inženýři. Jejich motivace může spočívat zejména ve snaze získat osobní údaje, neoprávněný přístup k systémům, obejít zavedené bezpečnostní postupy nebo jednoduše otestovat možnosti manipulace s uživateli.[18]

3.2 Phishing

Patří k nečastějším online podvodům a stojí hlavně na důvěře uživatele. V praxi to funguje tak, že se vydává za někoho důvěryhodného – například za banku, poskytovatele služeb nebo správce sociální sítě – snaží se člověka přimět, aby mu sám předal citlivé údaje. Nejčastěji jde o přihlašovací jména a hesla, PIN kódy nebo informace k platebním kartám.

[17] KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. s. 186. ISBN 978-80-88168-15-7
[18] ANDRAŠKO, J., MESARČÍK M., a SOKOL P. Právo kybernetickej bezpečnosti. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. ISBN 978-80-7160-632-1.

Typickým znakem phishingu je vytváření pocitu naléhavosti nebo hrozby. Útočník například tvrdí, že je účet zablokovaný, že je nutné okamžitě ověřit údaje, nebo že hrozí jeho zrušení. E-maily, které k tomu útočník používá, často vypadají na první pohled velmi věrohodně – jak obsahem, tak i graficky. Součástí zprávy většinou bývá odkaz na falešnou webovou stránku, která se snaží co nejvíce podobat originálu. I když může odkaz působit autenticky, jde o podvrh vytvořený jen proto, aby z oběti vylákal citlivé informace.

Phishing je úzce spojen se sociálním inženýrstvím, tedy s technikami psychologické manipulace, jejichž cílem je ovlivnit chování uživatele. Útočník spoléhá na nepozornost uživatele, strach nebo snahu rychle situaci vyřešit. Tyto faktory vedou k tomu, že oběť na podvod reaguje, aniž by si byla jistá, že jde o její pravost.[19] [20]

3.2.1 Spear phishing

Spear phishing představuje specifickou podobu phishingu, která se od běžných hromadných útoků liší tím, že je mířena na přesně vybraný cíl. Útočníci se zaměřují na konkrétní osobu, skupinu nebo organizaci a snaží se získat informace či data, která mají pro ně zvláštní hodnotu. Na rozdíl od klasického phishingu tedy nejde o náhodné rozesílání podvodných zpráv, ale o promyšlený a personalizovaný útok.[21]

3.2.2 Vishing

Vishing označuje podvodné telefonáty, při nichž se útočník snaží pomoci sociální manipulace získat od volaného citlivé údaje, například čísla účtu, přihlašovací informace nebo data k platebním kartám. Podvodníci při tom často předstírají identitu pracovníků bank či jiných důvěryhodných institucí, aby v oběti vzbudili dojem, že jde o legitimní hovor a snížili tak její podezření.[22]

3.2.3 Smishing

Smishing vychází ze stejných principů jako phishing nebo vishing, jen místo e-mailů či telefonátů využívá klasické SMS zprávy. Podvodné textové zprávy mají obvykle

[19] PETROWSKI, T. *Bezpečí na internetu: pro všechny*. Přeložil Tomáš KURKA. Tajemství. Liberec: Dialog, 2014. s. 43-45. ISBN 978-80-7424-066-9.
[20] KYBERNETICKÁ BEZPEČNOSŤ [online]. Bratislava: Ministerstvo školstva Slovenskej republiky, 2024 [cit. 18. 1. 2026]. Dostupné z: https://www.minedu.sk/data/files/13338_digiq_kyberneticka-bezpecnost_final-text-na-web.pdf
[21] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 264. ISBN 978-80-88168-15-7.
[22] KOŽÍŠEK, M., a PÍSECKÝ V. Bezpečně na internetu: průvodce chováním ve světě online. Grada Publishing a.s, 2016. ISBN 978-80-271-9074-4.

za cíl přimět uživatele k zaplacení určité částky – například zavoláním na drahou linku nebo odesláním speciální SMS.[23]

3.3 Důsledky phishingu pro oběti

Důsledky phishingu mohou být opravdu vážné. Pokud útočník získá citlivé údaje, může se dostat k bankovnímu účtu, zneužít platební kartu nebo dokonce ukrást identitu. Lidé tak mohou přijít o peníze nebo se potýkat s dalšími komplikacemi, které souvisejí se zneužitím jejich osobních dat.

Phishing nezpůsobuje jen finanční škody. Mnoho obětí popisuje i psychickou zátěž – stres, pocit selhání nebo ztrátu důvěry v online služeb a komunikaci. Tato zkušenost vede k větší opatrnosti na internetu, ale může také zanechat dlouhodobý pocit nejistoty a obavy, že se podobná situace může opakovat.[24]

3.4 Malware jako škodlivý software

Malware, tedy škodlivý software, představuje souhrnné označení pro programy nebo jejich části, jejichž účelem je narušit běžnou činnost počítačového systému, získat neoprávněný přístup k datům nebo způsobit jinou formu škody. Tyto programy mohou být využívány k celé řadě činností, například ke krádeži informací, sledování uživatele, narušení funkčnosti systému nebo k šíření dalších škodlivých kódů. Malware se může do zařízení dostat různými způsoby, nejčastěji prostřednictvím e-mailových příloh, podvodných odkazů, infikovaných webových stránek nebo stahování neověřeného obsahu z internetu.[25] Oproti phishingu, který je založen na zneužití důvěry uživatele, malware zpravidla spoléhá na to, že uživatel sám spustí nebo nainstaluje škodlivý program.

Z historického hlediska se škodlivý software vyvíjel spolu s rozvojem výpočetní techniky a internetu. Původně šlo často o jednoduché programy, jejichž cílem bylo spíše experimentování nebo demonstrace technických možností. Postupem času se však malware stal sofistikovaným nástrojem, který je dnes využíván především k páchání kybernetické kriminality, často s cílem finančního zisku.

[23] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 266. ISBN 978-80-88168-15-7.
[24] PETROWSKI, T. *Bezpečí na internetu: pro všechny*. Přeložil Tomáš KURKA. Tajemství. Liberec: Dialog, 2014. s. 43-45. ISBN 978-80-7424-066-9.
[25] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 204-205. ISBN 978-80-88168-15-7.

Současná odborná literatura rozlišuje několik základních druhů malwaru podle jeho funkce a způsobu působení. Mezi nejčastější patří například spyware, počítačové viry, trojské koně nebo ransomware. Jednotlivé typy se liší způsobem šíření i dopady na uživatele, avšak společným znakem je jejich negativní vliv na bezpečnost informačních systémů a ochranu dat.[26]

3.4.1 Spyware

Spyware je označení pro typ škodlivého softwaru, jehož cílem je shromažďovat informace o uživateli a jeho činnosti na počítači bez jeho vědomí nebo souhlasu. Získaná data mohou zahrnovat například informace o chování uživatele, navštívených webových stránkách nebo technické údaje o systému. Tyto informace jsou následně zpracovávány a v některých případech odesílány dále, například za účelem cílené reklamy nebo dalšího zneužití.

Spyware může být do systému nainstalován samostatně, ale často bývá součástí jiných programů, přičemž jeho přítomnost zůstává pro uživatele skrytá. Z tohoto důvodu představuje ochrana soukromí a bezpečnost osobních údajů významné riziko.[27]

3.4.2 Počítačové viry

Počítačové viry představují další druh škodlivého softwaru, které navazují na existující soubory nebo programy a k šíření využívá jejich spuštění. Virus se obvykle aktivuje v okamžiku, kdy uživatel otevře infikovaný soubor, a následně se může dále šířit v rámci systému nebo na další zařízení. Jejich cílem může být narušení funkčnosti systému, poškození či zničení dat nebo vytvoření prostoru pro další škodlivé aktivity. Počítačový virus může být v počítači přítomen, ale nemůže se aktivovat sám bez zásahu člověka.[28] [29]Dále může dojít i ke získání informací, které tvůrce počítačového viru vymáhává od uživatele.

3.4.3 Trojské koně

Trojské koně jsou další škodlivé programy, které se vydávají za legitimní nebo užitečný software, aby přesvědčily uživatele k jejich spuštění či instalaci. Po aktivaci útočník může v systému provádět skryté činnosti, například umožnit neoprávněný

[26] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 204-205. ISBN 978-80-88168-15-7.
[27] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 207. ISBN 978-80-88168-15-7.
[28] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 207-208. ISBN 978-80-88168-15-7.
[29] PANDĚ, J. Introduction to Cyber Security. Haldwani: Uttarakhand Open University, 2017. s. 19. ISBN 978-93-84813-96-3.

vzdálený přístup, narušit funkčnost systému nebo zneužít uložená data. Na rozdíl od počítačových virů se trojské koně samy nešíří a k jejich aktivaci zpravidla dochází poté, co uživatel program sám spustí.[30] [31]

3.5 Ransomware jako aktuální hrozba

Ransomware v současnosti patří mezi nejzávaznější a nejnebezpečnější formy kybernetických hrozeb, a to zejména kvůli svým přímým a často velmi závažným dopadům na uživatele i organizace.[32] Ransomware je dlouhodobě zmiňován jako aktuální bezpečnostní riziko v pravidelných hodnotících zprávách vydávaných českým NÚKIB i evropskou agenturou ENISA.[33] Tento typ škodlivého softwaru je zaměřen na omezení nebo úplné znemožnění přístupu k datům či k celému počítačovému systému.

Způsoby šíření ransomwaru jsou různé, mezi nejčastější patří podvodné e-mailové zprávy s přílohami nebo odkazy na škodlivé webové stránky nebo zneužití bezpečnostních slabin v operačních systémech a aplikacích. Útočníci často využívají techniky sociálního inženýrství jako u předešlých kybernetických hrozeb, aby zvýšili pravděpodobnost úspěchu útoku a přiměli uživatele k neuváženému jednání. Ransomware se tak neomezuje pouze na technickou stranu útoku, ale výrazně zasahuje i do oblasti lidského faktoru.

Aktuálnost ransomwaru je dána také jeho neustálým vývojem a přizpůsobováním se novým bezpečnostním opatřením. Moderní varianty ransomwaru jsou stále sofistikovanější, obtížněji odhalitelné a v některých případech cílí nejen na běžné uživatele, ale také na státní instituce, zdravotnická zařízení či kritickou infrastrukturu. V důsledku těchto útoků může docházet nejen k finančním ztrátám, ale také k narušení důvěry v digitálním prostředí a k ohrožení základních funkcí společnosti.[34]

3.5.1 Systém managementu bezpečnosti informací

Systém managementu bezpečnosti informací (ISMS) je dokumentovaný systém řízení informačních aktiv, jehož cílem je minimalizace rizik prostřednictvím identifikace

[30] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 208-209. ISBN 978-80-88168-15-7.
[31] MOJMÍR, Král. *Bezpečný internet: Chraňte sebe i svůj počítač*. Grada Publishing a.s, 2015. s. 86. ISBN 978-80-247-9821-9.
[32] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 221. ISBN 978-80-88168-15-7.
[33] KUDRLOVÁ, K., PALOUŠOVÁ, V. a VLACH, J. *Kyberkriminalita z pohledu justiční praxe a každodenních uživatelů*. Vydání: první. Studie. Praha: Institut pro kriminologii a sociální prevenci, 2023. s. 67. ISBN 978-80-7338-204-9.
[34] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 221. ISBN 978-80-88168-15-7.

chráněných aktiv, řízení bezpečnostních rizik a zavádění odpovídajících bezpečnostních opatření proti hrozbám, jako je malware či ransomware.[35]

3.6 Kyberšikana a další sociálně patologické jevy v online prostředí

Kyberšikana představuje specifickou formu šikany, která se odehrává prostřednictvím informačních a komunikačních technologií, zejména internetu, sociálních sítí a mobilních zařízení.[36] Jejím cílem je úmyslně ubližovat jiné osobě, ponižovat ji, zesměšňovat nebo jí jiným způsobem způsobovat psychickou újmu. Na rozdíl od klasické šikany není kyberšikana omezena fyzickým prostorem ani časem a může probíhat nepřetržitě, což výrazně zvyšuje její dopad na oběť. Podle těchto znaků je kyberšikana výrazně horší než klasická šikana.

Charakteristickým znakem kyberšikany je také pocit anonymity útočníka, který může vést k menší sebekontrole a k intenzivnějším projevům agrese. Je složitější získat identifikaci útočníka a zároveň se zvyšuje pocit bezmoci na straně oběti. Kyberšikana je navíc obtížně zjistitelná, protože její projevy nemusí být na první pohled viditelné a oběť nemusí vykazovat zjevné vnější známky šikany.

Kyberšikana může mít různé podoby a projevy, které se liší použitými prostředky i intenzitou útoků. Mezi nejčastější formy patří opakované urážení, zesměšňování, vyhrožování nebo zastrašování prostřednictvím sociálních sítí, e-mailů, chatovacích aplikací či SMS zpráv. Útočníci mohou zneužívat osobní údaje oběti, vytvářet falešné profily nebo neoprávněně zasahovat do jejích online účtů.

Další formou kyberšikany je pořizování a následné zveřejňování fotografií, videí či zvukových záznamů bez souhlasu oběti, často s cílem ji zesměšnit nebo poškodit její pověst. Zvlášť závažným projevem je zveřejňování záznamů fyzického napadení či psychického týrání, které jsou následně šířeny v online prostředí. Tyto materiály mohou být opakovaně sdíleny, čímž dochází k prodlužování a prohlubování negativních dopadů na oběť.

Kyberšikana má dlouhou trvalost, neboť jednou zveřejněný obsah může v internetovém prostředí zůstávat dostupný dlouhodobě a oběť se s ním může opakovaně

[35] DRASTICH, M. *Systém managementu bezpečnosti informací*. Grada Publishing a.s, 2011. s. 18-20. ISBN 978-80-247-7616-3.
[36] ČERNÁ A., (ED.), LENKA, D., HANA, M., ANNA, Š. a DAVID, Š. Kyberšikana: Průvodce novým fenoménem. Grada Publishing a.s, 2013. ISBN 978-80-247-8846-3.

setkávat. To může vést k dlouhodobým psychickým následkům, jako jsou úzkosti, stres nebo sociální izolace.[37] [38]

3.6.1 Kybergrooming

Na kyberšikanu navazuje kybergrooming, který cíleně navazuje dlouhodobé udržování kontaktu s dítětem v online prostředí za účelem sexuálního zneužití. Útočník si postupně buduje důvěru oběti, často prostřednictvím empatie, dárků nebo lichotek, a snaží se komunikaci směřovat k sexuálnímu obsahu. V pozdější fázi může usilovat o osobní setkání nebo využívat vydírání hrozbou zveřejnění získaných materiálů.[39]

3.6.2 Dopady na oběti

Kyberšikana může mít na oběti významné negativní dopady, zejména v oblasti psychického zdraví a sociálních vztahů. Často se u nich objevují pocity úzkosti, stresu, sníženého sebevědomí nebo obavy z dalšího napadání. Tyto problémy mohou vést ke stažení se z kolektivu, narušení vztahů s vrstevníky a omezení běžné komunikace v online prostředí. Dlouhodobé vystavení kyberšikaně se může projevit také zhoršením školních výsledků, poruchami spánku nebo celkovým snížením psychické pohody oběti.[40]

3.7 Další vybrané kybernetické hrozby

Jedna z vybraných kybernetických hrozeb jsou podvodné nabídky, které představují častou formu internetových podvodů. Cílí na získání finančních prostředků nebo osobních údajů uživatelů. Tyto nabídky jsou zpravidla šířeny hromadně prostřednictvím e-mailů, sociálních sítí, inzertních portálů nebo různých komunikačních aplikací a často si z toho útočník odnese rychlý zisk, výhodné pracovní příležitosti nebo mimořádně nízké úroky při půjčkách. Jejich cílem je vzbudit důvěru a přimět uživatele k rychlé reakci bez dostatečného ověření pravdivosti nabídky.

---

[37] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 309-311. ISBN 978-80-88168-15-7.
[38] ŠVESTKOVÁ, R., SOLDÁN L. a ŘEHKA M. *Kyberšikana* [online]. České Budějovice: ZSF JU, 2019. 7. kapitola. ISBN 978-80-7394-752-1. Dostupné z: https://publi.cz/books/5555/index.html#7-kyberneticka-sikana
[39] VLACH, J., KUDRLOVÁ, K. a PALOUŠOVÁ, V. *Kyberkriminalita v kriminologické perspektivě*. Vydání: první. Studie. Praha: Institut pro kriminologii a sociální prevenci, 2020. s. 92. ISBN 978-80-7338-189-9.
[40] BEZPEČNOST A OCHRANA ZDRAVÍ ŠKOLNÍ MLÁDEŽE PŘI POUŽÍVÁNÍ DIGITÁLNÍCH TECHNOLOGIÍ — Kyberšikana a její dopady [online]. [s.l.]: Výzkumný ústav bezpečnosti práce, v. v. i., [n.d.] [cit. 15. 1. 2026]. Dostupné z: https://skoly.vubp.cz/soubory/boz-skolni-mladeze-pri-pouzivani-digitalnich-technologii-kybersikana-a-jeji-dopady.pdf

Na podvodné nabídky často navazují podvodné webové stránky, které mají působit důvěryhodným dojmem a napodobují vzhled oficiálních e-shopů, bankovních institucí nebo známých firem. Útočníci využívají sociální inženýrství a nepozornost uživatelů, aby je přiměli k zadání citlivých údajů, jako jsou přihlašovací údaje, kontaktní informace nebo platební data. Tyto informace pak mohou být dále zneužity k neoprávněnému přístupu k účtům nebo k dalším podvodným aktivitám.

Typickým znakem těchto útoků je snaha vyvolat pocit naléhavosti, například omezenou časovou platností nabídky nebo hrozbou zablokování účtu. V důsledku toho uživatelé často jednají rychle a nevěnují dostatečnou pozornost ověřování zdroje, což zvyšuje úspěšnost těchto forem kyberkriminality. Například nabídka nového telefonu za výrazně nižší cenu než obvykle, zadají se platební údaje, kontaktní informace. Oběť potvrdí platbu, která se odešle a telefon, který si zaplatil nikdy nepřijde a útočník získá potřebné informace k páchání dalším trestným činům.[41]

Další vybraná kybernetická hrozba je krádež identity. Kybernetický útok, při němž dochází k neoprávněnému získání a následnému zneužití osobních nebo přístupových údajů jiné osoby. Útočník tímto způsobem získává kontrolu nad virtuální identitou oběti, například nad jejími uživatelskými účty, e-mailovou schránkou nebo dalšími online službami. Motivem takového jednání bývá opět finanční zisk, získání dalších citlivých informací nebo usnadnění dalších podvodných aktivit.

Existuje mnoho způsobů, jak může k odcizení identity dojít. Mezi nejčastější patří prolomení přístupových údajů, podvodné vylákání informací prostřednictvím už zmíněného phishingu nebo instalace škodlivého softwaru do zařízení oběti. Po získání identity může útočník vystupovat jménem napadené osoby, komunikovat s dalšími uživateli nebo zneužívat důvěru jejího okolí.

Odcizená identita bývá následně využívána například k rozesílání podvodných zpráv, provádění phishingových či malwarových útoků, získávání neveřejných informací nebo k neoprávněnému přístupu k dalším službám. Vzhledem k provázanosti online účtů může mít zneužití jedné identity za následek kompromitaci celé řady dalších účtů a systémů.[42]

[41] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 240-242. ISBN 978-80-88168-15-7.
[42] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 318-319. ISBN 978-80-88168-15-7.

4 Informovanost veřejnosti o kybernetických hrozbách

4.1 Pojem informovanost veřejnosti

Informovanost se chápe jako míra znalostí a porozumění informacím, které má jednotlivec nebo společnost k dispozici a které je schopen smysluplně využívat. Nejde přitom pouze o samotné množství informací, ale především o jejich správné pochopení, interpretaci a zasazení do širších souvislostí. V dnešní moderní společnosti je informovanost spojená s fungováním složitých systémů, v nichž informace přispívají k organizovanosti, stabilitě a orientaci jednotlivců nebo firem ve stále komplexnějším prostředí na internetu.

4.1.1 Rozdíl mezi informovaností a digitální gramotností

Informovanost nelze spojit s digitální gramotností, ačkoliv spolu trochu souvisejí. Digitální gramotnost se zaměřuje hlavně na schopnost uživatelů technicky ovládat digitální zdroje, pracování s technologiemi nebo využívání digitálních služeb, například Google Docs, e-shopy, bankovnictví nebo umělá inteligence. Informovanost zahrnuje schopnost informace kriticky hodnotit, rozlišovat jejich důvěryhodnost, chápat jejich význam a důsledky. Člověk může být technicky zdatný, ale přesto nedostatečně informovaný, pokud není schopen rozpoznat rizika, manipulaci či dezinformace.

4.2 Význam informovanosti pro bezpečné chování na internetu

Dostatečná informovanost veřejnosti hraje klíčovou roli v oblasti bezpečného chování, zejména v digitálním a online prostředí. Internet jako komplexní a dynamicky se vyvíjející systém nabízí nejen široké možnosti komunikace a sdílení informací, ale zároveň i prostor pro různé formy zneužití. Informovaný jedinec je schopen lépe porozumět fungování tohoto prostředí, rozpoznat potenciální hrozby a přizpůsobit své chování tak, aby minimalizoval rizika.

Informovanost tak přispívá k prevenci nebezpečných situací, protože umožňuje včas identifikovat problematické jevy, pochopit jejich mechanismy a reagovat na ně adekvátním způsobem. Zároveň posiluje schopnost jednotlivců rozhodovat se odpovědně a uvědoměle, což je zásadní nejen pro jejich vlastní bezpečí, ale i pro stabilitu a bezpečnost společnosti jako celku.[43]

[43] GŘIVNA, T. a POLČÁK, R. *Kyberkriminalita a právo*. 2008. s. 12-15. ISBN 978-80-903786-7-4.

4.3 Úroveň informovanosti veřejnosti

Úroveň informovanosti veřejnosti v oblasti kybernetických hrozeb je v současné době považována za jeden z klíčových faktorů ovlivňujících bezpečné chování uživatelů na internetu. Většina odborných dokumentů upozorňuje na skutečnost, že s rostoucím využíváním digitálních technologií a internetu se zvyšuje také vystavení veřejnosti různým formám kybernetických rizik, které byly již zmíněny. Důležité je porozumět povaze hrozeb, rozpoznat jejich projevy a přizpůsobit jim své chování.

Z hlediska evropského přístupu ke kybernetické bezpečnosti je informovanost veřejnosti vnímána jako nedílná součást preventivních opatření. Zvyšování povědomí o kybernetických hrozbách je považováno za nezbytný předpoklad pro posilování odolnosti společnosti vůči kybernetickým útokům a pro podporu odpovědného chování uživatelů. Jde o dlouhodobý proces, který neustále doplňuje opatření v oblasti kybernetické bezpečnosti.[44]

Výrazné rozdíly existují mezi jednotlivými skupinami obyvatel, zejména v závislosti na věku, vzdělání, profesním zaměření a míře každodenního využívání digitálních technologií. Informovanější bývají zpravidla osoby, které se s informačními technologiemi setkávají v rámci své profese nebo disponují vyšší úrovní digitálních dovedností. Naopak některé skupiny uživatelů mohou být vůči kybernetickým hrozbám zranitelnější, zejména z důvodu nedostatku zkušeností nebo podcenění rizik na internetu.

Výsledky sociologických šetření z českého prostředí ukazují, že ačkoli si značná část veřejnosti existenci kybernetických hrozeb uvědomuje, mnozí uživatelé se stále domnívají, že se jich tato rizika osobně netýkají, ale může kdykoliv riziko nastat o kterém nemusíme ani vědět. Tento rozpor mezi obecnou znalostí hrozeb a vlastním pocitem ohrožení může vést k rizikovému chování, například k nedostatečnému zabezpečení uživatelských účtů nebo k neopatrnému nakládání s osobními údaji.[45]

Dále je informovanost ovlivňována řadou vzájemně propojených faktorů. Mezi nejvýznamnější patří úroveň vzdělání, přístup k relevantním a srozumitelným informacím, mediální prostředí, osobní zkušenosti s kybernetickými incidenty a míra

[44] SARRI, A. a ARCUS, R. *Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies*. 2021. s. 6-8. ISBN 978-92-9204-544-9.
[45] IPSOS. Češi a kybernetické hrozby [online]. 18. 7. 2024 [cit. 21. 1. 2026]. Dostupné z: https://www.ipsos.com/cs-z/cesi-kybernetricke-hrozby

podpory osvěty ze strany státu a veřejných institucí. Nejdůležitější je způsob prezentace informací, například jejich forma, jazyk a přizpůsobení konkrétním cílovým skupinám.

Odborné studie poukazují na to, že efektivní zvyšování informovanosti vyžaduje systematický a cílený přístup. Mezi osvědčené nástroje patří využívání oficiálních vládních webových stránek, informačních kampaní, edukačních materiálů či interaktivních prvků, jako jsou návody, videa nebo online testy. Tyto aktivity přispívají nejen ke zvyšování znalostí, ale také k posilování schopnosti uživatelů rozpoznat rizikové situace.[46]

4.4 Zdroje informací o kybernetické bezpečnosti

4.4.1 Státní instituce

Podle informací zveřejněných Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) státní instituce pravidelně zveřejňují informační a metodické materiály zaměřené na prevenci kybernetických hrozeb. Tyto zdroje zahrnují podpůrné materiály vysvětlující bezpečnostní opatření a aktuální přehledy rizik, jejichž cílem je zvýšit povědomí veřejnosti a podpořit bezpečné chování v digitálním prostředí.[47]

4.4.2 Média a online zdroje

Média a různé online platformy také hrají důležitou roli v šíření povědomí o kybernetické bezpečnosti. Sociální média, blogy, podcasty nebo specializované portály nabízí aktuální informace o nejnovějších hrozbách, typech útoků a doporučených opatřeních. Běžně se využívají online zdroje, které mohou pomoci uživatelům nejen lépe porozumět bezpečnostním rizikům, ale také osvojit si praktické dovednosti, jako je rozpoznání phishingových útoků nebo správné nastavení ochrany osobních údajů.[48]

[46] RAMA, P. a M. KEEVY. Public cybersecurity awareness good practices on government-led websites [online]. *International Journal of Research in Business and Social Science*, 2023, roč. 12, č. 7, s. 94–104 [cit. 21. 1. 2026]. Dostupné z: https://www.researchgate.net/publication/375096855_Public_cybersecurity_awareness_good_practices_on_government-led_websites

[47] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). Kybernetická bezpečnost v ČR [online]. [cit. 21. 1. 2026]. Dostupné z: https://portal.nukib.gov.cz/informacni-servis/kyberneticka-bezpecnost-v-cr

[48] ANAZHI, A. H. I. a M. A. Osman. Cyber Security Awareness on Social Media: Knowledge Sharing Among Orang Asli Students [online]. *Journal of Information Security*, 2023, roč. 14, č. 4, s. 211–220 [cit. 21. 1. 2026]. Dostupné z: https://www.researchgate.net/publication/391495892_Cyber_Security_Awareness_on_Social_Media_Knowledge_Sharing_Among_Orang_Asli_Students

4.4.3 Školy a vzdělávací programy

Vzdělávací instituce hrají důležitou roli při budování dlouhodobé kybernetické gramotnosti a bezpečného chování. Školy a univerzity začleňují témata kybernetické bezpečnosti do výuky nejen jako technické dovednosti, ale i jako součást širší digitální gramotnosti, čímž pomáhají studentům lépe porozumět rizikům a prevenci v prostředí informačních technologií. Výukové aktivity vedou k lepší připravenosti žáků a studentům čelit reálným kybernetickým hrozbám a zvyšují.[49]

[49] Národní úřad pro kybernetickou a informační bezpečnost. Školy [online]. Národní úřad pro kybernetickou a informační bezpečnost, [bez data publikování] [cit. 21. 1. 2026]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/

5 Prevence kriminality

5.1 Vymezení pojmu prevence kriminality

Prevence kriminality je soubor opatření a strategií, jehož cílem je snižovat riziko vzniku trestné činnosti a omezovat její dopady ještě před tím, než k samotnému protiprávnímu jednání dojde. Nezaměřuje se pouze na pachatele, ale vychází z širšího pohledu na společenské, ekonomické a další faktory, které mohou ke kriminalitě přispívat. Důraz je dáván zejména na identifikaci rizikových podmínek na globální, národní, lokální i individuální úrovni, jelikož právě jejich kombinace může vytvářet prostředí příznivé pro vznik kriminality.

Součástí prevence kriminality je také systematická práce s ohroženými skupinami obyvatel a územími, kde se rizikové faktory hromadí. Umožňuje cíleně navrhovat preventivní programy a opatření, které jsou dlouhodobě považovány za efektivnější a ekonomicky výhodnější. Dále poukazuje na příčiny a okolnosti, které vedou k trestné činnosti.[50]

5.2 Druhy prevence kriminality

V kriminologické teorii se prevence kriminality tradičně rozlišuje na primární, sekundární a terciární. Toto členění není v mezinárodních dokumentech vždy explicitně pojmenováno, avšak je obsahově přítomno prostřednictvím práce s rizikovými faktory a cílovými skupinami prevence.

Primární prevence se soustřeďuje na celou společnost a jejím cílem je odstraňování obecných rizikových faktorů, například prostřednictvím zlepšování sociálních podmínek a vzdělávání. Tato úroveň prevence se snaží předcházet vzniku kriminality ještě před tím, než se objeví samotná konkrétní kriminalita.

Sekundární prevence směřuje na skupiny nebo jednotlivce, u kterých již existuje zvýšené riziko páchání trestné činnosti. Navazují na to zmíněné rizikové faktory, například s rodinným prostředím, školním neúspěchem nebo problematickými vrstevnickými vztahy. Cílem je včas zasáhnout a zabránit protiprávnímu jednání.

[50] SHAW, M. *Handbook on the Crime Prevention Guidelines: Making Them Work*. Criminal Justice Handbook, 2010. s. 9-13. ISBN 978-92-1-130300-1.

Terciární prevence se orientuje na osoby, u nichž již k trestné činnosti došlo, a jejím hlavním smyslem je zabránit recidivě. Zahrnuje především resocializační a reintegrační opatření, která mají snížit pravděpodobnost opakovaného páchání trestné činnosti a zároveň omezit další negativní dopady kriminality na jednotlivce i společnost.[51]

5.3 Prevence kriminality v oblasti kyberprostoru

Prevence kriminality v kyberprostoru je soubor opatření a strategií, které mají za cíl bránit vzniku a šíření trestné činnosti v digitálním prostředí a zmenšit škody způsobené kybernetickými útoky. Kybernetická bezpečnost je v tomto kontextu chápána jako složitý systém technických, organizačních i vzdělávacích nástrojů, které směřují k identifikaci, hodnocení a zmírňování kybernetických rizik a zároveň ke zvětšení důvěry uživatelů na internetu. Mezi nejdůležitější faktory patří osvěta veřejnosti o rizicích, zvýšení digitální gramotnosti, aktivní role státních institucí při poskytování informací a realizace preventivních kampaní a materiálů.[52]

Dále odborné studie upozorňují, že účinná prevence kybernetické kriminality nemůže navazovat na obecná bezpečnostní opatření, ale musí dostatečně porozumět samotné skutečnosti. Pro efektivní prevenci je nezbytné znát nejen rozsah škod způsobených kybernetickou kriminalitou, ale i to, kdo jsou pachatelé a oběti a jaké typy škod vznikají, protože právě na základě těchto informací je možné přímo plánovat preventivní strategii a opatření.[53]

5.4 Význam informovanosti v prevenci kybernetické kriminality

Informovanost veřejnosti je v oblasti kybernetické kriminality považována za jeden ze základních nástrojů primární prevence. Jak už bylo zmíněno, řada kybernetických útoků je založena na zneužití lidského faktoru, zejména nedostatku znalostí, nepozornosti nebo podcenění rizik. Zvyšování povědomí o kybernetických hrozbách je proto důležité, aby uživatelé v digitálním prostředí dokázali rozpoznat nebezpečné situace a vyhnout se jednání, které by mohlo dojít až k bezpečnostnímu incidentu.

---

[51] SHAW, M. *Handbook on the Crime Prevention Guidelines: Making Them Work*. Criminal Justice Handbook, 2010. s. 13-28. ISBN 978-92-1-130300-1.

[52] PREVENCE KRIMINALITY. *Kybernetická kriminalita – prevence kriminality* [online]. Prevence kriminality – Ministerstvo vnitra ČR, 2026. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/

[53] INSTITUT PRO KRIMINOLOGII A SOCIÁLNÍ PREVENCI V PRAZE. *Škody působené kybernetickou kriminalitou.* Praha: IKSP, 2019. s. 13-15. ISBN 978-80-7338-175-2

Sleduje se, jak je dobrá osvěta bezpečnostních návyků, jako je například obezřetné zacházení s elektronickou poštou, používání silných hesel, pravidelná aktualizace softwaru nebo ochrana osobních údajů. Pokud jsou tyto informace poskytovány systematicky a srozumitelně, mohou významně snížit pravděpodobnost úspěšných útoků, zejména těch, které využívají principy sociálního inženýrství, které bylo zmíněno v minulých kapitolách.

Význam informovanosti se odráží také ve vlivu na chování uživatelů v online prostředí. Účinné programy pro zvýšení povědomí se zaměřuje hlavně na poskytování informací i na posilování odpovědnosti uživatelů za vlastní bezpečnost. Cílem je, aby se bezpečné postupy staly běžnou součástí každodenní práce s digitálními technologiemi.

Také je nutné upozornit na limity informovanosti jako samostatného preventivního nástroje. Osvěta sama o sobě nemůže zajistit úplnou ochranu před kybernetickou kriminalitou, pokud není doplněna technickými a organizačními opatřeními, které musí být dodržena, například šifrování, firewally nebo vícefaktorové ověřování. V praxi mohou uživatelé selhat i přes základní znalosti, například pod tlakem času nebo v důsledku složitosti bezpečnostních mechanismů. Z tohoto důvodu je informovanost nejúčinnější tehdy, je-li součástí komplexního přístupu k prevenci, který kombinuje vzdělávání, technická řešení a jasně nastavená pravidla.[54]

5.5 Role institucí v prevenci kybernetických hrozeb

5.5.1 Role státu a veřejné správy

Stát a orgány veřejné správy hrají v prevenci kybernetických hrozeb klíčovou roli především prostřednictvím tvorby a uplatňování právního rámce, který upravuje chování subjektů v kyberprostoru. Prevence je zde realizována zejména formou legislativních opatření, vymezením trestněprávní odpovědnosti a stanovením povinností poskytovatelů služeb informační společnosti. Významnou roli má také zapojení státu do mezinárodní spolupráce a harmonizace právních předpisů na úrovni Evropské unie, což přispívá ke sjednocení preventivních přístupů a k efektivnějšímu potírání kybernetické kriminality.[55]

[54] SARRI, A. a ARCUS, R. Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies. 2021. s. 8-15. ISBN 978-92-9204-544-9.
[55] KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. S. 85-101; 331-338 ISBN 978-80-88168-15-7

5.5.2 Policie ČR

Policie České republiky se podílí na prevenci kybernetických hrozeb hlavně prostřednictvím odhalování a vyšetřování kybernetické kriminality. Systematické vyšetřování kybernetických trestných činů, specializace policejních útvarů a zvyšování odborné úrovně kriminalistických metod přispívají ke snižování latentní kriminality a působí odstrašujícím efektem na potenciální pachatele. Preventivní význam má rovněž spolupráce Policie ČR s dalšími státními orgány a subjekty při sdílení informací a zvyšování povědomí o aktuálních hrozbách.[56]

5.5.3 Neziskové a vzdělávací organizace

Významnou roli v prevenci kybernetických hrozeb sehrávají také neziskové a vzdělávací organizace, které se zaměřují především na osvětu, vzdělávání a zvyšování informovanosti uživatelů. Tyto subjekty se podílejí na realizaci vzdělávacích programů, bezpečnostních kampaní a projektů zaměřených na zvyšování digitální gramotnosti. Jejich činnost přispívá k posilování schopnosti jednotlivců rozpoznat rizikové situace v online prostředí a přijímat preventivní opatření, čímž se snižuje jejich zranitelnost vůči kybernetickým útokům.[57]

[56] KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. S. 401-417. ISBN 978-80-88168-15-7
[57] KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. S. 379-397. ISBN 978-80-88168-15-7

6 Právní a strategický rámec kybernetické bezpečnosti

6.1 Právní úprava kybernetické bezpečnosti v České republice

Zákon č. 264/2024 Sb., o kybernetické bezpečnosti, představuje základní právní rámec ochrany kybernetického prostoru v České republice. Jeho cílem je vymezit práva a povinnosti orgánů veřejné moci, provozovatelů informačních a komunikačních systémů a dalších subjektů v oblasti zajišťování kybernetické bezpečnosti a předcházení kybernetickým bezpečnostním incidentům.

Právní úprava se zaměřuje zejména na ochranu informačních systémů kritické informační infrastruktury, významných informačních systémů a komunikačních systémů, jejichž narušení by mohlo mít závažný dopad na fungování státu nebo poskytování základních služeb.[58]

Zákon stanovuje povinným osobám přijímat technická a organizační bezpečnostní opatření, mezi která patří například ochrana integrity a dostupnosti informací, řízení přístupových opatření, detekce kybernetických bezpečnostních událostí a zajištění evidence incidentů. Další součástí těchto povinností je identifikovat kybernetickou bezpečnostní událost a hlásit ji příslušnému orgánu, především Národnímu úřadu pro kybernetickou a informační bezpečnost.

Význam právní úpravy záleží na posílení preventivního působení státu v oblasti kybernetické bezpečnosti. Zákon vytváří podmínky pro systematickou ochranu veřejných i soukromých informačních systémů, omezení dopadů kybernetických incidentů a zvýšení celkové odolnosti společnosti vůči kybernetickým hrozbám. Právní regulace plní důležitou preventivní funkci zaměřenou na ochranu veřejnosti a zachování důvěry v digitálním prostředí.[59]

6.2 Strategické dokumenty v oblasti kybernetické bezpečnosti

Národní strategie kybernetické bezpečnosti České republiky představuje hlavní koncepční rámec, podle kterého stát plánuje, koordinuje a řídí opatření zaměřená na prevenci kybernetických hrozeb. Tento dokument definuje základní priority, které odrážejí současné bezpečnostní prostředí, jako je důraz na posílení důvěry v digitální

[58] ČESKO. Zákon č. 264/2024 Sb., o kybernetické bezpečnosti. Sbírka zákonů České republiky [online]. 2025, částka 264. [cit. 2025-02-22]. Dostupné z: https://www.e-sbirka.cz/sb/2025/264?zalozka=text.
[59] ČESKO. Zákon č. 264/2024 Sb., o kybernetické bezpečnosti. Sbírka zákonů České republiky [online]. 2025, částka 264. [cit. 2025-02-22]. Dostupné z: https://www.e-sbirka.cz/sb/2025/264?zalozka=text.

prostor, budování odolné společnosti či rozvoj spolehlivých aliančních vztahů. Strategie vyzdvihuje potřebu celonárodního přístupu, jehož součástí je sdílení informací, koordinace mezi institucemi a rozvoj kapacit veřejné správy a dalších klíčových aktérů v oblasti bezpečnosti. Tímto uceleným přístupem se česká kybernetická politika snaží uspět v dynamickém prostředí, kde se hrozby neustále mění a vyžadují rychlé reakce a flexibilní strategické plánování.

K doplnění institucionálního rámce strategie se využívají také další koncepční dokumenty, které rozpracovávají jednotlivé části národních cílů do konkrétních opatření. Typicky jde o akční plány k Národní strategii, jež stanovují implementační kroky, odpovědnosti jednotlivých orgánů a časový harmonogram plnění strategických záměrů, a o podobné strategie v návazných oblastech, jako je ochrana kritické infrastruktury nebo identifikace priorit mezinárodní spolupráce. Tyto dokumenty pomáhají promítnout obecné směry a vize strategie do praktických kroků, které mají vést ke zvýšení odolnosti státu i jeho obyvatel vůči kybernetickým útokům.[60]

6.3 Mezinárodní přístupy a doporučení

Mezinárodní přístupy ke kybernetické bezpečnosti v rámci Evropské unie vycházejí z koordinovaných politik a rámců, které usilují o harmonizaci postupů a posílení schopností členských států čelit kybernetickým hrozbám. Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), jako odborný orgán EU, se podílí na tvorbě společných standardů, certifikačních schémat a strategií, které mají zajistit vysokou úroveň zabezpečení v celé Unii a zároveň podporovat sdílení informací a budování kapacit mezi jednotlivými zeměmi. Tento přístup je založen na spolupráci, budování důvěry, výměně znalostí a společném zvyšování odolnosti digitálního prostoru, čímž se EU snaží lépe koordinovat reakci na kybernetické incidenty a posílit preventivní opatření na společné evropské úrovni.

Další mezinárodní doporučení a koncepční rámce nad rámec EU vycházejí z dlouhodobých iniciativ Rady Evropy či Organizace spojených národů, které zdůrazňují potřebu a význam přeshraniční spolupráce v oblasti kybernetické bezpečnosti. Tato doporučení podporují sdílení dobrých postupů, harmonizaci legislativních opatření i

[60] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti České republiky na období 2020–2025.* Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2020. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

koordinaci při řešení kybernetických hrozeb, protože hrozby v kyberprostoru často překračují národní hranice a vyžadují integrovaný mezinárodní přístup.[61]

[61] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *National Capabilities Assessment Framework.* [PDF]. Heraklion: ENISA, 2020. ISBN 978-92-9204-473-2. Dostupné z: https://www.enisa.europa.eu/sites/default/files/all_files/National%20Capabilities%20Assessment%20Framework_CS.pdf

7 Informovanost veřejnosti a prevence kriminality

7.1 Prevence kriminality a její význam

Prevence kriminality zahrnuje různá opatření, hlavním cílem je předcházet vzniku trestné činnosti a omezovat její negativní dopady na společnost. Na rozdíl od represivních přístupů, které řeší trestnou činnost až po jejím spáchání, se prevence zaměřuje na včasné působení na rizikové chování a okolnosti, které mohou ke kriminalitě vést. Cílem není pouze snížení kriminality, ale také posílení pocitu bezpečí mezi obyvateli.[62]

V oblasti kybernetické bezpečnosti má prevence stále větší význam. Kybernetické útoky dnes neohrožují jen technické systémy nebo velké organizace, ale stále častěji zasahují i běžné uživatele internetu. Důsledky těchto útoků se mohou projevit například ztrátou osobních údajů, finančními škodami nebo narušením soukromí. Odborné zprávy upozorňují na to, že vývoj kybernetických hrozeb je velmi rychlý a vyžaduje důraz na preventivní přístup.[63]

7.2 Informovanost veřejnosti jako nástroj prevence

Informovanost veřejnosti hraje v prevenci kybernetické kriminality důležitou roli. Mnoho útoků je založeno na chybách uživatelů, kteří například nedokážou rozpoznat podvodný e-mail nebo falešnou internetovou stránku. Útočníci často spoléhají na nepozornost, nedostatek zkušeností nebo důvěřivost uživatelů, což potvrzuje význam lidského faktoru v oblasti kybernetické bezpečnosti.[64]

Zvyšování povědomí o kybernetických hrozbách a základních zásadách bezpečného chování může pomoci snížit úspěšnost těchto útoků. Informovaný uživatel je obvykle opatrnější, dokáže lépe vyhodnotit rizikové situace a přizpůsobit tomu své chování na internetu. Zároveň je však nutné zdůraznit, že samotné informace nestačí. Aby

[62] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Strategický rámec prevence kriminality v České republice na období 2021–2025 [online]. Praha: Ministerstvo vnitra ČR, 2021. Dostupné z: https://www.mvcr.cz

[63] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Národní strategie kybernetické bezpečnosti České republiky na období 2020–2025. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2020. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[64] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA Threat Landscape 2025 [online]. 1. October 2025. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

měla informovanost skutečný přínos, musí být doplněna ochotou uživatelů své znalosti využívat v praxi a měnit své online návyky.[65]

7.3 Vzdělávání v oblasti kybernetické bezpečnosti

Vzdělávání představuje jeden z nejdůležitějších nástrojů dlouhodobé prevence v oblasti kybernetické bezpečnosti. Základní znalosti bezpečného chování na internetu by měly být dostupné všem uživatelům, bez ohledu na jejich věk nebo technické znalosti. Vzdělávací aktivity by proto měly být přizpůsobeny různým skupinám obyvatel, od dětí a studentů až po dospělé a seniory.[66]

Významnou roli v této oblasti sehrávají školy, které mohou již od raného věku formovat bezpečné návyky při používání digitálních technologií. Stejně tak zaměstnavatelé mohou prostřednictvím školení a interních pravidel posilovat povědomí o aktuálních hrozbách. Tyto znalosti si zaměstnanci často přenášejí i do svého soukromého života. Důležitým aktérem jsou rovněž média a státní instituce, které mohou veřejnost oslovovat prostřednictvím srozumitelných informačních kampaní a preventivních programů.[67]

[65] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Národní strategie kybernetické bezpečnosti České republiky na období 2020–2025. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2020. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[66] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA Threat Landscape 2025 [online]. 1. October 2025. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[67] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Strategický rámec prevence kriminality v České republice na období 2021–2025 [online]. Praha: Ministerstvo vnitra ČR, 2021. Dostupné z: https://www.mvcr.cz

8 Praktická část - dotazníkové šetření

8.1 Metodika výzkumu

Cílem dotazníkového šetření bylo zjistit, jak dobře jsou respondenti obeznámeni s problematikou kybernetických hrozeb a zda si uvědomují rizika, která jsou spojena s používáním internetu. Zajímalo mě také, do jaké míry dodržují zásady bezpečného chování v online prostředí, zda mají osobní zkušenost s kybernetickým útokem a jak vnímají význam prevence v oblasti kybernetické bezpečnosti. Výsledky měly ukázat, jak důležitá je informovanost veřejnosti jako jeden z nástrojů prevence kybernetické kriminality a zároveň poukázat na oblasti, ve kterých je potřeba osvětu dále posílit.

Dotazník byl sestaven jako strukturovaný nástroj a zaměřoval se na několik navzájem souvisejících oblastí. Otázky byly rozděleny do tematických okruhů tak, aby odpovídaly stanoveným cílům práce a umožnily získat ucelený přehled o zkoumané problematice. Konkrétně se dotazník zaměřoval na:

- obecnou informovanost respondentů o kybernetických hrozbách a jejich vnímání rizik v online prostředí,
- znalost konkrétních typů kybernetických hrozeb, jako je phishing, malware, ransomware, krádež identity nebo kyberšikana,
- osobní zkušenosti respondentů s kybernetickými útoky a podvody,
- chování respondentů v online prostředí, zejména v oblasti používání hesel a bezpečnostních opatření,
- zdroje informací o kybernetické bezpečnosti a postoje respondentů k významu prevence a zvyšování informovanosti.

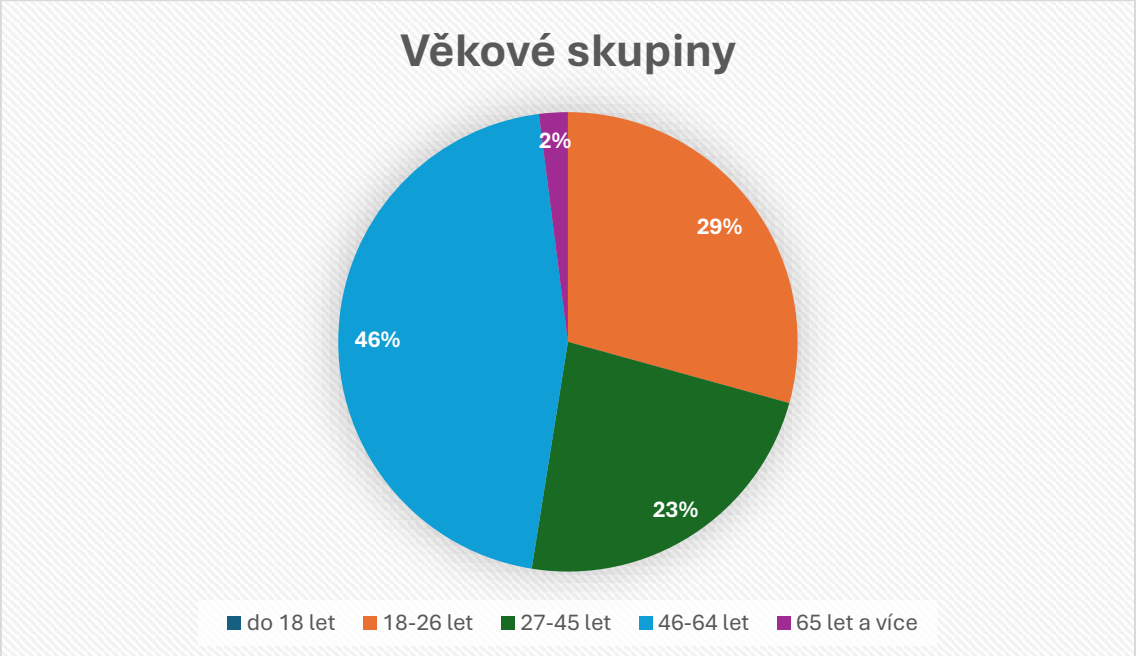
Dotazník tak sloužil k získání přehledu o znalostech, postojích a chování respondentů v oblasti kybernetické bezpečnosti, přičemž jednotlivé tematické okruhy odpovídají výzkumným otázkám práce.

8.2 Charakteristika respondentů

Dotazníkové šetření proběhlo mezi osobami, které v běžném životě aktivně využívají internet a digitální technologie, a to jak pro pracovní, tak i osobní účely. Celkem se do výzkumu zapojilo 123 respondentů. Oslovení proběhlo elektronickou formou, což bylo vzhledem k zaměření práce na online prostředí logickou volbou. Tento způsob distribuce zároveň umožnil rychlý, efektivní a finančně nenáročný sběr dat. Dotazník byl vyplňován anonymně, což mohlo přispět k větší otevřenosti a upřímnosti odpovědí, zejména u otázek týkajících se osobních zkušeností s kybernetickými útoky či vlastního chování na internetu.

Věkové složení účastníků šetření bylo poměrně rozmanité. Největší zastoupení měli respondenti ve věku 46–64 let (46 %), kteří tvořili téměř polovinu celého výzkumného souboru. Dále byly výrazně zastoupeny věkové skupiny 18–26 let (29 %) a 27–45 let. (23 %) Osoby ve věku 65 let a více (2 %) se v grafu objevily pouze okrajově. Věkovou kategorii do 18 let nezvolil žádný respondent. Věkové rozložení tak umožňuje nahlížet na problematiku informovanosti o kybernetických hrozbách z perspektivy různých generací uživatelů internetu.

Graf č. 1 Věkové skupiny[68]



Takto získaná struktura respondentů zároveň umožňuje porovnat úroveň informovanosti, zkušeností i přístupů ke kybernetické bezpečnosti napříč jednotlivými generacemi. Lze předpokládat, že věkové skupiny se mohou lišit jak ve znalostech

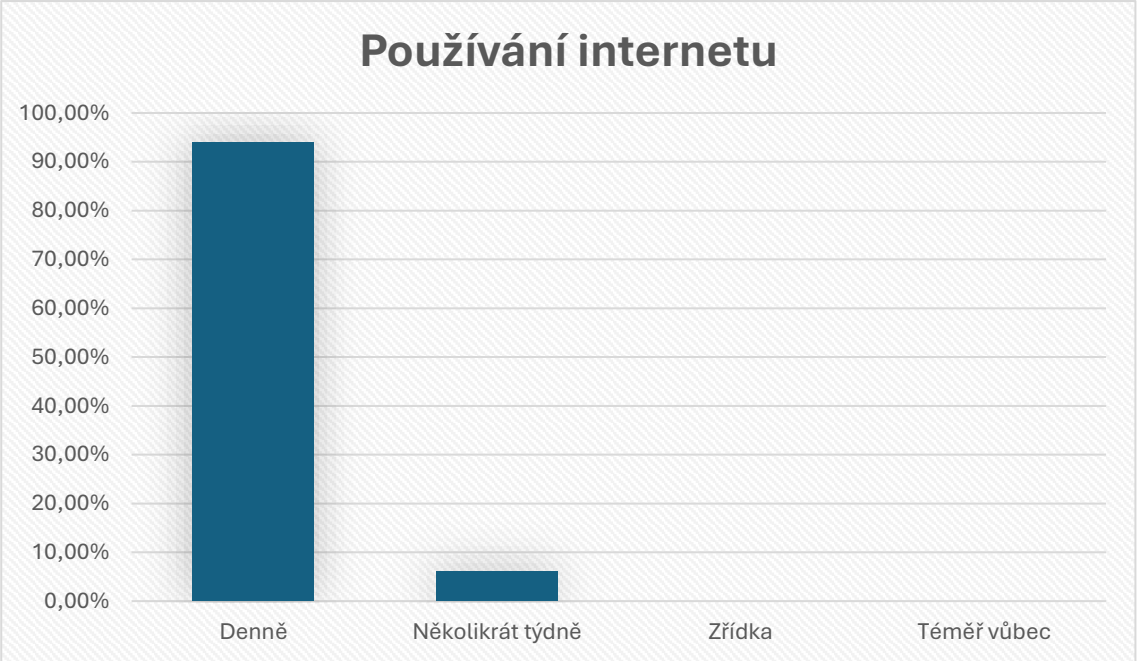
[68] Vlastní zpracování

konkrétních hrozeb, tak i v míře opatrnosti při používání digitálních technologií a online služeb.

Z odpovědí vyplynulo, že naprostá většina dotázaných využívá internet každý den. (94 %). To znamená, že jsou v pravidelném a intenzivním kontaktu s online prostředím, a tedy i potenciálně vystaveni různým formám kybernetických hrozeb. Pouze malé procento účastníků uvedlo, že internet používá méně často, například jen několikrát týdně nebo výjimečně. (6 %)

Tato skutečnost je z hlediska výzkumu velmi významná. Pravidelné využívání internetu zvyšuje pravděpodobnost setkání s podvodnými e-maily, falešnými odkazy, pokusy o zneužití osobních údajů nebo dalšími projevy kybernetické kriminality. Zároveň lze předpokládat, že častý kontakt s digitálním prostředím vede k postupnému vytváření určitých návyků – ať už bezpečných, nebo naopak rizikových. Uživatelé, kteří jsou online denně, tak mají nejen větší pravděpodobnost získat zkušenost s konkrétní hrozbou, ale také si postupně vytvářejí vlastní přístup k otázkám bezpečnosti, například v oblasti používání hesel, aktualizací či ověřování podezřelých zpráv.

Graf č. 2 Používání internetu[69]



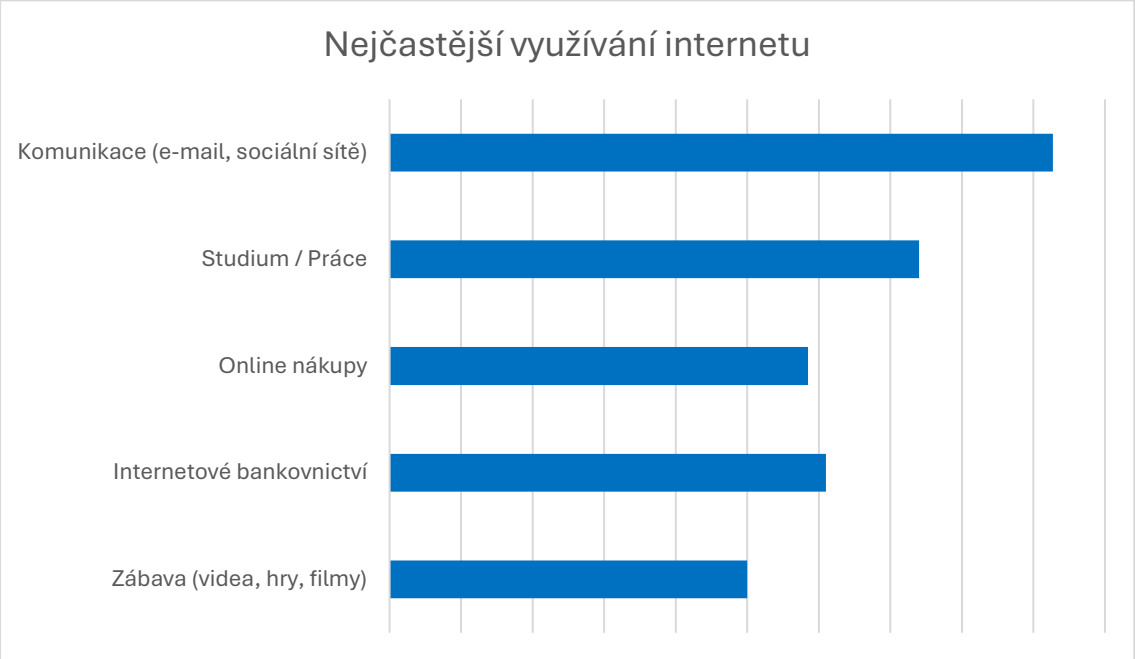
[69] Vlastní zpracování

Současně je však třeba si uvědomit, že časté používání internetu může představovat výhodu i určité riziko. Každodenní pohyb v online prostoru proto vyžaduje určitou míru obezřetnosti a schopnost rozpoznat podezřelé situace. Pravidelný kontakt s digitálními technologiemi může vést k získávání zkušeností, které následně ovlivňují další chování uživatelů.

Z odpovědí dále vyplynulo, že internet je nejčastěji využíván ke komunikaci, zejména prostřednictvím e-mailu a sociálních sítí. Tyto nástroje jsou dnes běžnou součástí každodenního života a slouží jak k osobní, tak i pracovní komunikaci. Významnou roli hraje také využívání internetu pro studijní a pracovní účely, což potvrzuje jeho důležitost v profesní i vzdělávací oblasti.

Řada dotázaných zároveň uvedla, že internet používá také k online nakupování a k internetovému bankovnictví, tedy k činnostem, které jsou spojeny s prací s osobními a finančními údaji. Část účastníků využívá digitální služby také pro zábavu, například ke sledování videí, hraní her nebo poslechu hudby.

Graf č. 3 Nejčastější využívání internetu[70]



Z uvedených odpovědí je patrné, že dotázané osoby představují běžné a aktivní uživatele digitálních technologií. Internet je pro ně přirozenou součástí každodenního života, a právě proto je pro tuto skupinu problematika kybernetické bezpečnosti velmi aktuální.

[70] Vlastní zpracování

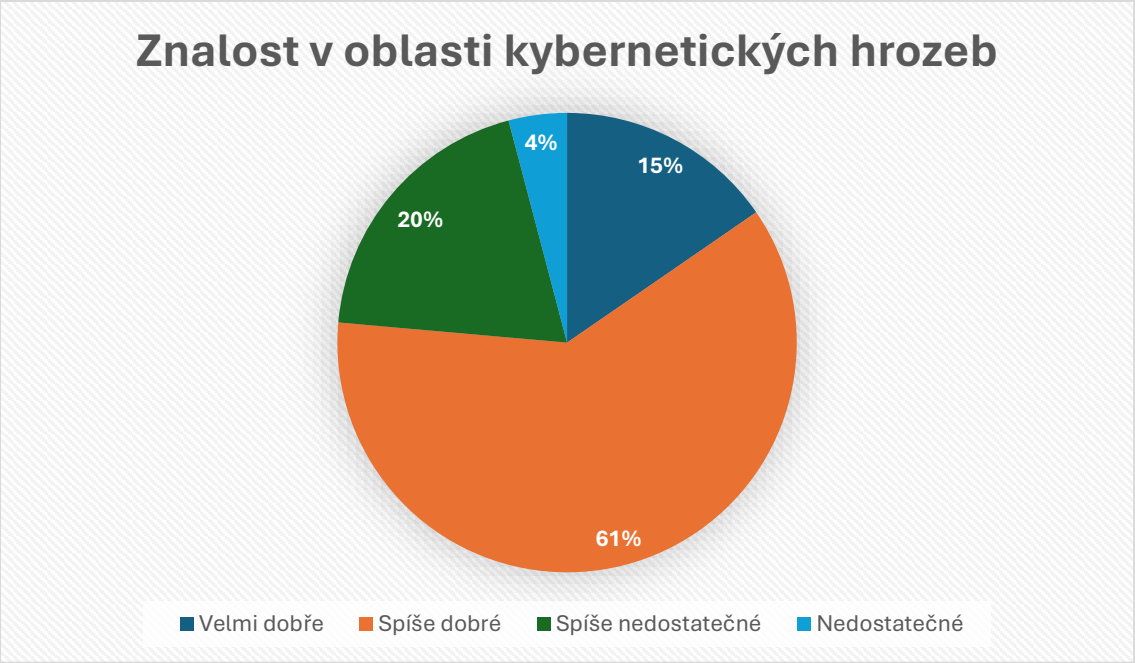
Získaná data byla zpracována pomocí základních statistických postupů. Odpovědi byly vyhodnoceny v podobě absolutních a relativních četností a následně přehledně zpracovány do grafů. Při interpretaci výsledků byl kladen důraz především na naplnění cíle práce a na posouzení možností zlepšení preventivních opatření v oblasti kybernetické bezpečnosti.

8.3 Vyhodnocení dotazníkového šetření

8.3.1 Informovanost respondentů o kybernetických hrozbách

Při hodnocení vlastních znalostí v oblasti kybernetické bezpečnosti účastníci šetření nejčastěji uváděli, že své znalosti považují za spíše dobré (61 %). Část dotázaných se hodnotila dokonce velmi pozitivně a vyjádřila přesvědčení, že má v této oblasti dostatečný přehled (15 %). Na druhou stranu přibližně pětina účastníků přiznala, že jejich znalosti jsou spíše nedostatečné (20 %) nebo zcela nedostatečné (4 %).

Graf č. 4 Znalost v oblasti kybernetických hrozeb[71]



Z provedené analýzy je tedy patrné, že ačkoli většina dotázaných má alespoň základní povědomí o kybernetických hrozbách, úroveň jejich skutečné informovanosti není jednotná. Někteří se v této problematice orientují poměrně dobře, zatímco jiní si uvědomují své mezery a nedostatek hlubších znalostí. Tento rozdíl může ovlivňovat nejen

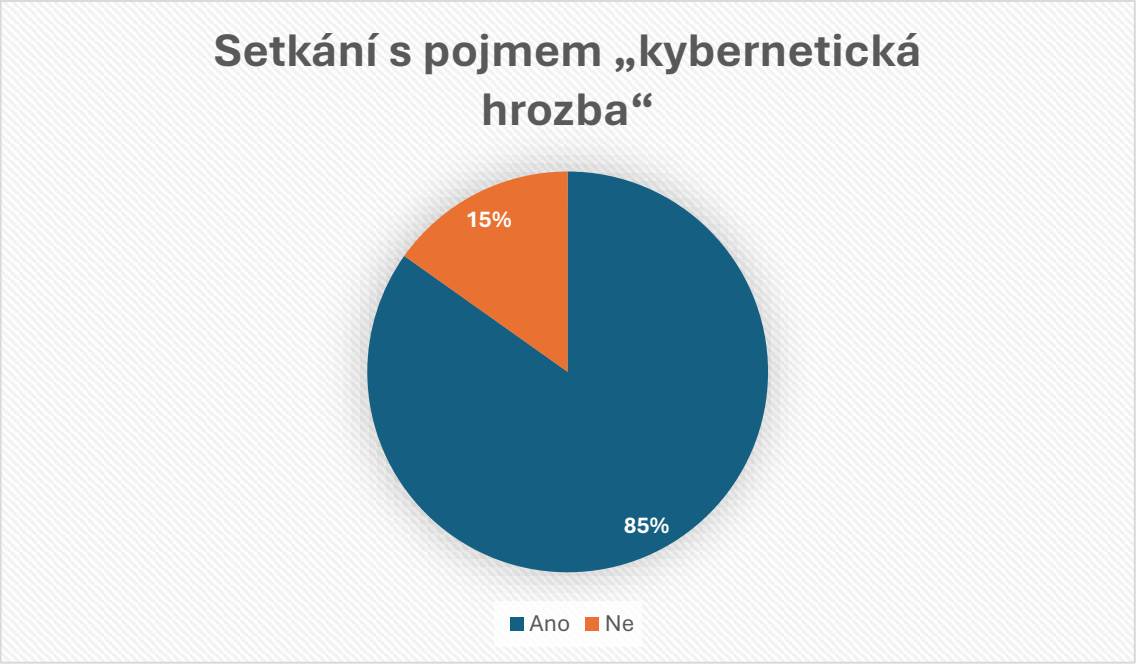
[71] Vlastní zpracování

schopnost rozpoznat konkrétní hrozby, ale také celkové chování uživatelů v online prostředí.

Z odpovědí zároveň vyplývá, že hodnocení vlastních znalostí je do určité míry subjektivní a může být ovlivněno osobními zkušenostmi nebo informacemi, se kterými se lidé běžně setkávají. Tento rozdíl ukazuje, že samotný pocit informovanosti nemusí vždy odpovídat skutečné úrovni znalostí a že stále existuje prostor pro další zvyšování povědomí o této problematice.

Dále byli účastníci šetření dotázáni, zda se již setkali s pojmem „kybernetická hrozba“. Většina z nich uvedla, že tento výraz zná a již o něm někdy slyšela (85 %). Pouze menší část dotázaných odpověděla, že se s tímto označením dosud nesetkala (15 %). Lze tedy konstatovat, že základní povědomí o kybernetických hrozbách je mezi veřejností poměrně rozšířené.

Graf č. 5 Setkání s pojmem „kybernetická hrozba“[72]



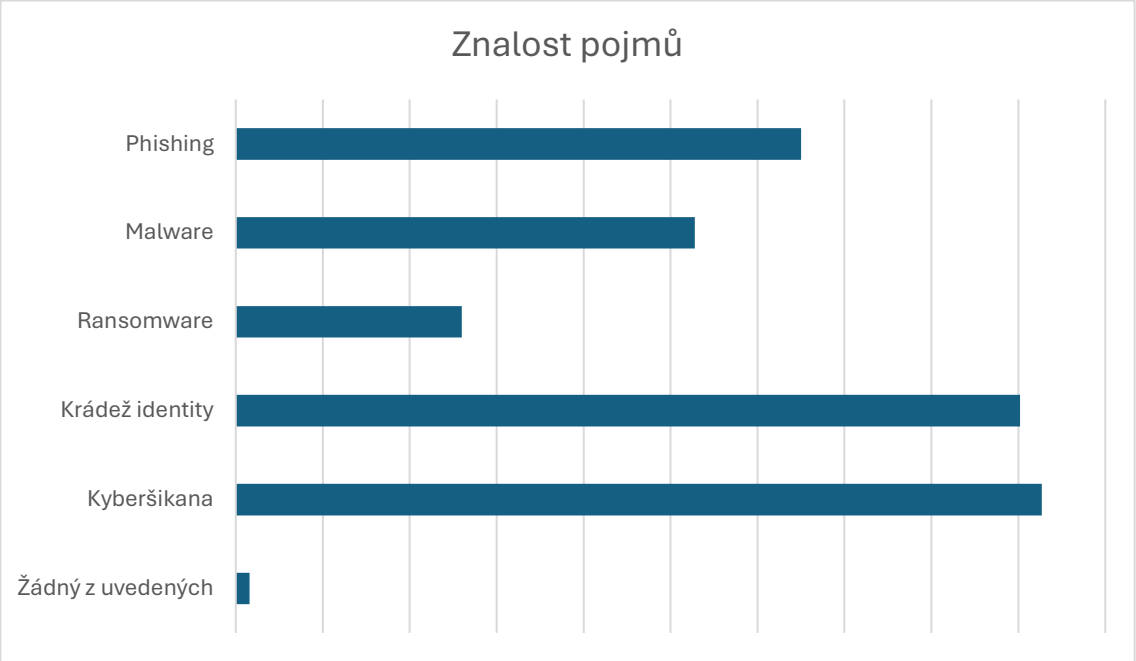
Tento výsledek naznačuje, že pojem kybernetická hrozba je mezi veřejností poměrně známý a objevuje se i v běžném veřejném diskurzu. Samotná znalost tohoto označení však ještě neznamená, že mu všichni lidé skutečně rozumí nebo si dokážou představit jeho konkrétní projevy a možné dopady v praxi. U části dotázaných se tak může jednat spíše o obecné povědomí než o hlubší a systematičtější znalosti.

[72] Vlastní zpracování

Tento rozdíl v úrovni porozumění se může promítat také do jejich chování na internetu. Uživatelé, kteří mají pouze základní představu o kybernetických hrozbách, nemusí vždy důsledně dodržovat zásady bezpečného používání digitálních služeb, například při práci s osobními údaji, při správě hesel nebo při otevírání neznámých odkazů.

Rozdíly se projevily také při znalosti konkrétních typů kybernetických hrozeb. Největší povědomí měli dotázaní o kyberšikaně a krádeži identity. Poměrně často byly uváděny také pojmy phishing a malware. Naopak ransomware byl známý menšímu počtu účastníků šetření. Tato skutečnost může souviset s tím, že některé typy útoků jsou častěji zmiňovány v médiích nebo se s nimi veřejnost může setkat v běžném životě.

Graf č. 6 Znalost pojmů[73]



Z odpovědí vyplývá, že veřejnost má větší přehled o těch hrozbách, o kterých se častěji hovoří v médiích nebo které si lidé dokážou spojit s konkrétní situací z každodenního života. Typickým příkladem je kyberšikana, která bývá často zmiňována v souvislosti se školním prostředím nebo se sociálními sítěmi. Díky tomu si ji mnoho lidí dokáže lépe představit a uvědomuje si možné dopady tohoto jednání.

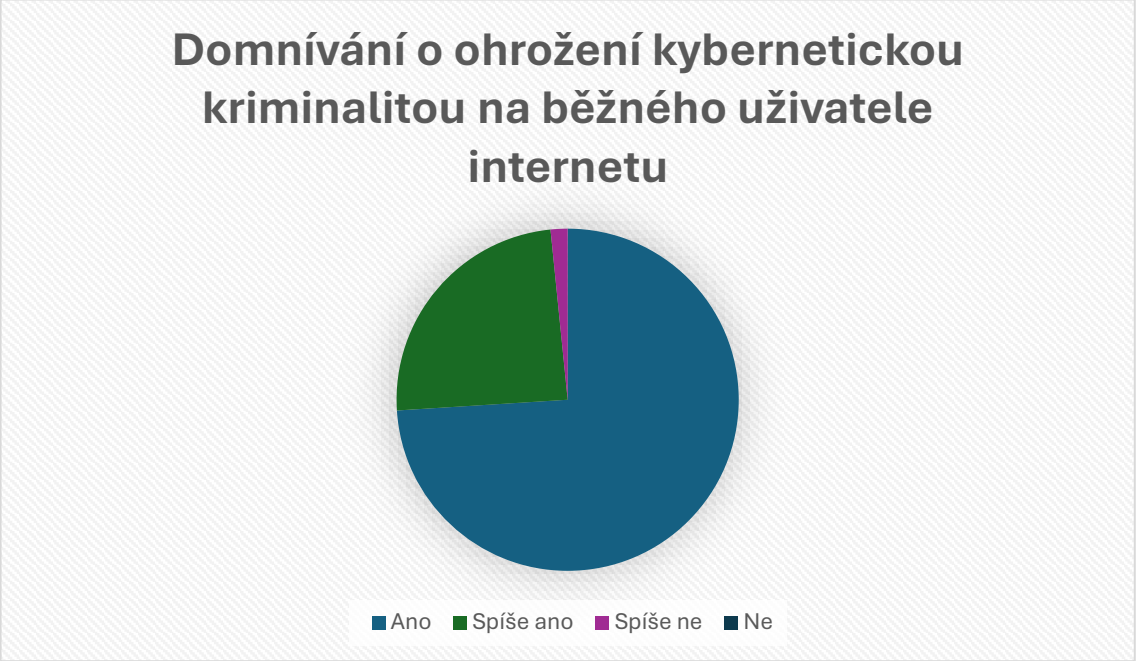
[73] Vlastní zpracování

Naopak označení ransomware může na běžného uživatele působit spíše technicky a abstraktně, zejména pokud se s ním osobně nesetkal nebo o něm neslyšel v konkrétním kontextu. V takovém případě může být jeho význam méně srozumitelný, přestože se jedná o závažnou formu kybernetické hrozby.

Tento rozdíl naznačuje, že úroveň informovanosti veřejnosti je do určité míry ovlivněna způsobem, jakým jsou jednotlivé hrozby prezentovány a vysvětlovány. Čím srozumitelnější a konkrétnější je výklad daného problému, tím větší je pravděpodobnost, že si jej lidé zapamatují a budou mu věnovat větší pozornost.

V závěru této části byli účastníci šetření dotázáni, zda se domnívají, že i běžný uživatel internetu může být ohrožen kybernetickou kriminalitou. Většina z nich odpověděla kladně. Z toho lze usuzovat, že si dotázaní uvědomují možná rizika spojená s používáním digitálních technologií, což může mít vliv na jejich chování v online prostředí.

Graf č. 7 Domnívání o ohrožení kybernetickou kriminalitou na běžného uživatele internetu[74]



Tento pohled naznačuje, že účastníci výzkumu nepovažují kybernetickou kriminalitu pouze za problém firem nebo odborníků na informační technologie, ale uvědomují si, že se může dotýkat i běžných uživatelů v každodenních situacích. Zároveň však nelze jednoznačně říci, že samotné uvědomění si rizik automaticky vede k

[74] Vlastní zpracování

odpovědnějšímu chování na internetu. U některých osob může zůstat spíše na úrovni obecného pocitu ohrožení, aniž by došlo ke konkrétním změnám jejich online návyků.

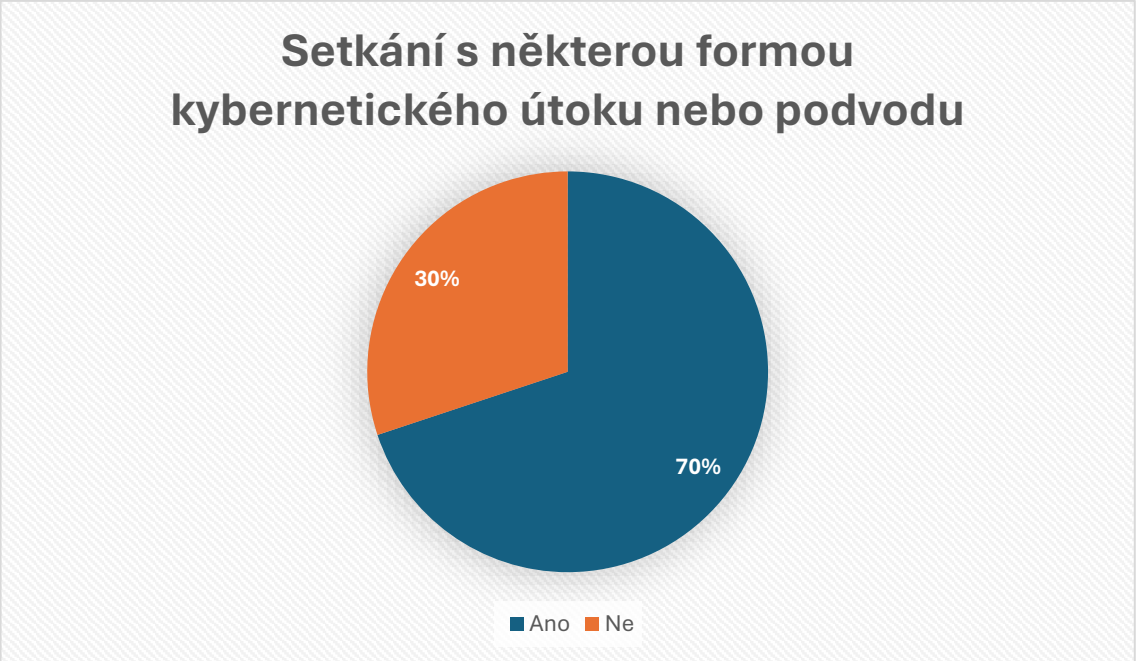
Z odpovědí dále vyplývá, že i když si dotázaní možná rizika uvědomují, často mají pocit, že se jich osobně podobné situace netýkají. Tento postoj může vést k podceňování některých bezpečnostních doporučení, například při práci s hesly nebo při otevírání podezřelých zpráv. V praxi tak může docházet k situacím, kdy uživatelé vědí, že určité chování není bezpečné, přesto ho nemění, protože jej nepovažují za bezprostředně rizikové.

8.3.2 Zkušenosti respondentů s kybernetickými útoky

Další část dotazníku byla zaměřena na osobní zkušenosti respondentů s kybernetickými útoky a podvody. Cílem bylo zjistit, zda se již s nějakou formou kybernetické kriminality setkali a jaké typy útoků se mezi nimi objevují nejčastěji.

Z odpovědí vyplývá, že poměrně velká část dotázaných má s kybernetickým útokem nebo internetovým podvodem osobní zkušenost (70 %). Přestože někteří uvedli, že se s podobnou situací dosud nesetkali, převažovaly odpovědi potvrzující opak (30 %). Tato skutečnost naznačuje, že kybernetická kriminalita nepředstavuje pouze teoretický problém, ale reálné riziko, se kterým se mohou setkat i běžní uživatelé internetu.

Graf č. 8 Setkání s některou formou kybernetického útoku nebo podvodu[75]



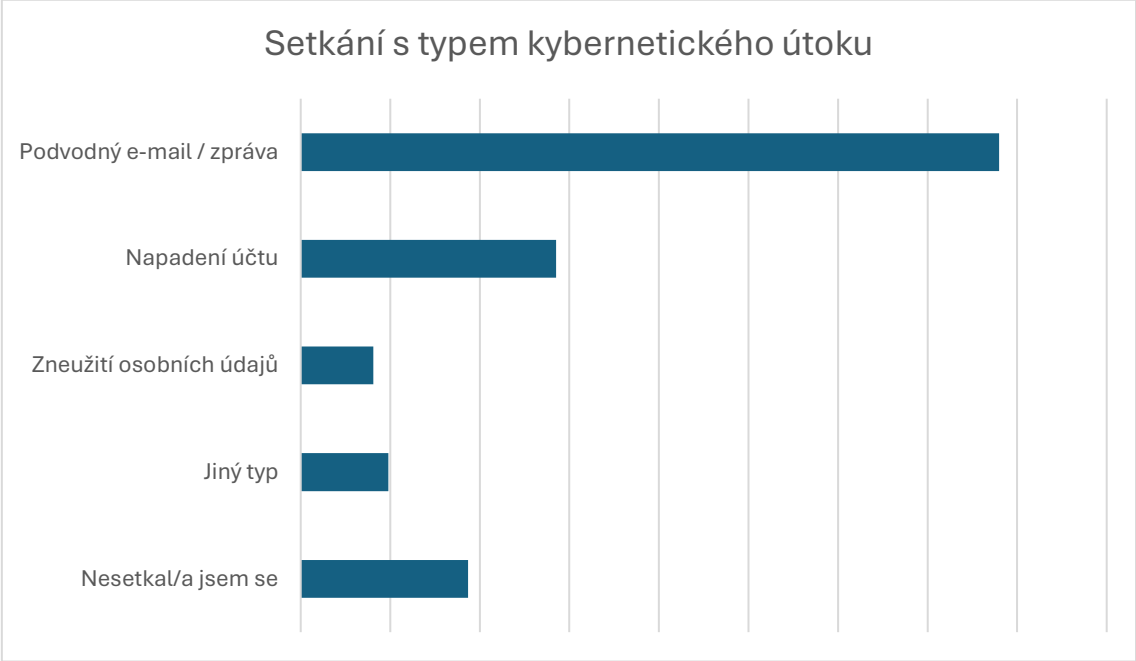
[75] Vlastní zpracování

Je možné, že skutečný počet těchto zkušeností je ještě vyšší, než uvádějí samotní účastníci šetření. Někteří lidé si totiž nemusí uvědomit, že se stali obětí podvodu, protože určité formy kybernetické kriminality nepůsobí na první pohled závažně.

Tato zjištění ukazují, že problematika kybernetických hrozeb je stále velmi aktuální a může se týkat širokého okruhu uživatelů bez ohledu na jejich věk či zkušenosti s digitálními technologiemi.

Nejčastěji dotázaní uváděli zkušenost s podvodnými e-maily nebo zprávami, což odpovídá častému výskytu phishingových útoků. Poměrně často se objevovaly také případy napadení uživatelského účtu. Méně účastníků šetření uvedlo zneužití osobních údajů nebo jiné typy incidentů. Část dotázaných zároveň uvedla, že se s žádným kybernetickým incidentem dosud nesetkala.

Graf č. 9 Setkání s typem kybernetického útoku[76]



Získané poznatky naznačují, že podvodná komunikace, zejména ve formě phishingu, patří mezi nejčastější hrozby, se kterými se uživatelé internetu setkávají. Osobní zkušenost s kybernetickým útokem přitom může výrazně ovlivnit způsob, jakým lidé tato rizika vnímají a zda jsou ochotni přijímat preventivní opatření.

[76] Vlastní zpracování

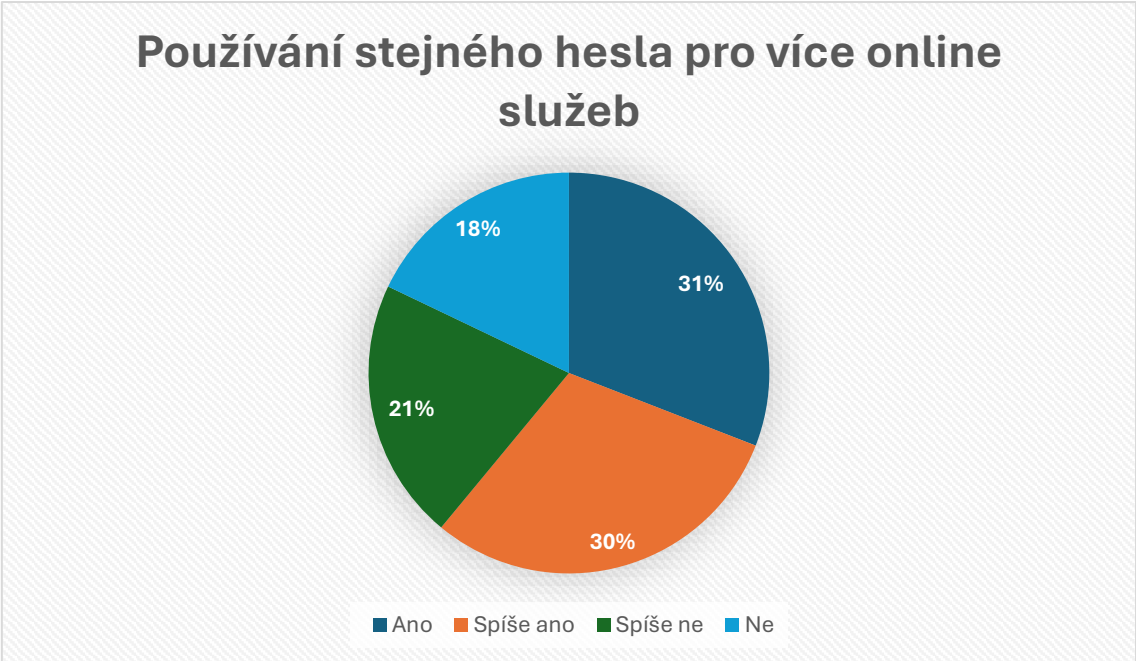
Vlastní negativní zkušenost bývá pro mnoho osob silnějším impulzem než obecná varování v médiích. Pokud se někdo s podvodem setká osobně, obvykle začne být opatrnější, pečlivěji kontroluje podezřelé zprávy a věnuje větší pozornost ochraně svých údajů. Naopak lidé, kteří podobnou zkušenost nemají, mohou rizika podceňovat nebo je považovat za problém, který se týká spíše ostatních.

8.3.3 Bezpečné chování respondentů v online prostředí

Tato část dotazníku byla zaměřena na bezpečnostní návyky respondentů, především na práci s hesly a využívání různých ochranných opatření. Cílem bylo zjistit, do jaké míry dotázaní dodržují zásady bezpečného chování v online prostředí.

Z odpovědí vyplynulo, že značná část účastníků šetření používá stejné heslo pro více online služeb, a to buď pravidelně, nebo alespoň v některých případech. Menší skupina uvedla, že pro jednotlivé služby používá vždy odlišná přístupová hesla. Tento výsledek naznačuje přetrvávající rizikové chování, které může v případě úniku přihlašovacích údajů vést k ohrožení více účtů současně.

Graf č. 10 Používání stejného hesla pro více online služeb[77]



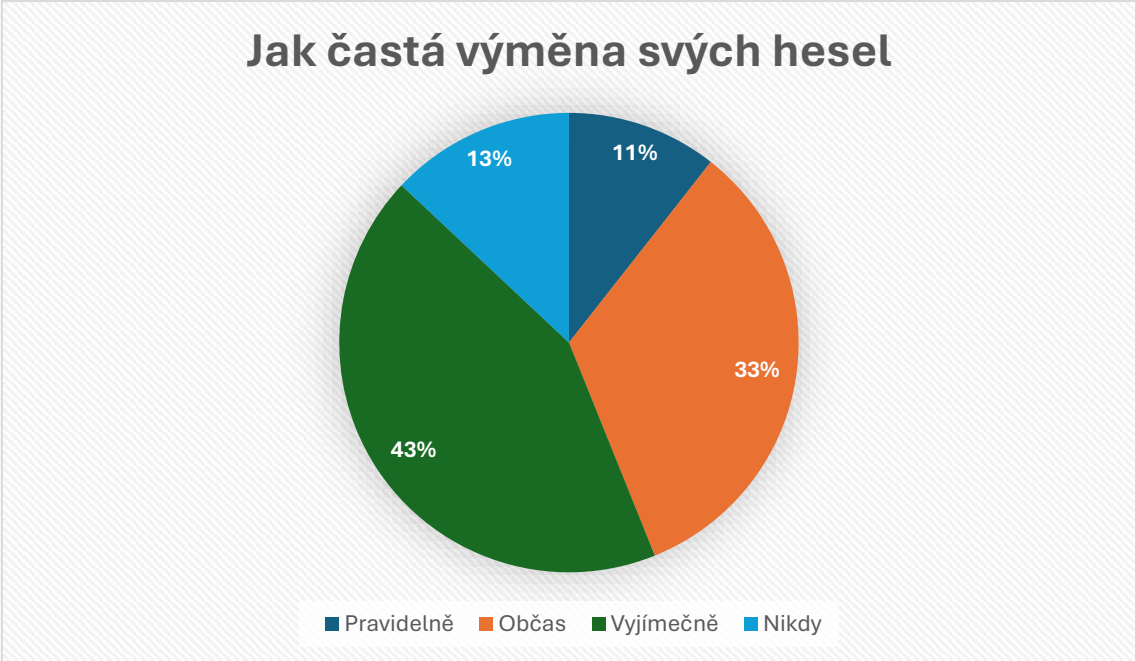
Používání stejného hesla je pro mnoho lidí pohodlné, protože si nemusí pamatovat několik různých přístupových údajů. Zároveň si však často plně neuvědomují, jaké riziko to představuje v případě prolomení některého z jejich účtů. Pokud útočník získá jedno heslo, může se poměrně snadno dostat i k dalším službám, kde je použito stejné přihlášení.

[77] Vlastní zpracování

Důsledky tak mohou být mnohem závažnější, než si uživatelé připouštějí – od ztráty přístupu k účtům až po zneužití osobních nebo finančních údajů.

Pokud jde o frekvenci změny hesel, většina dotázaných uvedla, že přihlašovací údaje mění spíše výjimečně (43 %) nebo pouze občas (33 %). Pouze menší část účastníků šetření je upravuje pravidelně (11 %), zatímco někteří je nemění vůbec (13 %). Tyto odpovědi naznačují, že i když si lidé rizika spojená s ochranou účtů uvědomují, jejich skutečné chování tomu ne vždy odpovídá.

Graf č. 11 Jak častá výměna svých hesel[78]



Z odpovědí dále vyplývá, že pravidelná změna hesla není pro mnoho osob prioritou. K úpravě přihlašovacích údajů často dochází až ve chvíli, kdy nastane konkrétní problém, například podezření na napadení účtu nebo upozornění ze strany poskytované služby. Preventivní přístup, tedy změna hesla bez předchozí negativní zkušenosti, se objevuje spíše výjimečně.

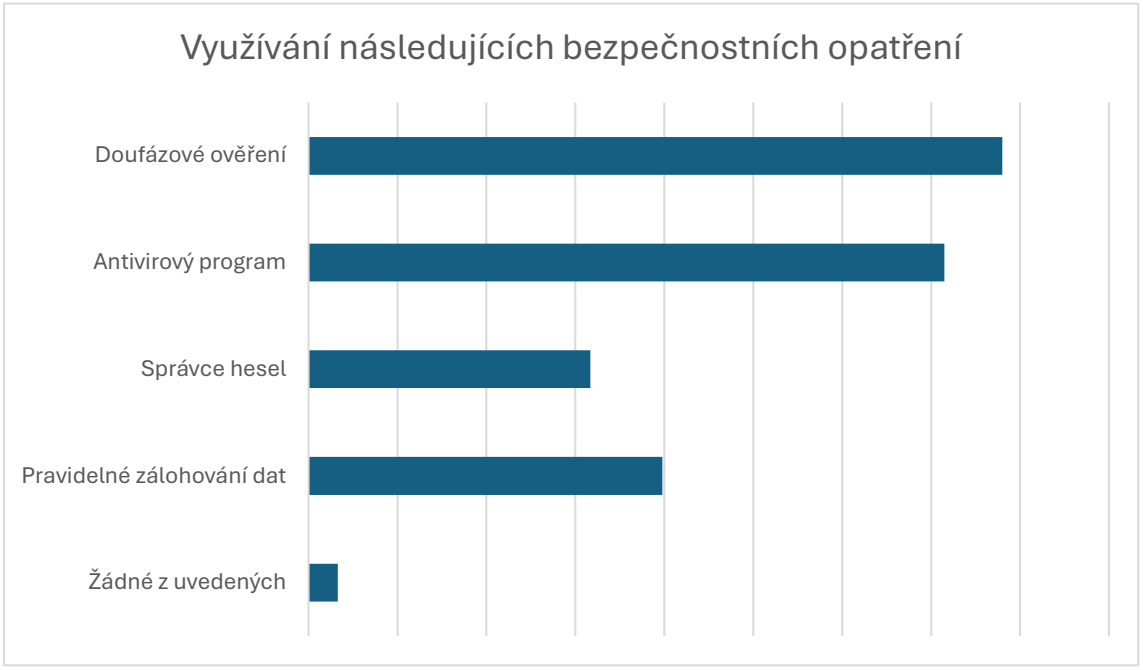
Někteří lidé mohou mít pocit, že jejich účet není pro útočníky dostatečně zajímavý, případně že se podobné incidenty týkají spíše jiných uživatelů. Tento pocit určité „bezpečné vzdálenosti“ však může vést k podcenění rizika. Slabé nebo dlouhodobě neměněné heslo totiž výrazně zvyšuje pravděpodobnost zneužití účtu, zejména pokud jsou stejné přihlašovací údaje používány i u dalších služeb.

[78] Vlastní zpracování

Zjištění tak naznačují, že i když si dotázaní obecně uvědomují existenci kybernetických hrozeb, v praxi nemusí vždy dodržovat základní preventivní opatření, která by mohla riziko výrazně snížit.

Respondenti byli dále dotazováni na využívání konkrétních bezpečnostních opatření. Nejčastěji uváděným nástrojem bylo dvoufázové ověření, které využívá významná část účastníků šetření. Poměrně často bylo zmiňováno také používání antivirového programu. Naopak správce hesel využívá pouze menší skupina dotázaných. Někteří zároveň uvedli, že žádné z nabízených bezpečnostních opatření nevyužívají.

Graf č. 12 Využívání následujících bezpečnostních opatření[79]



Celkové výsledky ukazují, že povědomí o možnostech zabezpečení účtů mezi respondenty existuje, avšak jejich praktické využívání není u všech samozřejmostí. Rozdíl mezi znalostí bezpečnostních zásad a jejich uplatňováním v praxi tak představuje důležitý aspekt prevence kybernetické kriminality.

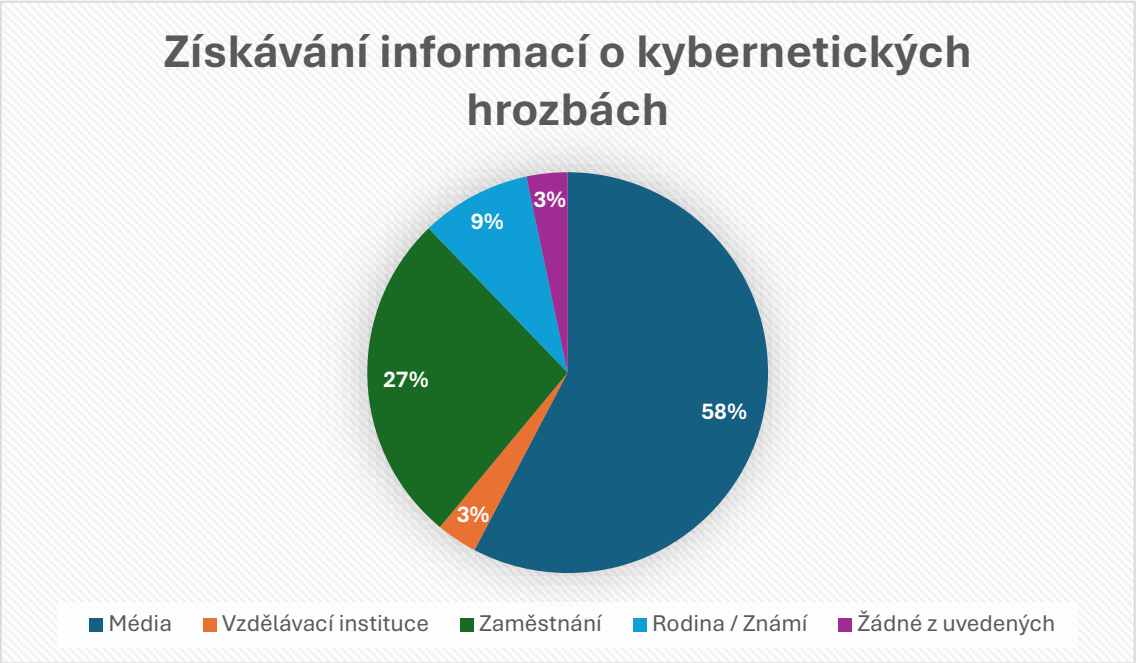
V praxi to znamená, že mnoho uživatelů sice ví, jak by se měli na internetu chovat bezpečně, ale z různých důvodů tato pravidla nedodržují důsledně. Často může jít o pohodlnost, nedostatek času nebo pocit, že se jim nic nestane. Právě tento rozpor mezi znalostmi a skutečným chováním ukazuje, že samotná informovanost nestačí a že je potřeba uživatele motivovat k tomu, aby bezpečnostní zásady skutečně uplatňovali v každodenním používání internetu.

[79] Vlastní zpracování

8.3.4 Zdroje informací a postoje k prevenci

Další část dotazníku se zaměřila na zdroje, ze kterých účastníci šetření nejčastěji získávají poznatky o kybernetických hrozbách. Nejčastěji byl jako hlavní zdroj uváděn mediální obsah (58 %). Významnou roli však hrají také zaměstnání (27 %). Menší část dotázaných čerpá poznatky od rodiny či známých (9 %), či ze vzdělávacích institucí (3 %). Další část uvedla, že žádný z nabízených zdrojů nevyužívá (3 %).

Graf č. 13 Získávání informací o kybernetických hrozbách[80]



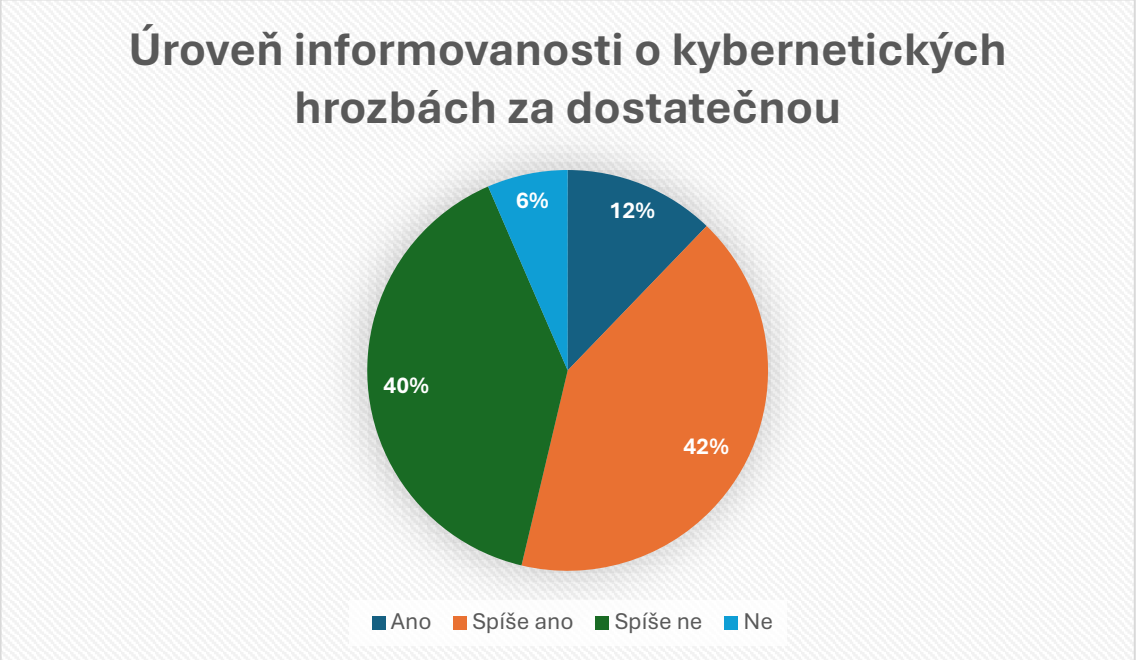
Z výsledků vyplývá, že mediální sdělení představují pro většinu respondentů nejdostupnější zdroj informací a často jsou jejich prvním setkáním s tématem kybernetické bezpečnosti. Média tak hrají důležitou roli při vytváření základního povědomí o aktuálních hrozbách a možných rizicích.

Současně se však ukazuje, že systematičtější a cílenější vzdělávání, například ve škole nebo v rámci pracovního prostředí, může mít výraznější vliv na skutečné porozumění této problematice. Takové vzdělávání bývá zpravidla podrobnější a poskytuje širší kontext, díky čemuž si lidé mohou lépe uvědomit konkrétní dopady kybernetických hrozeb i možnosti jejich prevence.

[80] Vlastní zpracování

Respondenti se dále vyjadřovali k tomu, zda považují současnou úroveň informovanosti veřejnosti o kybernetických hrozbách za dostatečnou. Z odpovědí vyplynulo, že značná část dotázaných tuto úroveň nepovažuje za zcela dostačující (40 %). Tento názor poukazuje na potřebu další osvěty a preventivních aktivit v oblasti kybernetické bezpečnosti.

Graf č. 14 Úroveň informovanosti o kybernetických hrozbách za dostatečnou[81]



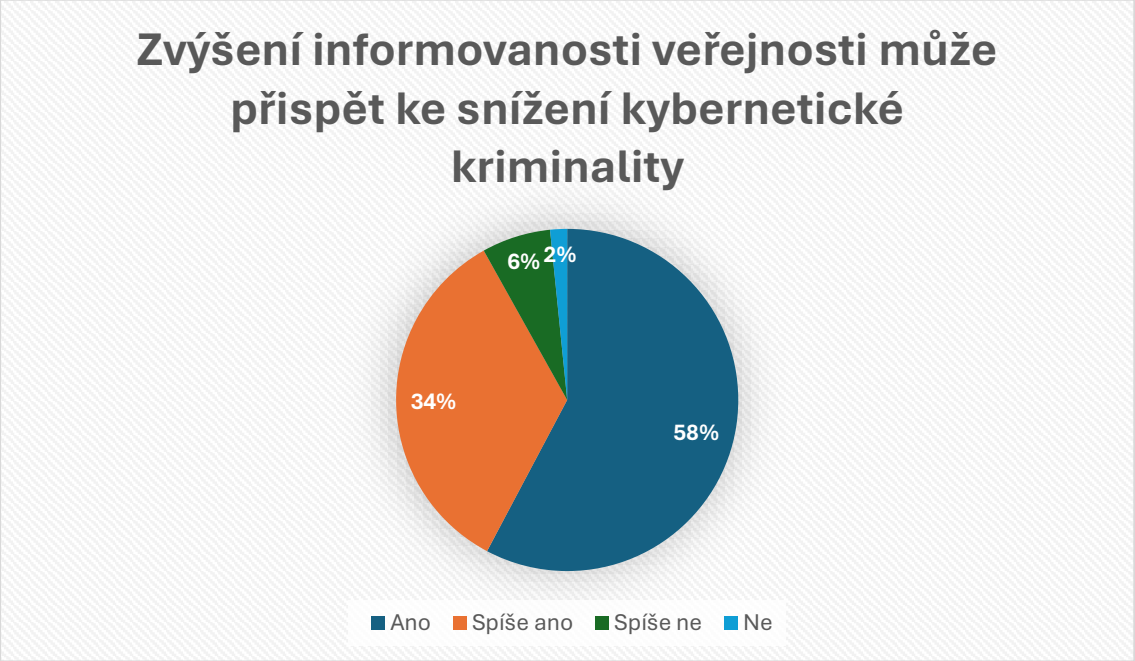
Z vyjádření účastníků šetření je patrné, že někteří mají pocit, že informace, se kterými se běžně setkávají, nejsou vždy dostatečné nebo dostatečně srozumitelné. Často může chybět praktické vysvětlení nebo konkrétní rady, jak v určitých situacích postupovat. Někdy se navíc potřebné poznatky k veřejnosti dostávají až ve chvíli, kdy již došlo k nějakému problému.

Tento pohled naznačuje, že preventivní aktivity by neměly být zaměřeny pouze na upozorňování na existenci rizik, ale také na poskytování jasných a praktických doporučení, která mohou uživatelům pomoci chovat se v online prostředí bezpečněji.

[81] Vlastní zpracování

Většina účastníků šetření se zároveň domnívá, že zvyšování informovanosti veřejnosti může přispět ke snížení kybernetické kriminality (58 %). Tento názor odpovídá závěrům uvedeným v teoretické části práce, kde je informovanost zdůrazňována jako jeden z důležitých nástrojů prevence.

Graf č. 15 Zvýšení informovanosti veřejnosti může přispět ke snížení kybernetické kriminality[82]



Z vyjádření dotázaných je patrné, že si uvědomují význam prevence a nevnímají kybernetickou bezpečnost pouze jako technickou oblast určenou odborníkům. Uvědomují si, že se jedná o téma, které se týká každého uživatele internetu. Mnozí z nich zastávají názor, že vyšší míra informovanosti může pomoci předejít zbytečným chybám, které často vedou k podvodům, úniku osobních údajů nebo jiným nepříjemným situacím.

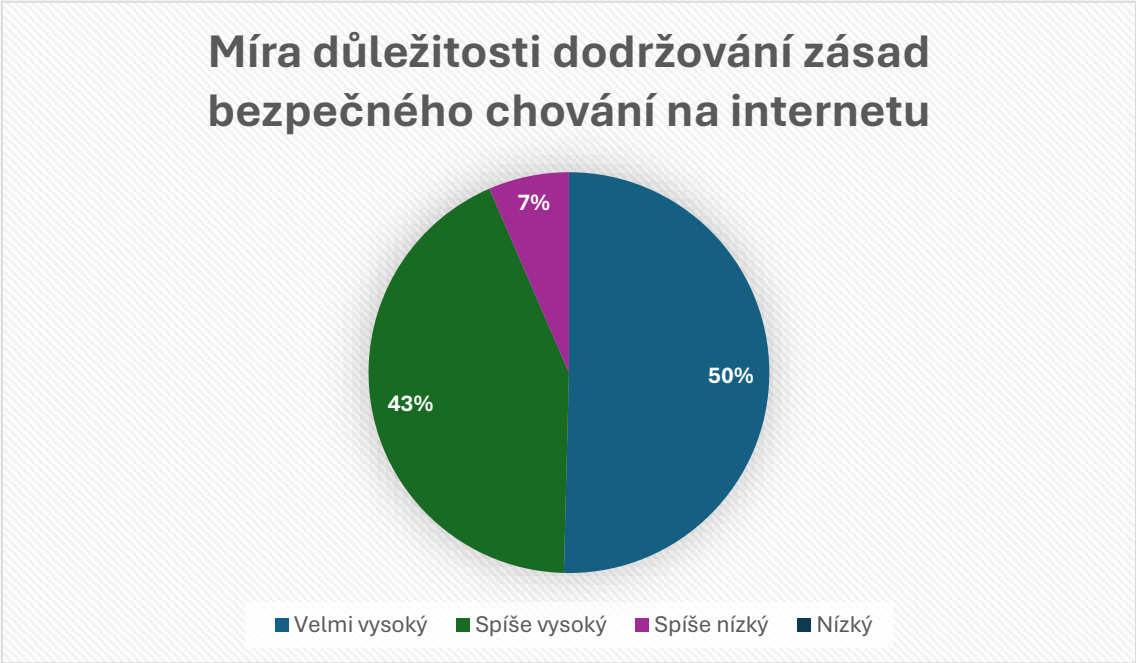
Zároveň však zjištění naznačují, že samotné získání informací nemusí být dostačující. Důležitou roli hraje také ochota jednotlivců své chování skutečně změnit a uplatňovat získané poznatky v praxi. Bez aktivního přístupu a větší obezřetnosti při používání internetu totiž ani dobrá informovanost nemusí automaticky znamenat vyšší úroveň bezpečnosti.

[82] Vlastní zpracování

Z hlediska vnímání důležitosti dodržování zásad bezpečného chování na internetu většina dotázaných uvedla, že tyto zásady považuje za velmi důležité (50 %) nebo spíše důležité. (43 %) Pouze menší část respondentů hodnotila jejich význam jako spíše nízký. (7 %) Z výsledků dále vyplývá, že žádný z respondentů neoznačil míru důležitost dodržování zásad bezpečného chování na internetu jako nízkou.

Tento výsledek naznačuje, že si většina účastníků šetření uvědomuje význam bezpečného chování při používání internetu a vnímá ho jako důležitý prvek ochrany osobních údajů a online účtů. Přestože se mohou jednotliví uživatelé lišit v konkrétních bezpečnostních návycích, obecné povědomí o důležitosti dodržování těchto zásad je mezi respondenty poměrně vysoké.

Graf č. 16 Míra důležitosti dodržování zásad bezpečného chování na internetu[83]



Z odpovědí vyplývá, že si lidé uvědomují, že bezpečné chování na internetu není pouze formální doporučení, ale faktor, který může mít přímý dopad na jejich vlastní bezpečnost. Vnímají, že každodenní rozhodnutí – například jaké heslo používají nebo jak reagují na podezřelé zprávy – mohou ovlivnit míru rizika, kterému jsou vystaveni.

Ochota upravovat své návyky na základě nových informací zároveň naznačuje, že preventivní působení může být účinné. Pokud jsou informace podávány srozumitelně, konkrétně a s praktickými příklady, lidé jsou více nakloněni tomu své chování skutečně

[83] Vlastní zpracování

změnit. Může jít například o důslednější ochranu účtů, větší obezřetnost při komunikaci s neznámými osobami nebo pečlivější zacházení s osobními údaji.

Z odpovědí respondentů dále vyplývá, že většina z nich považuje dodržování zásad bezpečného chování na internetu za velmi důležité (41 %) nebo spíše důležité (51 %). Tyto výsledky naznačují otevřenost vůči vzdělávání a preventivním opatřením, což představuje pozitivní předpoklad pro snižování rizik spojených s kybernetickou kriminalitou.

Graf č. 17 Ochoten/ochotna změnit své chování na internetu na základě nových informací o kybernetických hrozbách[84]

Z vyjádření respondentů je patrné, že bezpečné chování na internetu nevnímají pouze jako obecné doporučení, ale jako oblast, která se jich osobně dotýká. Uvědomují si, že jejich vlastní přístup může ovlivnit míru rizika, kterému jsou vystaveni. Ochota přizpůsobit své online návyky zároveň naznačuje, že pokud jsou informace podávány srozumitelně, konkrétně a s praktickými příklady, mohou mít skutečný vliv na každodenní jednání uživatelů.

Takový přístup může sehrát významnou roli v prevenci kybernetických incidentů, zejména u běžných uživatelů, kteří nemají odborné znalosti v oblasti kybernetické bezpečnosti. Právě u této skupiny může být kombinace informovanosti a praktických doporučení klíčem ke snížení rizika a bezpečnějšímu pohybu v online prostředí.

[84] Vlastní zpracování

8.3.5 Názory respondentů na opatření ke zvýšení bezpečnosti uživatelů internetu

Součástí dotazníku byla také otevřená otázka, ve které mohli účastníci šetření uvést vlastní názor na to, jaká opatření by podle nich nejvíce přispěla ke zvýšení bezpečnosti běžných uživatelů internetu. Odpovědělo na ni 71 dotázaných. Jejich vyjádření byla poměrně různorodá a nabídla doplňující pohled na to, jak lidé tuto problematiku vnímají z praktického hlediska.

Nejčastěji zmiňovaným opatřením bylo používání silných a jedinečných hesel. Řada účastníků upozorňovala na to, že slabá nebo opakovaně používaná hesla představují významné riziko pro ochranu online účtů. Tento názor navíc odpovídá zjištěním z předchozí části dotazníku, která naznačila, že správa hesel není u všech uživatelů dostatečná.

Další skupina odpovědí se týkala potřeby lepší a srozumitelnější informovanosti. Respondenti uváděli, že by ocenili více praktických příkladů, konkrétních situací a jasných doporučení, jak se v rizikových situacích zachovat. Někteří navrhovali také pravidelná upozornění prostřednictvím e-mailu nebo SMS zpráv, která by informovala o aktuálních podvodech či nových formách útoků.

Zajímavé je, že část respondentů zdůrazňovala také odpovědnost poskytovatelů online služeb. Podle jejich názoru by měla být ochrana nastavena co nejjednodušeji a pokud možno automaticky, aby nebyla závislá pouze na aktivitě samotných uživatelů. Tento pohled ukazuje, že lidé očekávají určitou míru zabezpečení také ze strany provozovatelů internetových platforem.

Menší část dotázaných uvedla, že si konkrétní opatření nedokáže představit nebo si v této oblasti není jistá. To může naznačovat, že někteří uživatelé nemají dostatečný přehled o možnostech, jak svou ochranu na internetu zvýšit.

Celkově otevřené odpovědi potvrzují, že vyšší úroveň bezpečnosti nelze zajistit pouze jedním opatřením. Důležitá je kombinace technických nástrojů, odpovědného přístupu uživatelů i kvalitní a srozumitelné informovanosti. Zároveň je zřejmé, že dotázaní vnímají kybernetickou bezpečnost jako téma, které se bezprostředně dotýká jejich každodenního života.

8.4 Diskuse výsledků

Tato kapitola shrnuje výsledky dotazníkového šetření a zasazuje je do kontextu teoretických poznatků uvedených v předchozí části práce. Cílem bylo zhodnotit úroveň informovanosti respondentů o kybernetických hrozbách, posoudit, jak se tyto poznatky promítají do jejich chování na internetu, a vymezit význam informovanosti z hlediska prevence kybernetické kriminality.

Analýza odpovědí ukázala, že většina dotázaných se s pojmem kybernetická hrozba již setkala a má alespoň základní přehled o této problematice. Tato skutečnost pravděpodobně souvisí s častější medializací kybernetických útoků i jejich přítomností ve veřejném prostoru. Samotná znalost pojmu však ještě neznamená hlubší porozumění jednotlivým typům rizik ani jejich konkrétním dopadům.

Rozdíly v informovanosti se nejvíce projevily při znalosti konkrétních forem útoků. Pojmy jako kyberšikana nebo krádež identity byly většině respondentů známé, zatímco techničtější označení, například ransomware, znala pouze menší část dotázaných. Lze tedy předpokládat, že veřejnost má lepší přehled o hrozbách, které jsou více medializované nebo které si lidé dokážou spojit s běžnou zkušeností, zatímco složitější formy útoků zůstávají méně srozumitelné.

Významným zjištěním je také skutečnost, že část respondentů má osobní zkušenost s některou formou kybernetického útoku, nejčastěji s podvodnou komunikací. To potvrzuje, že kybernetická kriminalita nepředstavuje pouze teoretický problém, ale reálné riziko, které se dotýká běžných uživatelů internetu. Negativní zkušenost přitom může posílit obezřetnost a motivovat ke změně chování v online prostředí.

Současně se však ukázal určitý nesoulad mezi deklarovaným významem bezpečnosti a skutečnou praxí. Typickým příkladem je používání stejných hesel pro více služeb nebo jejich nepravidelná změna. Přestože si respondenti možná rizika uvědomují, v každodenním fungování často volí pohodlnější řešení. To naznačuje, že teoretické znalosti samy o sobě nezaručují odpovědné chování a že klíčovou roli hraje dlouhodobá změna návyků.

Pozitivně lze hodnotit poměrně časté využívání některých bezpečnostních opatření, například dvoufázového ověřování. Naopak nižší využívání správců hesel může souviset s jejich menší známostí nebo obavami z jejich složitosti. I zde se tedy nabízí prostor pro lepší vysvětlení jejich funkce a praktických přínosů.

Dotázaní rovněž vyjádřili názor, že úroveň informovanosti veřejnosti není dostatečná a že její posílení by mohlo přispět ke snížení výskytu kybernetické kriminality. Tento postoj odpovídá teoretickým poznatkům, které zdůrazňují význam prevence a vzdělávání. Odpovědi na otevřenou otázku navíc ukázaly, že bezpečnost je vnímána jako společná odpovědnost uživatelů i poskytovatelů online služeb.

Je však třeba uvést, že dotazníkové šetření bylo realizováno na omezeném vzorku respondentů, a získané výsledky proto nelze zobecnit na celou populaci.

8.5 Návrhy a doporučení

Na základě provedeného dotazníkového šetření a jeho následné interpretace lze definovat několik doporučení, která by mohla přispět ke zvýšení úrovně kybernetické bezpečnosti běžných uživatelů internetu. Z provedené analýzy je patrné, že informovanost o kybernetických hrozbách sice existuje, ale vždy ne však se promítá do důsledného dodržování zásad bezpečného chování.

Jedním z hlavních doporučení je zaměřit se více na praktickou a srozumitelnou osvětu. Řada respondentů si uvědomuje význam obezřetného chování na internetu, nejsou si však vždy jisti, jak konkrétně postupovat v běžných situacích. Preventivní aktivity by proto měly obsahovat konkrétní příklady z praxe, například jak rozpoznat podvodný e-mail, falešnou internetovou stránku nebo podezřelou zprávu na sociálních sítích. Právě konkrétní situace mohou uživatelům pomoci lépe pochopit rizika a správně na ně reagovat.

Dalším důležitým krokem je zjednodušení bezpečnostních opatření. Zjištění naznačují, že některé nástroje, například správci hesel, nejsou mezi uživateli dostatečně rozšířené. Část lidí je může vnímat jako složité nebo nerozumí jejich přínosům. Poskytovatelé online služeb by proto měli usilovat o co největší uživatelskou přívětivost a jasné vysvětlení funkcí, které mají přispět ke zvýšení bezpečnosti.

Z odpovědí dotázaných rovněž vyplývá očekávání, že bezpečnost nebude záviset pouze na jejich vlastní aktivitě. Ochranné prvky by měly být nastaveny jako výchozí možnost a neměly by vyžadovat složité manuální nastavení. Automatická upozornění na podezřelé přihlášení, doporučení ke změně hesla nebo jednoduchá vysvětlení rizik přímo v prostředí konkrétní služby mohou významně přispět ke snížení počtu bezpečnostních incidentů.

Významnou roli mohou sehrát také vzdělávací instituce. Zařazení základů kybernetické bezpečnosti do výuky může pomoci vytvářet správné návyky již od mladého věku. Důležité je zaměřit se nejen na technické aspekty, ale především na situace, se kterými se mladí lidé běžně setkávají, například při používání sociálních sítí či online komunikaci.

Podobně může přispět i vzdělávání v pracovním prostředí. Pravidelná a stručná školení zaměřená na aktuální hrozby mohou zaměstnance vést k větší obezřetnosti. Tyto poznatky si navíc často přenášejí i do svého soukromého života.

V neposlední řadě je vhodné využívat moderní komunikační kanály k šíření informací o aktuálních rizicích. Krátká a srozumitelná upozornění, praktické tipy nebo jednoduché návody sdílené prostřednictvím sociálních sítí, mobilních aplikací či webových stránek mohou oslovit široké spektrum uživatelů. Klíčová je především přehlednost a aktuálnost sdělení.

Z provedeného šetření vyplývá, že efektivní posilování kybernetické bezpečnosti by mělo stát na propojení vzdělávání, vhodně nastavených technických nástrojů a aktivní role institucí i poskytovatelů online služeb. Zjištění zároveň naznačují, že lidé jsou otevřeni změnám svého chování, pokud jsou jim informace předávány jasně, konkrétně a srozumitelným způsobem. Budoucí preventivní aktivity by proto měly klást důraz především na praktickou a dobře uchopitelnou formu osvěty.

Závěr

Cílem této bakalářské práce bylo poukázat na význam informovanosti veřejnosti o kybernetických hrozbách jako jednoho z nástrojů prevence kriminality v digitálním prostředí. Práce propojila teoretické vymezení problematiky s praktickým zjištěním úrovně informovanosti a chování běžných uživatelů internetu.

V teoretické části byly stanoveny základní pojmy, typy kybernetických hrozeb a jejich dopady, a zároveň byly představeny principy prevence i právní rámec kybernetické bezpečnosti. Praktická část pak ukázala, že základní povědomí o kybernetických hrozbách je mezi respondenty poměrně rozšířené, avšak hloubka znalostí i jejich promítnutí do praxe se výrazně liší.

Výzkum potvrdil, že mnoho uživatelů má osobní zkušenost s kybernetickým útokem, zejména s podvodnou komunikací. Přestože si většina respondentů uvědomuje rizika spojená s online prostředím, jejich každodenní chování ne vždy odpovídá doporučeným bezpečnostním zásadám. Zjištění tak poukazují na rozdíl mezi deklarovanými postoji a skutečnou praxí.

Zvyšování úrovně kybernetické bezpečnosti by proto mělo vycházet z propojení vzdělávání, prakticky zaměřené osvěty a vhodně nastavených technických opatření. Výsledky práce zároveň naznačují, že uživatelé jsou otevřeni změnám svého chování, pokud mají k dispozici jasné, konkrétní a srozumitelné informace.

Lze tedy shrnout, že informovanost veřejnosti představuje významný, nikoli však jediný předpoklad účinné prevence kybernetické kriminality. Největšího efektu lze dosáhnout tehdy, pokud jsou znalosti systematicky podporovány rozvojem bezpečnostních návyků a odpovědným přístupem jak ze strany jednotlivců, tak i institucí.

Seznam použitých zdrojů

Literární zdroje

1. ANDRAŠKO, J., MESARČÍK M., a SOKOL P. Právo kybernetickej bezpečnosti. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. s. 194. ISBN 978-80-7160-632-1.
2. ČERNÁ A., (ED.); LENKA, D., HANA, M., ANNA, Š. a DAVID, Š. Kyberšikana: Průvodce novým fenoménem. Grada Publishing a.s, 2013. s. 152. ISBN 978-80-247-8846-3.
3. INSTITUT PRO KRIMINOLOGII A SOCIÁLNÍ PREVENCI V PRAZE. Škody působené kybernetickou kriminalitou. Praha: IKSP, 2019. s. 106. ISBN 978-80-7338-175-2
4. KOLOUCH, J. a BAŠTA, P. CyberSecurity. CZ.NIC. Praha: CZ.NIC, 2019. s. 560. ISBN 978-80-88168-31-7.
5. KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. s. 526. ISBN 978-80-88168-15-7
6. KOŽÍŠEK, M., a PÍSECKÝ V. Bezpečně na internetu: průvodce chováním ve světě online. Grada Publishing a.s, 2016. s. 176. ISBN 978-80-271-9074-4.
7. KRÁL, M. Bezpečný internet: Chraňte sebe i svůj počítač. Grada Publishing a.s, 2015. s. 184. ISBN 978-80-247-9821-9.
8. KUDRLOVÁ, K., PALOUŠOVÁ, V. a VLACH, J. Kyberkriminalita z pohledu justiční praxe a každodenních uživatelů. Vydání: první. Studie. Praha: Institut pro kriminologii a sociální prevenci, 2023. s. 212. ISBN 978-80-7338-204-9.
9. MARTIN, D. Systém managementu bezpečnosti informací. Grada Publishing a.s, 2011. s. 128. ISBN 978-80-247-7616-3.
10. PETROWSKI, T., Bezpečí na internetu: pro všechny. Přeložil Tomáš KURKA. Tajemství. Liberec: Dialog, 2014. s. 244. ISBN 978-80-7424-066-9.
11. SAK, P. Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva. Petrklíč, 2018. s. 272. ISBN 978-80-7229-793-1.

12. SARRI, A. a ARCUS, R. Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies. 2021. s. 53. ISBN 978-92-9204-544-9.
13. SHAW, M. Handbook on the Crime Prevention Guidelines: Making Them Work. Criminal Justice Handbook, 2010. s. 124. ISBN 978-92-1-130300-1.
14. SMEJKAL, V.; SOKOL, T. a KODL, J. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. s. 378. ISBN 978-80-7380-765-8.
15. VLACH, J., KUDRLOVÁ, K. a PALOUŠOVÁ, V. Kyberkriminalita v kriminologické perspektivě. Vydání: první. Studie. Praha: Institut pro kriminologii a sociální prevenci, 2020. s. 146. ISBN 978-80-7338-189-9.

Elektronické zdroje

1. BRESNAHAN, E. How Digital Transformation Impacts IT And Cyber Risk Programs [online]. CyberSaint Security, [cit. 4. 1. 2026]. Dostupné z: https://www.cybersaint.io/blog/managing-risk-in-digital-transformation
2. KRÁLOVÁ, M. Kybernetické hrozby a jak se před nimi chránit [online]. CDC Data, 27. 3. 2023 [cit. 4. 1. 2026]. Dostupné z: https://www.cdc.cz/cs/kyberneticke-hrozby-a-jak-se-pred-nimi-chranit/
3. EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA Threat Landscape 2025 [online]. 1. October 2025 [cit. 4. 1. 2026]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
4. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Kybernetická bezpečnost, kybernetická kriminalita a AI [online]. 9. 4. 2025 [cit. 12. 1. 2026]. Dostupné z: https://www.kybersoutez.cz/finale2025/MV.pdf
5. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Strategický rámec prevence kriminality v České republice na období 2021–2025 [online]. Praha: Ministerstvo vnitra ČR, 2021 [cit. 2026-02-25]. Dostupné z: https://www.mvcr.cz
6. BADA, M. a JASON R. C. Nurse. The Social and Psychological Impact of Cyber-Attacks [online]. 29 9 2019 [cit. 12. 1. 2026]. Dostupné z: https://arxiv.org/pdf/1909.13256.pdf

7. DONNELLY, M. Social Impacts of Cyber Crime [online]. 2023 [cit. 12. 1. 2026]. Dostupné z: https://www.ebsco.com/research-starters/computer-science/social-impacts-cyber-crime
8. ŠVESTKOVÁ, R., SOLDÁN L. a ŘEHKA M. Kyberšikana [online]. České Budějovice: ZSF JU, 2019. 7. kapitola. ISBN 978-80-7394-752-1. Dostupné z: https://publi.cz/books/5555/index.html#7-kyberneticka-sikana
9. BEZPEČNOST A OCHRANA ZDRAVÍ ŠKOLNÍ MLÁDEŽE PŘI POUŽÍVÁNÍ DIGITÁLNÍCH TECHNOLOGIÍ — Kyberšikana a její dopady [online]. [s.l.]: Výzkumný ústav bezpečnosti práce, v. v. i., [n.d.] [cit. 15. 1. 2026]. Dostupné z: https://skoly.vubp.cz/soubory/boz-skolni-mladeze-pri-pouzivani-digitalnich-technologii-kybersikana-a-jeji-dopady.pdf
10. IPSOS. Češi a kybernetické hrozby [online]. 18. 7. 2024 [cit. 21. 1. 2026]. Dostupné z: https://www.ipsos.com/cs-z/cesi-kyberneticke-hrozby
11. RAMA, P. a M. KEEVY. Public cybersecurity awareness good practices on government-led websites [online]. International Journal of Research in Business and Social Science, 2023, roč. 12, č. 7, s. 94–104 [cit. 21. 1. 2026]. Dostupné z: https://www.researchgate.net/publication/375096855_Public_cybersecurity_awareness_good_practices_on_government-led_websites
12. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Národní strategie kybernetické bezpečnosti České republiky na období 2020–2025. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2020. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf
13. ANAZHI, A. H. I. a M. A. Osman. Cyber Security Awareness on Social Media: Knowledge Sharing Among Orang Asli Students [online]. Journal of Information Security, 2023, roč. 14, č. 4, s. 211–220 [cit. 21. 1. 2026]. Dostupné z: https://www.researchgate.net/publication/391495892_Cyber_Security_Awareness_on_Social_Media_Knowledge_Sharing_Among_Orang_Asli_Students
14. PREVENCE KRIMINALITY. Kybernetická kriminalita – prevence kriminality [online]. Prevence kriminality – Ministerstvo vnitra ČR, 2026. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/

15. ČESKO. *Zákon č. 264/2024 Sb., o kybernetické bezpečnosti.* Sbírka zákonů České republiky [online]. 2025, částka 264. [cit. 2025-02-22]. Dostupné z: https://www.e-sbirka.cz/sb/2025/264?zalozka=text

Legislativní dokumenty

1. Zpracování osobních údajů: nový zákon o zpracování osobních údajů a další právní předpisy. GDPR: obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů: redakční uzávěrka 1.5.2019. ÚZ: úplné znění. Ostrava: Sagit, [2019]. ISBN 978-80-7488-353-8.

Ostatní zdroje

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Národní strategie kybernetické bezpečnosti České republiky na období 2020–2025. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2020. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). National Capabilities Assessment Framework. [PDF]. Heraklion: ENISA, 2020. ISBN 978-92-9204-473-2. Dostupné z: https://www.enisa.europa.eu/sites/default/files/all_files/National%20Capabilities%20Assessment%20Framework_CS.pdf

Seznam zkratek

AI – Artificial Intelligence (umělá inteligence)

ČR – Česká republika

ENISA – European Union Agency for Cybersecurity (Agentura Evropské unie pro kybernetickou bezpečnost)

EU – Evropská unie

GDPR – General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)

ICT – Information and Communication Technologies (informační a komunikační technologie)

IKSP – Institut pro kriminologii a sociální prevenci

ISMS – Information Security Management System (Systém managementu bezpečnosti informací)

IT – Information Technology (informační technologie)

MV – Ministerstvo vnitra

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OSN – Organizace spojených národů

SMS – Short Message Service (textová zpráva)

ZSF JU – Zdravotně sociální fakulta Jihočeské univerzity

Seznam tabulek a grafů

Seznam příloh

Přílohy

Příloha – Dotazník

Dobrý den, jsem studentem 3. ročníku vysoké školy a v rámci zpracování své bakalářské práce se zabývám problematikou informovanosti veřejnosti o kybernetických hrozbách jako nástroj prevence kriminality.

Hlavním cílem tohoto dotazníku je zjistit úroveň znalostí běžných uživatelů internetu v oblasti kybernetických hrozeb a jejich ochotu dodržovat zásady bezpečného chování v online prostředí. Dotazník je určen široké veřejnosti, zejména studentům, dospělým a seniorům, kteří internet běžně využívají.

Vyplnění dotazníku je zcela anonymní a získaná data budou použita výhradně pro studijní účely při zpracování bakalářské práce.

Předem děkuji Vám za Váš čas a ochotu.

S pozdravem,

Tomáš Provazník, DiS.

1. Do které věkové skupiny patříte?

a) do 18 let

b) 18-26 let

c) 27-45 let

d) 46-64 let

e) 65 let a více

2. Jak často používáte internet?

a) Denně

b) Několikrát týdně

c) Zřídka

d) Téměř vůbec

3. K čemu internet nejčastěji využíváte? (možno zvolit více odpovědí)

a) Komunikace (e-mail, sociální sítě)

b) Studium / Práce

c) Online nákupy

d) Internetové bankovnictví

e) Zábava (videa, hry, filmy)

4. Jak hodnotíte své znalosti v oblasti kybernetických hrozeb?

a) Velmi dobře

b) Spíše dobré

c) Spíše nedostatečné

d) Nedostatečné

5. Setkal/a jste se s pojmem „kybernetická hrozba“?

a) Ano

b) Ne

6. Které z následujících pojmů znáte? (možno zvolit více odpovědí)

a) Phishing

b) Malware

c) Ransomware

d) Krádež identity

e) Kyberšikana

f) Žádný z uvedených

7. Domníváte se, že běžný uživatel internetu může být ohrožen kybernetickou kriminalitou?

a) Ano

b) Spíše ano

c) Spíše ne

d) Ne

8. Setkal/a jste se osobně s některou formou kybernetického útoku nebo podvodu?

a) Ano

b) Ne

9. S jakým typem kybernetického útoku nebo podvodu jste se setkal/a? (v případě, že jste se s žádným nesetkal/a, zvolte odpověď „nesetkal/a jsem se“)

a) Podvodný e-mail / zpráva

b) Napadení účtu

c) Zneužití osobních údajů

d) Jiný typ

e) Nesetkal/a jsem se s žádným kybernetickým útokem ani podvodem

10. Používáte stejné heslo pro více online služeb?

a) Ano

b) Spíše ano

c) Spíše ne

d) Ne

11. Jak často měníte svá hesla?

a) Pravidelně

b) Občas

c) Výjimečně

d) Nikdy

12. Využíváte následující bezpečnostní opatření? (možno zvolit více odpovědí)

a) Dvoufázové ověření

b) Antivirový program

c) Správce hesel

d) Pravidelné zálohování dat

e) Žádné z uvedených

13. Z jakých zdrojů nejčastěji získáváte informace o kybernetických hrozbách?

a) Média

b) Vzdělávací instituce

c) Zaměstnání

d) Rodina / Známí

e) Žádné z uvedených

14. Považujete úroveň informovanosti veřejnosti o kybernetických hrozbách za dostatečnou?

a) Ano

b) Spíše ano

c) Spíše ne

d) Ne

15. Domníváte se, že zvyšování informovanosti veřejnosti může přispět ke snížení kybernetické kriminality?

a) Ano

b) Spíše ano

c) Spíše ne

d) Ne

16. Do jaké míry považujete dodržování zásad bezpečného chování na internetu za důležité?

a) Velmi vysoký

b) Spíše vysoký

c) Spíše nízký

d) Nízký

17. Byl/a byste ochoten/ochotna změnit své chování na internetu na základě nových informací o kybernetických hrozbách?

a) Ano

b) Spíše ano

c) Spíše ne

d) Ne

18. Jaká opatření by podle vašeho názoru nejvíce přispěla ke zvýšení bezpečnosti běžných uživatelů internetu?

Otevřená otázka