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

BAKALÁŘSKÁ PRÁCE

POSTUP POLICIE ČESKÉ REPUBLIKY PŘI PROVĚŘOVÁNÍ OZNÁMENÍ O PODVODNÝCH E-SHOPECH

Autor práce: Daniel Šafránek, 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: Daniel Šafránek

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Postup Policie České republiky při prověřování oznámení o podvodných e-shopech

Název bakalářské práce v anglickém jazyce: Procedure of the Police of the Czech Republic in Investigating Reports of Fraudulent E-shops

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

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

Cíl bakalářské práce:

Hlavním cílem práce je posoudit postup Policie České republiky při prověřování oznámení týkajících se podvodných e-shopů, a to se zaměřením na jednotlivé fáze policejního procesu od přijetí oznámení až po případné zahájení trestního řízení a vedení prověřování.

Vedlejším cílem práce je zhodnotit úroveň povědomí uživatelů internetu o bezpečném chování při nákupu na e-shopech, identifikovat rizikové faktory, které jsou veřejností často přehlíženy, a navrhnout opatření směřující k minimalizaci těchto rizik.

Student: Daniel Šafránek, DiS.	31.12.2025 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	5.1.2026 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	22.1.2026 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	27.1.2026 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	1.2.2026 *datum*	*podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval 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 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 bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

ŠAFRÁNEK, D. Postup Police České republiky při prověřování o podvodných e-shopech. České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 70 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: kybernetická kriminalita, podvodné e-shopy, Policie České republiky, trestní řízení, prevence

Bakalářská práce se zabývá problematikou podvodných e-shopů jako formy kybernetické kriminality a postupem Policie České republiky při prověřování oznámení o této trestné činnosti. Cílem práce je popsat procesní postup od přijetí trestního oznámení až po rozhodnutí v rámci prověřování a poukázat na specifika těchto případů v online prostředí.

Práce vymezuje základní pojmy, charakterizuje formy kybernetické kriminality a přibližuje mechanismy fungování podvodných e-shopů. Dále se zaměřuje na jednotlivé úkony Policie ČR při prověřování, včetně zajišťování důkazů a práce s poškozenými. Součástí je také analýza vybraných případů a zdůraznění významu prevence v oblasti bezpečného chování na internetu.

ABSTRACT

ŠAFRÁNEK, D. Procedure of the Police of the Czech Republic in Investigating Reports of Fraudulent E-shops. České Budějovice: The College European and Regiolan Studies, 2026. 70 pgs. Supervisor: RNDr. Růžena Ferebauerová

Keywords: cybercrime, fraudulent e-shops, Police of the Czech Republic, criminal proceedings, prevention

This bachelor's thesis addresses the issue of fraudulent e-shops as a form of cybercrime and the procedures of the Police of the Czech Republic when investigating reports of such criminal activity. The aim of the thesis is to describe the procedural steps from the receipt of a criminal complaint to the final decision within the investigation phase, while highlighting the specifics of these cases in the online environment.

The work defines fundamental concepts, characterizes various forms of cybercrime, and explains the operational mechanisms of fraudulent e-shops. Furthermore, it focuses on the individual actions taken by the Police of the Czech Republic during the investigation, including the securing of evidence and communication with victims. The thesis also includes an analysis of selected cases and emphasizes the importance of prevention in the context of safe online behavior.

Obsah

Úvod

Dynamický rozvoj informačních a komunikačních technologií v posledních dvou desetiletích zásadně proměnil podobu moderní společnosti. Internet přestal být pouhým zdrojem informací a stal se integrální součástí každodenního života, ovlivňující způsob, jakým komunikujeme, pracujeme a v neposlední řadě i jak nakupujeme. Rozmach e-commerce sektoru, který byl ještě více urychlen globální pandemií onemocnění COVID-19, přinesl spotřebitelům nesporné výhody v podobě pohodlí, širokého výběru a možnosti snadného srovnání cen. Souběžně s tímto pozitivním trendem se však do kybernetického prostoru přesunula i značná část kriminálních aktivit. Tradiční formy majetkové trestné činnosti jsou stále častěji nahrazovány sofistikovanými metodami v online prostředí, mezi nimiž zaujímají přední místo podvodné e-shopy.

Problematika podvodných e-shopů představuje pro současné orgány vynucující právo jednu z největších výzev. Pachatelé v tomto prostředí využívají anonymity internetu, nízkých nákladů na vytvoření vizuálně přesvědčivých stránek a často i přeshraničního charakteru sítě, což značně komplikuje jejich odhalování a následné usvědčování. Pro Policii České republiky to znamená nutnost neustálé adaptace procesních postupů, technického vybavení i odborných znalostí policistů. Efektivita postupu policie při prověřování oznámení o těchto podvodech je klíčová nejen pro ochranu majetku občanů, ale také pro zachování důvěry veřejnosti v právní systém. Bakalářská práce se zaměřuje na analýzu činnosti Policie České republiky v souvislosti s fenoménem podvodného prodeje zboží a služeb na internetu.

Hlavním tématem je procesní cesta, kterou musí každé podané oznámení urazit. Od momentu, kdy se poškozený dostaví na služebnu nebo podá elektronické oznámení, přes fázi vytěžování informací a zajišťování digitálních stop, až po rozhodnutí o zahájení úkonů trestního řízení podle trestního řádu.

Kromě represivní složky, tedy postupu policie, je však nezbytné nahlížet na problematiku i z pohledu prevence. Kriminalita v prostředí e-shopů totiž velmi často těží z nízké úrovně digitální gramotnosti a určité míry naivity nebo nepozornosti uživatelů. Ačkoliv jsou bezpečnostní varování a osvětové kampaně v médiích relativně časté, počet obětí podvodů neklesá, ba naopak. To naznačuje, že existuje propast mezi dostupnými informacemi o bezpečném nákupu a jejich reálnou aplikací v praxi. Proto se tato práce věnuje také analýze chování spotřebitelů a identifikaci rizikových faktorů, které vedou k úspěšnému dokončení podvodu ze strany pachatele.

Z hlediska metodologie bude práce vycházet z kombinace teoretických a praktických přístupů. V teoretické části bude provedena rešerše odborné literatury a relevantních právních předpisů, se kterými Policie České republiky při šetření těchto činů pracuje. Praktická část bude opřena o analýzu dostupných statistických dat o kybernetické kriminalitě a o kvantitativní šetření zaměřené na spotřebitelské chování. V neposlední řadě budou využity poznatky z kazuistik, které ilustrují typické postupy a obtíže v policejní praxi. Struktura práce je rozdělena do několika logických celků. První kapitoly definují základní pojmy. Následující část je věnována samotnému procesnímu postupu Policie České republiky. Závěrečné kapitoly se zaměřují na prevenci, vyhodnocení provedeného šetření a návrhy opatření pro minimalizaci rizik spojených s nákupy v podvodných e-shopech.

1 Cíl a metodika bakalářské práce

Tato kapitola definuje záměry bakalářské práce a popisuje konkrétní kroky, postupy a nástroje, které budou využity k naplnění stanovených cílů. Metodika je rozdělena na teoretickou část, založenou na literární rešerši, a praktickou část, využívající kvantitativní i kvalitativní výzkum.

1.1 Cíle práce

Hlavním cílem bakalářské práce je analýza a posouzení postupu Policie České republiky při prověřování oznámení o podvodných e-shopech. Práce se zaměřuje na procesní kroky od přijetí trestního oznámení až po případné zahájení trestního stíhání, se zvláštním zřetelem na specifika kybernetické kriminality v českém právním prostředí.

Vedlejší cíle práce jsou stanoveny následovně:

- Zhodnotit úroveň povědomí běžných uživatelů internetu o bezpečnostních prvcích a rizicích spojených s online nakupováním.
- Identifikovat nejčastější rizikové faktory a chyby, kterých se spotřebitelé dopouštějí a které vedou k úspěšnému dokončení podvodu.
- Navrhnout doporučení a preventivní opatření pro veřejnost i orgány činné v trestním řízení směřující k efektivnější ochraně spotřebitele a eliminaci rizik.

1.2 Charakteristika objektu zkoumání

Objektem zkoumání v teoretické rovině je procesní postup Policie České republiky (především služby kriminální policie a vyšetřování) v souladu se zákonem číslo 141/1961 Sb., o trestním řízení soudním. V praktické rovině jsou objektem zkoumání aktivní uživatelé internetu v ČR a konkrétní kazuistiky podvodného jednání v kyberprostoru.

1.3 Pracovní postupy a použité metody

Pro naplnění cílů práce budou využity následující vědecké metody:

- Analýza a syntéza: Rozbor právní úpravy a odborné literatury zabývající se kyberkriminalitou.
- Komparace: Srovnání teoretických postupů s reálnou praxí popsanou v případových studiích.

1.4 Metody vyhodnocení a interpretace výsledků

Data získaná z dotazníkového šetření budou zpracována pomocí metod popisné statistiky. Výsledky budou interpretovány prostřednictvím tabulek a grafů (koláčové, sloupcové), které umožní vizualizaci míry povědomí o kybernetických hrozbách.

U případových studií bude využita metoda interpretativní analýzy, která bude zaměřena na identifikaci "modus operandi" pachatelů a kritických míst v postupu policie. V závěru práce dojde ke konfrontaci zjištěných dat s teoretickými předpoklady a budou stanovena doporučení pro praxi.

2 Vymezení základních pojmů

Pro snazší proniknutí do problematiky kybernetické kriminality je nejprve potřeba vymezit některé ze základních pojmů, které se k této oblasti trestné činnosti pojí. Jedná se o pojmy, jejichž pochopení a vymezení je ve vztahu k předmětu následujícího textu nezbytné. Zároveň se však nejedná o vyčerpávající výčet všech pojmů, jejichž definice lze nalézt například ve Výkladovém slovníku kybernetické bezpečnosti vydaném pod záštitou Národního bezpečnostního úřadu a Národního centra kybernetické bezpečnosti. Tento slovník je k dispozici jak v tištěné, tak v elektronické verzi.[1]

Vzhledem k širokému rozsahu a dynamickému vývoji informačních technologií text selektivně definuje ty fenomény, které mají přímý vztah k podvodnému jednání v prostředí e-shopů a k následnému procesnímu postupu Policie České republiky.[2]

2.1 Kybernetická trestná činnost (Cybercrime)

Užívání výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je jevem, který je pro dnešní dobu charakteristický. Lze konstatovat, že v podstatě nejde nalézt takovou oblast lidské činnosti, kde by se přímo, nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie. Bohužel, tak jak rostou možnosti užívání těchto vymožeností dnešní doby a vědeckotechnického pokroku, rostou i možnosti a zároveň i četnost jejich zneužívání k páchání trestné činnosti.

Různí autoři i různé právní normy používají pro označení těchto aktivit různé pojmy, mezi které patří: informační, informatická, elektronická kriminalita, počítačová trestná činnost, počítačová kriminalita, kybernetická trestná činnost, kyberkriminalita. U této problematiky přetrvávají rozdíly nejen v označování tohoto jevu, ale rozdílně je chápán též jejich obsahový význam, což mnohdy přispívá k nesprávnému pochopení významu tohoto druhu trestné činnosti.

[1] JIRÁSEK, Petr. Cyber security glossary. Páté doplněné a upravené vydání. Centrum kybernetické bezpečnosti, z. ú., 2022. 352 s. ISBN 978-80-908388-4-0.
[2] Vlastní text

Na tomto místě je třeba předně konstatovat terminologickou nejednotnost a různorodost v chápání výše uvedených pojmů. To je do značné míry odůvodněné interdisciplinárností přístupu k řešení dané problematiky. Proto bývají v různých odborných pracích i v právních dokumentech často zaměňovány pojmy „počítačový trestný čin“ s „počítačovou kriminalitou“, „kybernetický trestný čin“ s pojmem „kyberkriminalita“ apod., respektive jsou mnohdy užívány jako synonyma.

V 90. letech 20. století se pro trestnou činnost páchanou pomocí informační techniky ustálil pojem „počítačová kriminalita“. Pod pojmem počítačová kriminalita je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení, případně větší množství počítačů samostatných nebo propojených do počítačové sítě. Z uvedené definice je patrné, že počítačová kriminalita se vztahovala pouze na počítačové systémy, jakožto na cíle útoku.

Označení „počítačová kriminalita" evokuje představu, že trestný čin musí být spáchán na počítači, nebo prostřednictvím počítače, nejčastěji počítače osobního. Takové chápání je dnes zjednodušující, zároveň i poněkud kvantitativně redukuje množství jevů, které lze pod pojem trestná činnost páchaná prostředky informačních a komunikačních technologií zahrnout. Mnohá technická zařízení v dnešní době, díky implementaci mikroprocesoru spolu s jejich miniaturizací, již dávno převzala funkci osobních počítačů, aniž by byla sama za osobní počítače označována. A i tyto prostředky, přestože nejsou nazývány počítači, mohou být terčem trestné činnosti či prostředkem k jejímu spáchání. Z těchto důvodů se pojem „počítačová kriminalita“ i „počítačový trestný čin“ v dnešní době již v odborné literatuře téměř nepoužívají. Namísto pojmu „počítač“ je v dnešní době používán spíše vyraz „informační a komunikační technologie“.[3]

Mezi nejčastější typy kybernetických útoků patřily v roce 2022 dle statistik NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) různé druhy phishingu, vishingu a podvodných e-mailů, dále pak útoky zaměřené na dostupnost, a to především formou DDoS útoků.[4]

[3] KOLOUCH, Jan. Cybercrime [online]. CZ.NIC, z. s. p. o., 2016. Str. 31-32. ISBN 978-80-88168-16-4.
[4] ŠTĚDROŇ, B.; JAŠEK, R.; SVÍTEK, M. a kol. Umělá inteligence a právo. Plzeň: Aleš Čeněk, 2024. str. 54. ISBN 978-80-7380-947-8.

2.2 Uživatel

Uživatel je každá fyzická, nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací.

2.3 Kybernetický prostor

Podle § 2 písm. a) Zákona o kybernetické bezpečnosti „se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací." Kyberprostor je tedy chápán jako množina zahrnující vše, co obsahuje digitální data.[5]

2.4 Poškozený

Ten, komu bylo trestným činem ublíženo na zdraví, způsobena majetková škoda nebo nemajetková újma, nebo ten, na jehož úkor se pachatel trestným činem obohatil.

2.5 Pachatel podvodu

Pachatelem může být zásadně kterákoliv fyzická osoba, která vyvolala nebo využila omylu jiné osoby, popř. jí zamlčela podstatné skutečnosti, přičemž v důsledku dispozice oklamané osoby došlo ke škodě na cizím majetku a obohacení pachatele nebo jiné osoby.[6]

2.6 Orgán činný v trestním řízení

Orgány činnými v trestním řízení se rozumějí soud, státní zástupce a policejní orgán.[7]

---

[5] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Aleš Čeněk, 2019. str. 75. ISBN 978-80-7380-765-8.
[6] VANTUCH, Pavel. Trestní zákoník s komentářem. ANAG, 2011. str. 744. ISBN 978-80-7263-677-8.
[7] JELÍNEK, Jiří. Trestní právo procesní. 7. aktualizované a doplněné vydání. Leges, 2023. str. 254 ISBN 978-80-7502-687-3.

3 Formy a projevy kybernetické kriminality

Následující kapitola se věnuje nejčastějším projevům trestné činnosti v kyberprostoru. Zvláštní pozornost je věnována těm modům operandi, které přímo souvisejí s podvodným jednáním v prostředí e-commerce, jako jsou podvodné e-shopy, phishing či zneužití metod sociálního inženýrství. Pachatelé v digitálním prostředí své metody neustále vyvíjejí, což klade vysoké nároky na flexibilitu a odbornost Policie České republiky.

3.1 Podvodná jednání (§ 209 Trestního zákoníku)

V policejní statistice i praxi je nejčastěji dokumentovaným jednáním přečin Podvod podle § 209 trestního zákoníku. V prostředí informačních technologií dochází velmi často k jednočinnému souběhu s trestným činem Neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ (Trestní zákoník).

Specifickou kategorií jsou podvodné e-shopy, které vznikají za jediným účelem: vylákat finanční prostředky od obětí. Tyto platformy vykazují krátkou životnost (zpravidla dny až týdny) a zanikají ihned poté, co je nashromážděn dostatečný objem prostředků. Pro snížení pravděpodobnosti odhalení jsou finance okamžitě vyváděny do zahraničí nebo konvertovány do virtuálních měn, což komplikuje jejich zajištění v rámci trestního řízení. Obdobný mechanismus lze sledovat u podvodných inzerátů, fiktivních sbírek či tzv. nigerijských podvodů.

3.2 Phishing a jeho deriváty

Phishing představuje techniku oklamání uživatele za účelem získání jeho identity (jména, hesla, údaje o platební kartě). Útočník vytváří vizuálně věrohodnou kopii legitimní instituce (banky, státního úřadu, přepravní společnosti).[8]

[8] Phishing. Online. Www.eset.com/cz/phishing. 2025. Dostupné z: https://www.eset.com/cz/phishing/#:~:text=Phishing%20je%20typ%20kybernetick%C3%A9ho%20%C3%BAtoku,nebo%20prod%C3%A1vaj%C3%AD%20na%20%C4%8Dern%C3%A9m%20trhu.. [cit. 2026-03-25].

3.2.1 Vishing

Telefonická forma phishingu, kde pachatel za využití sociálního inženýrství a technické manipulace s číslem odesílatele (spoofing) vystupuje například jako prodejce, pracovník banky či policista.[9]

3.3 Specifika podvodných webových stránek

Podvodné stránky využívají sociální inženýrství k vyvolání pocitu výhodnosti či časového nátlaku. Typicky se jedná o:

1. Sběr dat (Phishing): Uživatel dobrovolně vyplní údaje v domnění, že se registruje do soutěže nebo e-shopu.

2. Přímý majetkový podvod: Prodej neexistujícího zboží za extrémně nízké ceny (např. kauza elektrosmart.cz). Zde je klíčová rychlá reakce policie a bankovních domů k zablokování finančních toků.

3.4 Mravnostní a ostatní kriminalita v kyberprostoru

Internet slouží také jako prostor pro páchání mravnostních deliktů, zejména vůči dětem (§ 191–193b TZ). Kyberprostor umožňuje pachatelům snadnější navazování kontaktů a šíření nelegálních materiálů. Do širšího rámce kyberkriminality řadíme i:

- **Trestné činy proti autorskému právu (§ 270 TZ):** Nelegální sdílení obsahu.

- **Násilné projevy a Hate Crime:** Stalking (§ 354 TZ), nebezpečné vyhrožování a podněcování k nenávisti, kde internet poskytuje pachateli zdánlivou anonymitu.[10]

[9] Vishing a spoofing. Online. Policejní prezidium ČR. 2021. Dostupné z: https://policie.gov.cz/clanek/vishing-a-spoofing.aspx. [cit. 2026-03-25].
[10] Jednotlivé druhy kyberkriminality. Online. Policie ČR. 2024. Dostupné z: https://policie.gov.cz/clanek/jednotlive-druhy-kyberkriminality.aspx. [cit. 2026-01-15].

4 Poznání podvodného jednání

V souvislosti s podvodnými nabídkami na internetu vydalo Evropské spotřebitelské centrum doporučení pro uživatele, které by jim mělo umožnit poznat podvodná jednání:

- Zadejte údaje o společnosti (např. název společnosti, adresu webu, e-mail) do internetového vyhledávače.

- Zamyslete se nad tím, jak se obchodník prezentuje.

Je vzhled webu, na kterém se chystáte nakoupit, profesionální? Důvěryhodný dojem rozhodně nebudí e-mailové adresy na bezplatných a anonymních serverech typu yahoo.com, hotmail.com, gmail.com, live.com, seznam.cz apod. Stejně tak, je-li web umístěn na bezplatném hostingovém serveru, není to znak profesionality.

- Platbu předem provádějte jen tehdy, jde-li o skutečně důvěryhodného obchodníka. Jistě nedáte peníze na ulici neznámému člověku s příslibem, že Vám v budoucnu dodá věc. Na internetu tak však řada uživatelů činí. Platbu předem provádějte jen tehdy, pokud jste si jisti, že jednáte s důvěryhodným dodavatelem. Především údaje o platební kartě je třeba chránit.

- Zvlášť podezřelý je požadavek na platbu systémem Western Union.

U bankovních převodů nikdy nezasílejte peníze na účty soukromých osob, pokud se nejedná o účet prodávající firmy/společnosti. Mezi obvyklé znaky podvodu patří špatná jazyková úprava, požadavek platby předem, v hotovosti či převodem, další požadavky na platby pod smyšlenou záminkou (clo, pojištění, přibalení většího počtu kusů výrobků) a tak podobně. Pamatujte si, že pokud se nabídka zdá příliš výhodná, než aby byla skutečná, tak nejspíš skutečná není!

- Nahlédněte do obchodního rejstříku dané země, zda je v něm společnost registrována. Stává se také, že někdo zneužije jméno existující společnosti a založí web s podobným označením.

- Zkontrolujte doménu webové stránky.

Stává se, že webová adresa je stejná jako adresa skutečné existující a registrované firmy. Je zde ovšem jeden rozdíl. Doména, tedy koncovka internetové adresy, je jiná (např. nikoli „couk" pro Velkou Británii, ale třeba coco" pro Kokosové ostrovy). Najděte si sídlo společnosti na internetovém serveru nabízejícím pouliční fotografie měst, a to podle adresy, uváděné u inzerátu a na webové stránce společnosti.

- Važte si svých osobních údajů.

Nesdělujte informace o sobě na nedůvěryhodných i Vám dosud neznámých stránkách. Uvádějte jen takové údaje, které jsou skutečně nezbytné.

- Nereagujte na nevyžádanou poštu (spam).

Na nevyžádanou poštu nereagujte, v žádném případě nesdělujte e-mailem údaje o bankovním účtu, číslo platební karty, nebo třeba přihlašovací údaje do internetového bankovnictví. Nevyžádaný e-mail smažte, nikdy neotvírejte neznámé přílohy.[11]

[11] Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech. Praha: Policejní akademie České republiky v Praze a kolektiv autorů, 2020. str. 149. ISBN 978-80-7251-505-9.

5 Kdo jsou pachatelé kybernetické kriminality

Pachateli trestné činnosti v oblasti kybernetické kriminality jsou nejčastěji čtyři skupiny pachatelů nebo organizátorů trestné činnosti.

V prvé řadě jsou to cizí státy. Jde o kybernetickou válku, tak jako dnes provozuje Rusko v souvislosti s Ukrajinou válku informační, tak jako Izrael zaútočil na centrifugy vyrábějící látky pro atomovou bombu, prostřednictvím viru, který napadl odstředivky na výrobu uranu, a tak dále.

Další kategorií jsou samozřejmě teroristé. Teroristé jsou schopni zejména v rámci tzv. asymetrických konfliktů zaútočit na stát velice účinně prostřednictvím počítačových sítí.

V mnoha případech si to neuvědomíte, ale nejnebezpečnější jsou vlastně zaměstnanci. Zaměstnanci jsou ti, kteří mají přístup ke všemu, kteří mají obvykle dostatečná oprávnění, dostatečné možnosti a informace na to, aby vaše data poškodili, modifikovali, odcizili, prodali či použili k vydírání. Dovolím si upozornit, že to samozřejmě mohou být i data soudu, mohou to být data advokátní kanceláře, mohou to být data kohokoliv, kdo má nějaké zaměstnance.

Čtvrtým a nejčastějším „uživatelem“ výnosů páchaní kybernetické kriminality jsou organizované skupiny. Organizovaný zločin, který kyberprostor používá pro praní peněz, pro nelegální převody a pro všechny ostatní další činnosti, ke kterým lze počítače využít. My při odhalování a dokazování kybernetické kriminality máme řadu problémů. Problém jurisdikce, problém, aby vůbec byla trestná činnosti odhalena, abychom dokázali, kdo je pachatelem a dokázali jsme mu, že jde o jeho trestnou činnost. Problémem jsou i chybějící nebo nedobře popsané skutkové podstaty nového trestního zákoníku, byť ten je samozřejmě daleko sofistikovanější, než byl trestní zákoník předchozí.[12]

[12] Kybernetická kriminalita - fenomén dneška. Online. PRÁVNÍ PROSTOR. 2015. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/kyberneticka-kriminalita-fenomendneska. [cit. 2024-09-09].

6 Osobní ochrana uživatele

Osobní ochranou rozumíme, že by měl uživatel dodržovat všeobecně známá základní pravidla při používání internetu. Mezi taková všeobecná pravidla pro ať už jednotlivce či společnosti řadíme, dostatečně silná hesla a jiná zabezpečení profilů, dbát zvýšené opatrnosti při manipulaci s neznámými přílohami, nesdílet data svá nebo svých blízkých tam kde je k nim snadný přístup, udržovat aktualizovaný software a hardware, používání legálního softwaru atd.

Obecně lze říci, že každý uživatel by měl být při práci na počítači a internetu opatrný, nedůvěřovat všemu co vidí, pochybné weby si ověřit, nesdělovat nikomu své osobní údaje atd. V rámci zaměstnání by navíc měl vždy dbát na bezpečností politiku společnosti či organizace a její pokyny ohledně chování na internetu.

Výše zmíněná pravidla se sice mohou zdát dospělým jasná, nicméně ve větším ohrožení jsou děti. Děti si zpravidla softwarovou nebo hardwarovou ochranu nezajistí a nemusí vědět, co je na internetu považováno za normální chování a co ne. Je tedy na rodičích, školách či různých organizacích předat dětem informace, jak se na internetu chovat a jaké nebezpečí na ně může v kyberprostoru čekat.

Mezi organizace podporující a organizující různé kurzy či semináře o internetové bezpečnosti patří například „Kraje pro bezpečný internet“. Jedná se o projekt poskytující online e-learningové kurzy pro děti, učitele, policisty, rodiče ale i seniory nebo sociální pracovníky. Dalším takovým projektem je „internetem bezpečně“, jehož cílem je pomocí různých vzdělávacích akcí zvýšení povědomí o bezpečnostních rizicích, které mohou na uživatele v kyberprostoru čekat a jak se proti nim bránit. V neposlední řadě je důležité zmínit projekt „E-bezpečí“. „Projekt E-Bezpečí je celorepublikový certifikovaný projekt zaměřený na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a souvisejícími fenomény.“ Specializací tohoto projektu jsou primárně útoky spočívající v šíření škodlivého obsahu, jako je sexting, kybergrooming, kyberstalking a další.[13]

[13] Kyberneticka_kriminalita.pdf POKORNÝ, Pavel. Kyberkriminalita [online]. Zlín, 2016. Diplomová práce

7 Co je to podvod?

Dle definice trestního zákoníku spáchá trestný čin podvodu ten, kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou. S rozmachem internetu a služeb na něm došlo k ohromnému zvýšení výskytu takto popisovaného jednání. Díky nepřímému kontaktu s obětí, téměř neomezenému počtu potencionálních cílů a malému riziku odhalení se stal počítačový svět doslova rájem pro všelijaké podvodníky a šmelináře. Pro policisty z Krajského ředitelství v Praze tvoří podvody a podvodná jednání na internetu téměř polovinu případů, kterými se zabývají. Z pohledu internetové kriminality je to nejčastější množina trestných činů. Podvody mohou být různé, obzvlášť na internetu. V případě podvodů při nakupování je možné celou problematiku zjednodušit na dvě oblasti. Podvodné e-shopy a podvody na inzertních nebo aukčních službách.[14]

§ 209 TZ Podvod

(1) Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a. spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

[14] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 111. ISBN 978-80-271-9074-4.

b. spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

c. spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo

d. způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a. způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b. spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309 TZ), teroristického útoku (§ 311 TZ) nebo teroru (§ 312 TZ).

(6) Příprava je trestná.[15]

[15] DRAŠTÍK, Antonín a FREMR, Robert. Trestní zákoník: komentář. 1. díl. Praha: Wolters Kluwer, 2015. str. 1193. ISBN 978-80-7478-790-4.

8 E-shopy

Jedním z nejčastějších typů transakcí, které na internetu realizujeme, je nákup v internetovém obchodě. Většina e-shopů má své stránky strukturovány tak, aby nám umožňovaly si v rámci katalogu vybrat zboží, a následně toto zboží vložit do virtuálního košíku. Poté přecházíme k virtuální pokladně, kde se od nás očekává vložení nezbytných informací důležitých pro zpracování objednávky.

U pokladny obchodu pak vedle zadání svých kontaktních údajů musíme zpravidla zvolit způsob doručení a platby. Co se doručení týče, máme obvykle na výběr z několika možností. Nakupování v kamenném obchodě se nejvíce přiblížíme, pokud zvolíme možnost převzít zboží v kamenné provozovně e-shopu.

Tato možnost však může být zpoplatněna, protože i s vydáním zboží v provozovně má obchodník určité náklady. Pokud preferujeme osobni převzetí, ale daný e-shop nemá kamennou provozovnu, mohou pro nás představovat zajímavou alternativu některé zásilkové služby, které umožňují osobní vyzvednutí zboží ve zvolené provozovně v rámci sítě kontaktních míst po celé České republice.

Dalším možným způsobem doručení je doručení poštou či přepravní službou. Různé poštovní a přepravní služby se zpravidla liší cenou, rychlostí i kvalitou doprovodných služeb. V případě některých přepravních služeb nás bude doručovatel kontaktovat v den doručení zásilky a dohodne s námi čas předání. V jiných případech můžeme zvolit komfortní dopravu, kdy nám doručovatel pomůže dopravit např. novou lednici nejen za první uzamykatelné dveře našeho domu, ale až na její místo v našem bytě. Pokud nás tlačí čas, můžeme využit pro doručení zvláštní kurýrní služby, které jsou často schopny zajistit doručení zboží v řádu hodin nebo dokonce desítek minut po objednání.

Druhou volbou, kterou musíme provést vedle způsobu doručení, je výběr způsobu placení. Ten někdy bývá závislý na způsobu doručení. Např. v případě převzetí zboží v kamenném obchodě nebo na kontaktním místě bývá většinou jediná možná platba v hotovosti při převzetí. Mnohdy není v provozovně či na kontaktním místě možné platit platební kartou, což nás může nemile překvapit, pokud u sebe nemáme hotovost.

Při doručení poštou či přepravní službou je platebních možnosti zpravidla více. Konzervativní možností je dobírka, kdy cenu uhradíme pracovníkovi přepravce při převzetí zboží. I zde je zpravidla třeba platit v hotovosti a možnost platit kartou není samozřejmostí. Velmi rozšířená je možnost platby bankovním převodem. Takovou platbu zpravidla provádíme dopředu, a proto bychom měli vždy zvážit, zda své peníze svěřujeme dostatečně důvěryhodné protistraně. Platba také může byt spojena s poplatky účtovanými ze strany banky. Výhodou je skutečnost, že obchodníkovi ani jinému prostředníkovi neposkytujeme své důvěrné údaje, které by jinak bylo možné zneužít, jako např. číslo platební karty.

Právě platební karty jsou dalším nástrojem, který pro placení na internetu můžeme využit. Výhodou je rychlost a jednoduchost platby. Stačí zadat číslo kreditní karty, datum, do kterého je platná, a třímístný ověřovací kód na zadní straně karty. Prostředky jsou pak na učet obchodníka připsány okamžitě, a ten tak může začít naši objednávku neprodleně zpracovávat. Protože je však platba kartou natolik snadná, může být v některých případech srovnatelně snadné její zneužití. Za tímto účelem někteří vydavatelé karet zavádí zvláštní systémy autorizace internetových plateb např. pomoci SMS kódů. Klíčová je však zejména prevence zneužití, kterou bychom měli provádět my sami tím, že údaje o své kartě sdělíme pouze co nejmenšímu okruhu důvěryhodných subjektů a předáme je zabezpečeným způsobem.

Za tímto účelem slouží různé platební brány, které obchodníkům umožňují přijímat platby kartou, aniž bychom poskytli údaje o své platbě přímo jim. Podobně nám může pomoci systém PayPal, který slouží jako elektronická peněženka, kterou můžeme dobít a následně z ní platit. Svěření údajů o kartě přímo obchodníkovi by mělo být krajním prostředkem, který bychom měli důkladně zvážit a přistoupit na něj pouze tehdy, jsme-li si jistí, že obchodník je schopen tyto údaje dostatečně zabezpečit.

Zvláštním způsobem platby pak může být využití tzv. kryptoměn, zejména nejznámější z těchto měn - bitcoinu, které pracují na jako decentralizovaná sít, prostřednictvím které dochází ke směně platebních prostředků za virtuální měnu. Specifikem plateb provedených pomoci bitcoinu je zejména značná míra anonymity, kterou poskytuje.[16]

[16] DONÁT, Josef a TOMÍŠEK, Jan. Právo v síti: Průvodce právem na internetu. Praha: C. H. Beck, 2016. str. 152. ISBN 978-80-7400-610-4.

9 Podvodné e-shopy

E-shopy nabízejí zboží, které kupující vkládá do virtuálního nákupního košíku, kde si následně může zobrazit celkové množství produktů a jejich cenu. K dokončení objednávky je zapotřebí zadat doručovací adresu, zvolit způsob doručení a platby. Zákazník poté obdrží potvrzení o objednávce na zadaný e-mail. Přes všechny tyto pozitivní aspekty elektronického obchodování existují i stinné stránky v podobě různých podvodných aktivit. Ty mohou zahrnovat falešné e-shopy, phishing útoky, neoprávněné používání platebních karet a mnoho dalších.[17]

Trendem posledních let je zakládání celých falešných elektronických obchodů. Pro podvodníky to není nic složitého. V dnešní době existuje mnoho technických řešení pro vybudování navenek fungujícího e-shopu, která jsou k dispozici zdarma, nebo za velmi malý poplatek. Pak útočníkům stačí takový falešný e-shop naplnit atraktivním zbožím a uvést ještě atraktivnější ceny a zákazníci přijdou sami. Společným znakem takových falešných e-shopů je, že nemají možnost osobního odběru zboží. Platby probíhají pouze bankovním převodem, nebo ještě lépe prostřednictvím elektronických platebních služeb jako je PayPal, PayU atd.[18] Platební brána funguje jako prostředník, který šifruje citlivé údaje (čísla karet) a předává je ke zpracování.[19]

Také zde neexistuje žádná zákaznická podpora, nebo pouze formou elektronického formuláře. Kontaktní telefon, pokud už bývá uveden, zpravidla nikdo nezvedá. Po nějaké době e-shop přestane mít aktualizované nabídky, nebo zcela zmizí z internetu. I pár dní fungování se podvodníkům vyplatí k tomu, aby si přišli na tučný výdělek. Touto formou trestné činnosti se zabývají nejen jednotlivci, ale velmi často i organizované mezinárodní skupiny. Pak se stává, že podobný typ falešných obchodů se objeví v několika zemích najednou a škody často dosahují astronomických částek. V následujících podkapitolách budou uvedeny příklady podvodného jednání z prostředí internetu.

[17] KORMOŠOVÁ, I. Podvody na internetu [online].[cit. 2023-10-11]. Dostupné z WWW: https://www.policie.cz/clanek/podvody-na-e-shopech.aspx.
[18] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 111. ISBN 978-80-271-9074-4
[19] ČESKO. Zákon č. 370/2017 Sb., o platebním styku. In: Zákony pro lidi.cz [online]. [cit. 2026-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-370

9.1 Luxusní mobil za hubičku

Petr je zkušený právník. Nakupovat online se rozhodně nebojí, je to velmi příjemné, vzhledem k jeho časovému vytížení. Rád si vybrané zboží prohlédne na internetu, pak si vybere z nevýhodnější nabídky a nechá si ho doručit domů, případně do kanceláře. Ani z reklamací nemá strach. Zná svoje práva zákazníka víc než dobře a je si jistý, že v případě problému se svých práv vždy dovolá. Mimo to je také otcem dvou dospívajících dcer a jako milující otec se vždycky snaží děvčatům koupit, co jim na očích uvidí. Když přemýšlel, co by dcerám udělalo radost k Vánocům, vzpomněl si, jak se oběma líbí jeho mobilní telefon. Nakonec, který teenager dnes netouží po našlapaném stylovém smartphonu. Nejlépe po tom s nakousnutým jablkem v logu. A když mu do jeho e-mailové schránky přišla nabídka na nejnovější iPhone za téměř třetinovou cenu, bylo rozhodnuto. Jistě, trochu se podivil nad tak levnou cenou, ale vysvětlení v popisu zboží ho uklidnilo.

Jednalo se o zbytek zahraničním operátorem dotovaných přístrojů, takže ani platba na účet u zahraniční banky ho nezarazila. Navíc v podmínkách nákupu bylo jasně uvedeno, že na telefony se vztahuje plná záruka, uplatnitelná přímo u lokálního distributora. Takže kdyby s nimi cokoliv bylo, prostě si je nechá v rámci záruky vyměnit u nejbližšího prodejce. Aby měl vše stoprocentně pojištěné, dokonce si připlatil nadstandardní dodávku kurýrní službou, přece jenom Vánoce jsou už za dveřmi a pošta toho bude mít dost. Jeden termín dodání za druhým míjely a zboží pořád nikde. A když telefony nedorazily ani v polovině ledna a navíc stránky obchodu byly nedostupné, konečně pochopil, že to nebyl ten nejlepší nápad a nezbyde mu nic jiného, než se obrátit na policii.

Rada:

Zkuste si najit recenze nejen na zboží, ale i na elektronický obchod. Často se stává, že si kladné recenze píší sami podvodníci z falešných e-shopů. Neznámé, nebo krátce fungující e-shopy s neuvěřitelně výhodnými cenami nemusí být tou nejlepší volbou. [20]

[20] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 111-112. ISBN 978-80-271-9074-4.

9.2 Falešné inzeráty

Nákupy přes internet jsou skvělá věc. Zboží si můžeme vybrat z klidu domova, o přestávce v práci nebo klidně při jízdě tramvají. Vše bývá přehledné, nabídka je obrovská, prodejci se předhánějí s výhodnými cenami, případně s bonusy za nákupy. Internet je plný různých inzertních nebo aukčních služeb, kde můžeme velmi snadno nakoupit naše vyhlédnuté zboží za ty nejlepší ceny. Nebo také můžeme velmi snadno přijít o nemalé sumy peněz. Hned v úvodu je třeba konstatovat, že neexistuje jednoznačný návod, jak odlišit podvodný inzerát od pravé a seriózní nabídky. Je však mnoho maličkostí, které by nám mohly napovědět. Nejdůležitější a neustále opakovanou zásadou je nenechat se strhnout výhodnou cenou. Pravděpodobnost, že na inzerát koupíme nový, funkční a nepoužívaný tablet za desetinovou cenu oproti ceně v kamenném obchodě, je asi stejně velká, jako že vyhrajeme jackpot ve Sportce. Bohužel, naše lidská touha po výhodných nákupech je skvělým byznysem pro velké množství podvodníků.

Rada

Spousta podvodníků mylně spoléhá na to, že suma peněz, o kterou oběť připraví, bude tak malá, že poškozenému se nebude chtít věc oznamovat policii. Nebo že částka, kterou si nechají zaplatit za své podvody, je nižší než 10.000,-Kč a policie věc nebude ani prošetřovat, protože nedošlo k újmě ve výši částky, kdy se jedna o trestný čin. Při podezření, že by se mohlo jednat o podvodné jednání, se nebojte okamžitě oslovit provozovatele dané služby. V jejich možnostech je zájmového obchodníka lépe prověřit. Případně mohou dodat spoustu užitečných informací pro policii.

Dodávka a platba za zboží nám mohou také mnohé napovědět. Například při internetovém prodeji nebo spíše nákupu motorových vozidel ze zahraničí je transakce ihned podezřelá, pokud prodejce preferuje jako platební kanál službu Western Union. Právě přes tento jinak skvělý a fungující platební systém jsou požadovány platby největší části podvodných inzerátů v dnešní době.[21]

[21] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 113. ISBN 978-80-271-9074-4.

9.3 Největší bazary a aukční servery

Aukro.cz

Největší aukční portál v ČR. Velmi často tuto službu využívají také podvodníci. Díky letité spolupráci s policií jsou falešné aukce často odhaleny již při jejich založení. Služba též nabízí Program ochrany kupujících, který v případě podvodu vyplatí finanční náhradu škody až do plné výše zaplacené částky včetně poštovného.

Ebay.com

Celosvětově největší aukční server je často cílem různých falešných prodejců. Díky jeho rozsáhlosti je vyšetřování podvodných nákupů hodně složité.

Sbazar.cz

Na internetovém bazaru Sbazar.cz najdete zboží převážně z druhé ruky, které nabízejí lidé s uživatelským účtem u Seznam.cz. Na stránce je možné vyhledávat i třídit nabídky podle kategorií a regionu. Služba má specializovaný tým na odhalování podvodníků.

Bazos.cz

Je inzertní server, který umožňuje bezplatně zveřejňovat a vyhledávat nabídky a poptávky zboží, služeb a jiného majetku soukromých osob a podnikatelských subjektů. Služba nabízí možnost označit inzerát jako závadný.

Sauto.cz

Nabízí prodej ojetých a nových vozů od většiny prodejců v České republice. Inzeráty jsou kontrolovány administrátory a v případě nových podvodů upozorňuje uživatele prostřednictvím zpráv. Jakou roli hraje při koupi vozidla jeho cena? Podle Seznam.cz Výzkumníka je velmi důležitá pro 64 % dotázaných.[22]

[22] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 114. ISBN 978-80-271-9074-4.

9.3.1 Kočárek

Pro našeho malého syna, který se má narodit za měsíc, jsem sháněla kočárek. Na nový jsme neměli peníze, a tak jsem prolézala aukční servery a trávila večery hledáním. Byla jsem překvapena počtem kočárků, které lidé nabízeli, ale z většiny jsem byla zklamaná, podle fotografií to nebyl ten typ, který jsem si vysnila, nebo měl nějaké vady. Některé kočárky jsem vyloučila i z důvodu, že prodejci byli dost daleko a náklady na převoz by cenu kočárku navýšily o další výdaje.

Nakonec jsem objevila kočárek, který se mi zalíbil. Nastavila jsem si hlídacího psa a kdykoli, když někdo vložil kočárek této značky na bazar, mi přišlo upozornění. Jednou mi přišel e-mail s nabídkou v sedm hodin ráno. Kočárek na fotografiích vypadal jako nový a inzerát byl zadán bez gramatických chyb, takže jsem měla i dobrý vnitřní pocit.

Brzy jsme se dohodli, že mi kočárek zašle na dobírku. Zaplatila jsem tedy předem částku 4.700,-Kč na účet a se slibem, že mi přijde do tří dnů, jsem se s prodávající rozloučila. Čekala jsem marně a ani po týdnu mi zboží nedošlo. Inzerát byl samozřejmě smazán a služba, na které byl umístěn, na moje dotazy nereagovala a pořád odkazovala na licenční ujednání. Řešení nepovedeného nákupu přerušil můj porod a já měla úplně jiné starosti**.** Od nákupu uběhly již tři měsíce a já už rezignovala na řešení.

Rada:

Většina aukčních a inzertních služeb nabízí i hodnoceni prodejců. Je to taková zpětná vazba od nakupujících. Ověřte si, jakým způsobem chce zaplatit. U dražšího nákupu se vyplatí i zajet si několik desítek kilometrů na prohlídku nabízeného zboží. Vždy se vyplatí přemýšlet a nedělat ukvapená rozhodnutí.[23]

[23] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 117. ISBN 978-80-271-9074-4.

10 Desatero bezpečného nakupování na internetu

1. Internetový prodejce by měl být prověřen. U internetových obchodů má být zkontrolován zápis v obchodním nebo živnostenském rejstříku. Na stránce by měl být uveden také kontakt, který je v případě nejistoty využit k dotazům na nejasné skutečnosti. Solidními internetovými obchody je nabízeno několik způsobů kontaktu se zákazníkem. Pokud na stránkách není kromě e-mailu uveden žádný kontakt (adresa, telefon), nemá být riskováno ani nakupováno.

Mezi údaje, které musí prodejce zveřejnit, patří:

- název, obchodní jméno a sídlo poskytovatele služeb, resp. jméno, příjmení, místo podnikání a adresu bydliště poskytovatele služeb
- adresu elektronické pošty a telefonní číslo
- daňové identifikační číslo (pokud je plátcem DPH)

2. Možnosti dopravy a ceny za ni mají být předem ověřeny. Pečlivě mají být prozkoumány způsoby zaplacení zboží, informace o dodací lhůtě nebo termínu doručení. U neznámých obchodníků nemá být za zboží placeno předem a má být volena možnost platby na dobírku.

3. Věnujte tomu čas a vyhledejte si všechny dostupné informace o výrobku. Podstatný rozdíl je v tom, že od kamenného obchodu na zboží nemůže být sáhnuto a nemůže být vyzkoušeno.

4. Před nákupem zboží je dobré si vyhledat recenze na obchodníka. Může se stát, že nemá mezi prodejci dobré jméno. U služeb, které to nabízejí, může být dobrým vodítkem označení spolehlivého nebo ověřeného prodejce.

5. Je vhodné si porovnat ceny zboží na internetu. Může se stát, že jiný prodejce nabízí zboží za výhodnějších podmínek nebo jde o prodejce, který má dobré jméno.

6. Zakoupené zboží může být reklamováno do 30 dní. Reklamace, včetně odstranění vady, musí být vyřízena do 30 dní od jejího uplatnění.

7. Pokud jde o prodej zboží na bazarových službách, doporučujeme, pokud to je možné, osobní předání zboží. Určitě nikomu není doporučeno zasílat zálohu.

8. Sledujte www adresu obchodu, pokud budete z nějakého důvodu přesměrováni jinam, je to podezřelé.

9. Při nakupování není doporučeno zadávat víc údajů, než je požadováno. Žádný obchod nebude vyžadovat PIN ke kartě, CVV nebo rodné číslo. V případě neznámého prodejce není vhodné zadávat „hlavní e-mail“.[24]

10.1 Příklad: Vstupenky na koncert

Dozvěděla jsem se, že za měsíc bude vystupovat v Praze moje oblíbená zpěvačka. Hledala jsem proto na internetu lístky, ale všude bylo již vyprodáno. Byla jsem ochotna dát maximálně tři sta korun navíc, pokud bych je sehnala z nějakého bazaru. Nikdy jsem si je takhle nekupovala, ale nejsem naivní a vím, že se vždycky najde pár překupníků a ti pak lístky napálí za vyšší cenu. Blížil se termín koncertu a všude byla nabídka za dva tisíce. To jsem opravdu nechtěla akceptovat, navíc jsem chtěla jít na koncert s mým přítelem, a tak by se nám to opravdu prodražilo.

Nakonec jsem narazila v nějaké diskuzi na slečnu Hanku, která psala, že chtěla jít se svou kamarádkou, ale ta je nemocná, ona sama nechce jít a lístky prodává za původní cenu. Podmínka byla dojet někam v Praze na metro a zaplatit hotově. S Hankou jsem se potkala v domluvený čas na domluveném místě a v obálce mi opravdu přinesla dvě vstupenky. Byly vytištěné, ale tomu jsem nevěnovala pozornost, protože dnes vám klidně může dorazit kód i do e-mailu nebo mobilu. Druhý den jsem s přítelem vyrazila na koncert, na který nás nechtěli pustit, protože kód na vstupence byl neplatný. Chtěla jsem volat Hance, ale telefonní číslo bylo nedostupné.

Doporučení: Vyvarujte se neautorizovaných prodejců s lístky na sportovní i společenské akce. Ty kupujte jen u autorizovaných prodejců nebo po ověření platnosti.[25]

[24] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 119. ISBN 978-80-271-9074-4.

11 Oběť trestného činu

Stejně jako v reálném světě, i v tom virtuálním se můžeme dostat do situace, kdy se staneme obětí nějakého protiprávního jednání. V takovém případě nám většinou nezbývá nic jiného, než se obrátit na policii. Provozovatelé různých internetových služeb nám mohou v mnohém pomoci, ale pokud byl spáchán trestný čin, je policie jediným orgánem státní moci, který může danou věc prošetřit.[26]

11.1 Trestný čin

Trestný čin je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně (§13 odst. 1).[27] Co to přesně znamená? Velmi jednoduše řečeno, aby nějaké jednání mohlo být považováno za trestný čin, musí být v našem trestním zákoníku uvedeno a popsáno. Typickým příkladem je tzv. kyberšikana. Jak už z předchozích kapitol víme, kyberšikana je jakékoliv jednání, jehož záměrem je vyvést z rovnováhy, ublížit, zastrašit nebo jinak ohrozit oběť za pomoci moderních informačních technologií (zejména pak internetu nebo mobilního telefonu). Všichni tušíme, že kyberšikana není jednání, které by bylo v pořádku, ale i přesto se nejedná o trestný čin. A to z prostého důvodu – kybešikana jako skutek není v našem trestním zákoníku nikde uvedena. Na druhou stranu ale také již víme, že jedním z projevů kyberšikany je například vyhrožování nebo vydírání. Oba tyto projevy už v trestním zákoníku uvedeny jsou, a proto je možné tyto činy trestně stíhat. Znamená to tedy, že sice za tzv. kyberšikanu není možné v naší zemi nikoho trestně stíhat, ale za jednotlivé projevy tohoto jevu už to přípustné je.

11.2 Trestní oznámení

Trestní oznámení je v zákoně definováno jako „oznámení o skutečnostech nasvědčujících tomu, že byl spáchán trestný čin“.[28]

---

[25] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 121. ISBN 978-80-271-9074-4.

[26] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 131. ISBN 978-80-271-9074-4.

[27] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: Zákony pro lidi.cz [online]. [cit. 2026-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[28] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: Zákony pro lidi.cz [online]. [cit. 2026-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

Pokud se staneme, a to nejen na internetu, obětí jakéhokoli jednání, jehož následkem nám vznikla nějaká újma, a nemusí se jednat pouze o hmotnou škodu, máme právo podat tzv. trestní oznámení. My nemusíme přesně určit (odborně se tomu říká kvalifikovat), o jaký trestný čin se jedná. Toto nechme na policii nebo dalších složkách, souhrnně nazývaných orgány činné v trestním řízení. Podle právních předpisů nemůže státní zástupce ani policejní orgán v zásadě odmítnout přijetí žádného trestního oznámení. Tyto instituce mají dokonce povinnost oznámení přijmout a bez průtahů věc vyřešit. Trestní oznámení lze podat písemně, ale třeba i ústně, na kterémkoliv policejním oddělení nebo přímo na státním zastupitelství. Státní zástupce je právník, který je zařazen k určitému státnímu zastupitelství a vykonává jeho úkoly.[29]

11.3 Možnosti podání trestního oznámení

Chceme-li podat trestní oznámení ústně, stačí se dostavit na kterékoliv oddělení Policie České republiky či na státní zastupitelství a tam s námi bude sepsán protokol. Při tomto sepisování bude oznamovatel vyslechnut o okolnostech, za nichž byl trestný čin spáchán, o důkazech které jsou, a také o výši škody způsobené oznamovaným trestným činem. Policisté nebo státní zástupce také mají povinnost oznamovatele řádně poučit o jeho právech a všech okolnostech, které s podáním souvisejí. Tísňová linka 158 (stejně jako ostatní linky) slouží k oznámení bezprostředního ohrožení života, zdraví a majetku. Je proto dobré v případě podávání trestního oznámení zvážit, zda je využití tohoto kontaktu opravdu nezbytné.

11.4 Obsah trestního oznámení

Po obsahové stránce by každé trestní oznámení mělo obsahovat kromě informací o osobě oznamovatele také odpovědi na několik základních otázek:

Kdo? Určení totožnosti účastníků skutku: pachatel, poškozený, svědci (pokud je totožnost osob neznámá, je důležité uvést například internetové přezdívky, e-mailové adresy, registrační údaje a další).

[29] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 132. ISBN 978-80-271-9074-4.

Kdy? Co nejpřesnější určení doby, kdy k události došlo.

Kde? Místo nebo místa, kde k oznamované události došlo, případně kde skutek vyšel najevo, a to včetně přesných adres internetových stránek, tzv. URL. Vzhledem k neustále se měnícímu obsahu různých internetových služeb je časový údaj společně s co nejpřesnější adresací místa jedna z nejdůležitějších informací pro možné vyšetřování na internetu.

Jak? Popis jednání všech zúčastněných osob.

Co? Přesný popis skutku. Zde není třeba se starat o tzv. právní kvalifikaci, to nechme na orgánech činných v trestním řízení, ale jde o co možná nejpřesnější popsání toho, co a jak se stalo.

Proč? Co bylo cílem skutku, čeho pachatel svým jednáním dosáhl nebo čeho chtěl dosáhnout.

Následek? Byla způsobena nějaká újma na zdraví nebo majetku, případně v jaké výši. Stačí odhad, není ihned nutné škodu přesně vyčíslit.

11.5 Lhůty pro vyřízení a délka vyšetřování

Policejní orgán má minimálně dva měsíce na to, aby prověřil skutečnosti, nasvědčující tomu, zda byl spáchán trestný čin. Tato lhůta může být ovšem delší pokud se jedná o závažnější trestné činy, může být případně prodloužena. Opět z praxe víme, že prošetřování trestných činů na internetu bývá velmi zdlouhavé, především z důvodů vyžadování důkazních materiálů od mnoha návazných subjektů, poskytovatelů služeb a připojení, kteří mají často své sídlo mimo území České republiky. [30]

[30] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 133-134. ISBN 978-80-271-9074-4.

12 Policie České republiky a kyberzločiny

Odhalování a vyšetřování trestné činnosti na internetu je dnes doslova každodenní prací Policie České republiky. V rámci organizační struktury jsou dnes vytvořena specializovaná pracoviště pro boj s internetovou kriminalitou na každém krajském ředitelství policie. Tato pracoviště poskytují ostatním složkám policie odborné znalosti při zajišťování důkazů ze sítě internet. Prudký rozvoj informačních technologií a s tím spojené přenesení části zločinů do virtuálního světa přinesly potřebu výše uvedená pracoviště rozšiřovat a prohlubovat jejich odborné znalosti. Není proto náhoda, že boj proti kyberkriminalitě se stal jednou z hlavních priorit Policie České republiky. Ovšem bez aktivní pomoci poskytovatelů služeb obsahu a připojení v rámci sítě internet bude tato snaha marná. Vzhledem k absenci centrální autority v rámci internetu leží pořizování důkazních materiálů o protiprávní činnosti pouze na straně poskytovatelů. Bez jejich součinnosti není možné důkazy pro trestní řízení často zadokumentovat.

Je jen na nás bychom například k nakupování na internetu využívali takové služby, které v rámci platných zákonů monitorují činnost svých uživatelů a v případě protiprávního jednání rychle a účinně poskytnou tyto informace pouze orgánům činným v trestním řízení na základě příslušných právních předpisů.[31]

Kyberzločiny řeší především Národní centrála pro boj proti terorismu, extremismu a kybernetické kriminalitě, která vznikla v roce 2023.[32]

12.1 Policie a justice – problém s odhalováním kyberkriminality

Kyberkriminalita, jako trestná činnost, je páchána s použitím velmi specifických technologických nástrojů a specializovaných znalostí. K jejímu odhalení a prokázání je tedy opět třeba velmi speciálních nástrojů, znalostí a postupů. A to je právě jeden z hlavních problémů policie a justice - nedostatek vysoce kvalifikovaných pracovníků, kteří by byli schopni zvládnout problematiku kyberkriminality nejenom po stránce technologické, ale i po stránce právní a policejní praxe. Mimo to, policie se musí

[31] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 135. ISBN 978-80-271-9074-4.
[32] Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV. Online. 2026 Policie ČR. 2026. Dostupné z: https://policie.gov.cz/clanek/narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite.aspx. [cit. 2026-03-25].

vyrovnat i s tím, že klasické vyšetřovací metody selhávají. Je to zejména dáno odlišným charakterem stop v kyberprostoru, jejich trvanlivostí a použitelností v důkazním řízením. Zatímco stopy klasického trestného činu je možno zajistit ještě několik hodin nebo dnů po činu, v případě kyberkriminality je zajištění stop otázkou minut. Trestný čin se odehrává ve složitém technologickém prostředí, jehož stav se každou sekundou mění. Navíc, toto prostředí podléhá rychlému technologickému vývoji, a tak spektrum kybernetických trestných činů podléhá technologickým trendům, velmi rychle se rozvijí a modifikuje. Současná rychlost vyšetřovacího procesu neodpovídá technologickým trendům.

Obdobným problémem jako policie trpí i justice. Přestože je většina projevů kyberkriminality trestná, není vždy snadné takovou činnost odhalit, dokázat a pachatele odsoudit. Kromě běžných problémů nepomáhá jistě soudnímu řízení ani fakt, že soudci jsou specialisty na právo, nikoliv na informační technologie, takže v odborných případech musí využívat soudní znalce a spoléhat na ně. Nedostatek kvalifikovaného soudního personálu a soudců, kteří by byli schopni orientace ve složité struktuře kyberzločinu, nepřispívá ke kvalitě soudního řízení v případech, kdy je projednáván kybernetický trestný čin. Pomalost procesních postupů může vést i ke ztrátě důkazů, které bezprostředně po spáchání trestného činu existovaly, avšak dlouhé administrativní řízení neumožnilo jejich řádné zajištění.[33]

12.2 Oznamovací povinnost

Na závěr je třeba zmínit také skutečnost, že kdokoliv z nás se dozví o protiprávním jednání, je ze zákona povinen toto oznámit. Nesplnění této povinnosti ,je v některých případech postihováno jako trestný čin dle ustanovení § 368 trestního zákoníku. Skutkovou podstatu tohoto trestného činu naplní ten, kdo se hodnověrným způsobem dozví, že někdo jiný spáchal některý z taxativně vyjmenovaných trestných činů, a tuto skutečnost neoznámí policejnímu orgánu nebo státnímu zástupci. Za toto může provinilci hrozit trest odnětí svobody až ve výši tří let. Tato oznamovací povinnost platí také pro provozovatele různých internetových služeb.[34]

[33] JIROVSKÝ, Václav. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. str. 26-27. ISBN 978-80-247-1561-2.
[34] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-271-9074-4.

12.3 Úloha policie a justice při postihování počítačové kriminality

Kybernalita jako trestná činnost je páchána s použitím velmi specifických technologických nástrojů a specializovaných znalostí. K jejímu odhalení a prokázání je tedy opět potřeba velmi speciálních nástrojů, znalostí a postupů. A to je právě jeden z hlavních problémů policie a justice- nedostatek vysoce kvalifikovaných pracovníků, kteří by byli schopni zvládnout problematiku kybernality nejen po stránce technologické, ale i po stránce právní a policejní praxe. Mimo to se policie musí vyrovnat i s tím, že klasické vyšetřovací metody selhávají. Je to zejména dáno odlišným charakterem stop v kyberprostoru, jejich trvanlivostí a použitelností v důkazním řízení. Přestože je většina projevů kybernality trestná, není vždy snadné takovou činnost odhalit, dokázat a pachatele odsoudit. Na začátku roku 2006 došlo ke změně struktury a vzniklo nové oddělení informační kriminality. Došlo k vytvoření specializovaných míst operativních detektivů na útvarech s republikovou působností a současně na jednotlivých krajských územních odborech Policie české republiky.[35]

- **Specializované útvary:** Na kyberkriminalitu se zaměřují specializované odbory v rámci obecné i hospodářské kriminality.
- **Vyšetřování a odhalování:** Policie vyšetřuje případy neoprávněného přístupu k počítačovým systémům (hacking), počítačové podvody (phishing, krádeže financí) a šíření škodlivého softwaru (ransomware).
- **Zajišťování důkazů:** Klíčovou činností je zajišťování digitálních stop a dat, často v mezinárodním měřítku.
- **Prevence:** Policie realizuje osvětové kampaně a preventivní projekty k minimalizaci rizik na sociálních sítích.[36]

[35] FEREBAUEROVÁ, R., PEKÁREK, O. Aplikovaná informatika. 1. vydání. České Budějovice: Vysoká škola evropských a regionálních studií, 2014, str. 139. ISBN 978-80-87472-74-3.

[36] POŽÁR, Josef. Specifické problémy boje s kybernetickou kriminalitou. Online. 2025. Dostupné z: https://mv.gov.cz/soubor/policejniakademie.aspx#:~:text=(Zdroj%20informac%C3%AD:%20resortn%C3%AD%20materi%C3%A1l%20%E2%80%9EAnal%C3%BDza%20aktu%C3%A1ln%C3%AD%20%C3%BArovn%C4%9B,kter%C3%A9%20se%20pod%C3%ADlej%C3%AD%20na%20vy%C5%A1et%C5%99ov%C3%A1n%C3%AD%20kybernetick%C3%A9%20kriminality.. [cit. 2026-03-24].

13 Specifika a mechanismy podvodných e-shopů

Současným trendem v oblasti kybernetické kriminality jsou vysoce sofistikované napodobeniny zavedených e-shopů. Pachatelé již nevytvářejí amatérsky vyhlížející stránky, ale přistupují k tzv. copycat podvodům. Tyto weby parazitují na dobrém jménu známých prodejců tím, že kompletně kopírují jejich vizuální identitu, loga, a dokonce i obchodní podmínky či kontaktní údaje.

13.1 Mechanismy podvodných e-shopů

- **Vytvoření iluze důvěryhodnosti:** Podvodníci kopírují design známých značek, používají platební ikony (Visa/Mastercard) a "garance vrácení peněz", aby působili profesionálně.
- **Šíření přes sociální sítě a reklamu:** Odkazy na tyto weby se šíří skrze reklamy na Facebooku, Instagramu, nebo pomocí SMS a e-mailů (phishing).
- **Krádež identity:** Podvodníci zneužívají IČO a název existující, legitimní firmy, aby zmátli zákazníky kontrolující rejstříky.
- **Sběr údajů:** Cílem nemusí být jen okamžitá platba, ale i získání údajů o platební kartě pro následné zneužití.
- **"Mrtvý" zákaznický servis:** Po odeslání peněz e-shop přestane komunikovat, e-maily se vrací a telefonní čísla neexistují. [37]

13.2 Identifikační znaky podvodu

Navzdory vysoké úrovni napodobeniny existují určité indikátory, které mohou na podvodné jednání upozornit:

- **Manipulace s URL adresou:** Pachatelé využívají domény podobné originálu (např. záměna koncovky .cz za .com, přidání pomlčky či překlep v názvu).

[37] Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů. Online. 2025. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--ktere-kopiruji-weby-znamych-obchodu--289453/#:~:text=*%20Aktu%C3%A1ln%C3%AD%20informace.%20*%20Bezpe%C4%8Dnost%20v%C3%BDrobk%C5%AF. [cit. 2026-03-24].

- **Nestandardní požadavky na data:** Vyžadování informací, které nejsou pro proces nákupu a doručení nezbytné, může signalizovat pokus o sběr citlivých dat pro další zneužití (phishing).

13.3 Možnosti nápravy a role finančních institucí

V případě, že k podvodné transakci již došlo, hraje klíčovou roli v rámci minimalizace škod institut chargebacku. Jedná se o proces, kdy držitel karty žádá vydavatelskou banku o zpětné storno transakce z důvodu nedodání zboží či neautorizované operace.

Proces chargebacku v praxi typicky zahrnuje:

1. Podání žádosti: Poškozený doloží bance důvody pro vrácení platby.
2. Verifikace: Vydavatelská banka prověří legitimitu nároku.
3. Interakce s acquirerem: Kontaktování banky obchodníka k získání vyjádření.
4. Finální rozhodnutí: Při uznání reklamace jsou finanční prostředky připsány zpět na účet držitele karty.

Z hlediska dokazování v trestním řízení je nezbytné, aby poškozený zajistil důkazní materiál v podobě snímků obrazovky (screenshotů) a potvrzení o platbě, neboť podvodné stránky bývají pachatelem velmi rychle odstraněny.[38]

[38] MINISTERSTVO PRŮMYSLU A OBCHODU. *Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů* [online]. Praha: Ministerstvo průmyslu a obchodu, Odbor živností a spotřebitelské legislativy, 13. ledna 2025 [cit. 2026-01-27]. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--ktere-kopiruji-weby-znamych-obchodu--289453/

14 Postup Policie České republiky při prověřování oznámení o podvodných e-shopech

Tato kapitola detailně rozebírá procesní úkony Policie České republiky od okamžiku přijetí podnětu o spáchání trestného činu až po rozhodnutí. Proces je rozdělen do fází, které reflektují specifika vyšetřování v digitálním prostředí.

14.1 Příjem trestního oznámení a prvotní úkony

Proces začíná buď vlastním zjištěním policie, nebo (častěji) podáním trestního oznámení poškozeným (oznamovatelem).

- **Vytěžení poškozeného:** Policista musí od oznamovatele získat klíčové digitální stopy: přesnou URL adresu, potvrzení o transakci, komunikaci s „e-shopem“ a identifikaci bankovního účtu, na který byly prostředky zaslány.
- **Poučení o chargebacku:** V rámci praxe by měl policista již v této fázi ověřit, zda poškozený kontaktoval svou banku za účelem reklamace platby, což může minimalizovat škodu dříve, než dojde k prvotním procesním úkonům.[39]

14.2 Postup před zahájením trestního stíhání (prověřování)

V rámci prověřování podezření ze spáchání trestného činu opatřuje policejní orgán k objasnění a prověření skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin, potřebné podklady a nezbytná vysvětlení a zajišťuje stopy trestného činu. V rámci prověřování může být konstatováno, že se daný skutek vůbec nestal nebo se nejedná o trestný čin. Může být ale zjištěno, že se o trestný čin jedná a rovněž může dospět policejní orgán k závěru, že jej spáchala určitá osoba.[40]

[39] Vlastní text
[40] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. vydání. Plzeň: Aleš Čeněk, 2018. str. 724 .ISBN 978-80-7380-720-7.

14.2.1 Zahájení úkonů trestního řízení (§ 158 odst. 3 tr. řádu)

Jakmile policejní orgán na základě trestního oznámení nebo vlastních poznatků získá podezření ze spáchání trestného činu, sepíše neprodleně Záznam o zahájení úkonů trestního řízení. Tento moment je oficiálním začátkem prověřování. Opis záznamu zasílá policejní orgán do 48 hodin státnímu zástupci a v záznamu jsou uvedeny okolnosti, pro které se řízení vede, a předpokládaná právní kvalifikace.[41]

14.2.2 Výslech poškozeného a vytěžení informací (§ 158 odst. 6 tr. řádu)

Podání vysvětlení poškozeného je stěžejním důkazním prostředkem. Vzhledem k tomu, že poškozený je často jediným přímým zdrojem informací o podvodném e-shopu, musí být výslech velmi detailní:

- **Procesní poučení:** Poškozený musí být řádně poučen o svých právech.
- **Identifikace digitální stopy:** Do protokolu se zaznamenává přesná URL adresa, čas nákupu, IP adresy, e-mailová komunikace, čísla bankovních účtů a způsob, jakým na e-shop poškozený narazil (např. reklama na sociální síti).
- **Zajištění komunikace:** Policejní orgán vyzve poškozeného k vydání věci, v tomto případě digitálních dat (e-maily, potvrzení o platbě, screenshoty).[42]

14.2.3 Operativní a technické úkony v kyberprostoru

Souběžně s výslechem provádí policie úkony k identifikaci pachatele a zajištění důkazů na internetu:

- **Lustrace v otevřených zdrojích:** Prověření registrátora domény, hostingu a historie webu.
- **Žádost o údaje z informačních systémů:** Podle ust. § 8 odst. 2 tr. řádu žádá policie o informace, které podléhají bankovnímu tajemství, a podle ust. § 8b tr.

[41] *ÚZ Trestní předpisy*. Sagit, 2024. str. 190 ISBN 978-80-7488-634-8.
[42] Vlastní text

řádu o informace z databáze účastníků elektronických komunikací (např. kdo si registroval dané telefonní číslo nebo IP adresu).[43]

14.2.4 Zajišťovací úkony (§ 78 a § 79 tr. řádu)

Pokud jsou zjištěny relevantní nosiče dat nebo finanční prostředky, přistupuje se k jejich zajištění:

- **Vydání a odnětí věci (§ 78, § 79 tr. řádu):** Výzva k vydání počítačů, serverů nebo mobilních telefonů, pokud se nacházejí na území ČR.
- **Zajištění peněžních prostředků na účtu (§ 79a tr. řádu):** Pokud policie identifikuje „průtokový účet“, na který poškozený zaslal peníze, vydá usnesení o zajištění těchto prostředků. To je klíčový krok k tomu, aby peníze nebyly vyvedeny do zahraničí nebo do kryptoměn.

14.2.5 Odborné vyjádření a znalecké zkoumání (§ 105 tr. řádu)

V komplikovanějších případech policejní orgán přibírá znalce z oboru kybernetiky nebo žádá o odborné vyjádření specializované pracoviště (např. odbor analytiky a kybernetické kriminality). Cílem je prolomit šifrování, analyzovat logy serveru nebo zrekonstruovat smazaná data.[44]

14.3 Fáze prověřování (§ 158 odst. 1 tr. řádu)

Po přijetí oznámení zahajuje policejní orgán prověřování, aby zjistil skutečnosti nasvědčující tomu, že byl spáchán trestný čin.[45]

14.4 Specifika prověřování kybernetických podvodů

Vyšetřování podvodných e-shopů naráží na několik specifických bariér:

[43] Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád). Online. Zákony pro lidi. 2026. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141. [cit. 2026-03-25].
[44] Vlastní text
[45] ÚZ Trestní předpisy. Sagit, 2024. str. 190. ISBN 978-80-7488-634-8.

1. **Místní příslušnost:** Podle trestního řádu je příslušný útvar v místě spáchání činu. U e-shopů je to často komplikované – místo, kde sedí pachatel, místo serveru a bydliště oběti jsou tři různé lokace. Z praxe se nejčastěji jako místo spáchání bere místo, kde poškozený uskutečnil objednávku, respektive platbu.

2. **Mezinárodní prvek:** Pokud jsou servery i bankovní účty mimo EU, využívá PČR nástroje mezinárodní policejní spolupráce (Interpol, Europol).

14.5 Rozhodnutí v rámci prověřování

Fáze prověřování, zahájená podle § 158 odst. 3 tr. řádu, musí být ukončena zákonným způsobem. Policejní orgán posoudí, zda zjištěné skutečnosti odůvodňují zahájení trestního stíhání konkrétní osoby, nebo zda jsou dány důvody pro jiný procesní postup.

14.5.1 Zahájení trestního stíhání (§ 160 odst. 1 tr. řádu)

K tomuto rozhodnutí policie přistoupí v okamžiku, kdy zjištěné a odůvodněné skutečnosti nasvědčují tomu, že byl spáchán trestný čin a že jej spáchala konkrétní osoba. Pachatel je v tomto případě tedy známý.

- **Forma:** Děje se tak vydáním Usnesení o zahájení trestního stíhání, které se doručuje obviněnému. [46]

- **Specifikum u e-shopů:** U kybernetických podvodů k tomuto kroku dochází nejčastěji v případech, kdy se podaří ztotožnit majitele bankovního účtu (často tzv. „bílého koně“), nebo pokud technické šetření (IP adresy) ukáže na konkrétní osobu na území ČR. Tímto úkonem se prověřování mění ve fázi vyšetřování.

14.5.2 Odložení věci (§ 159a tr. řádu)

Toto je v praxi nejčastější způsob ukončení věci u podvodných e-shopů operujících ze zahraničí.

[46] Vlastní text

- **§ 159a odst. 1 (Nejde o podezření z trestného činu):** Pokud se ukáže, že věc není trestným činem (např. šlo o obchodní spor, nikoliv o úmyslný podvod).

- **§ 159a odst. 5 (Pachatel nezjištěn):** Klíčové ustanovení pro online podvody. Pokud policejní orgán vyčerpal všechny dostupné prostředky a přesto se nepodařilo zjistit skutečnosti opravňující zahájit stíhání proti konkrétní osobě, věc odloží.

  Poznámka: Odložení neznamená definitivní konec. Pokud se v budoucnu objeví nové stopy, může policie v prověřování kdykoliv pokračovat.

14.5.3 Odevzdání věci (§ 159a odst. 1 písm. a, b tr. řádu)

Pokud policejní orgán dojde k závěru, že nebyly naplněny znaky trestného činu, ale jednání vykazuje znaky jiného deliktu:[47]

- **Odevzdání k přestupkovému řízení:** U e-shopů, kde způsobená škoda nedosahuje hranice 10.000,-Kč. Věc je postoupena příslušnému správnímu orgánu.

- **Odevzdání jinému orgánu:** Například České obchodní inspekci, pokud jde o klamavé obchodní praktiky, které nemají intenzitu podvodu. [48]

14.5.4 Dočasné odložení trestního stíhání (§ 159b tr. řádu)

V specifických případech organizovaného zločinu může policejní orgán se souhlasem státního zástupce rozhodnout o dočasném odložení, pokud je to nezbytné k rozložení celé sítě pachatelů nebo k odhalení hlavních organizátorů v pozadí podvodných e-shopů.[49]

14.5.5 Předání věci jinému orgánu

[47] ÚZ Trestní předpisy. Sagit, 2024. str. 193. ISBN 978-80-7488-634-8.
[48] Vlastní text
[49] ÚZ Trestní předpisy. Sagit, 2024. str. 194. ISBN 978-80-7488-634-8.

Vzhledem k přeshraničnímu charakteru e-commerce kriminality může dojít k situaci, kdy je věc předána k trestnímu řízení do jiného státu (v rámci právní pomoci), pokud je tamní vedení procesu efektivnější (např. tam sídlí pachatel i server).[50]

[50] Vlastní text

15 Případové kazuistiky

15.1 Případ číslo 1

NP (neznámý pachatel) z profilového účtu pod jménem T. R. reagovala dne 15. 04. 2024 na inzerát na sociální síti Facebook na prodejní aplikaci Marketplace, kde poškozená M. O. prodávala dětské jízdní kolo za částku 5.000,-Kč, kdy projevila zájem o zakoupení dětského jízdního kola. Dne 15. 04. 2024 po vzájemné komunikaci se společně domluvili na přepravě zboží kurýrem DPD včetně zaplacení zboží předem na účet. NP následně poslal odkaz (http://dpdcz.info371.com/*), kde si poškozená po kliknutí
na uvedený odkaz měla vybrat svoji banku Česká spořitelna a přihlásit se na údajný web DPD. Zde vyplnila své údaje k přihlášení do svého internetového bankovnictví, kam následně měla dostat peníze za prodané jízdní kolo. Poté dostala potvrzení Smart klíčem, které potvrdila. Následně zkontrolovala svůj účet a zjistila, že došlo k provedení dvou transakcí přes Transfergo a to ve výši 2 x 9.990,-Kč. Celkem byla poškozené způsobena škoda ve výši 19.980,-Kč.

Ve věci byly dne 15. 04. 2024 podle ust. § 158 odstavce 3 trestního řádu zahájeny úkony trestního řízení pro přečin Podvod podle ust. § 209 odst. 1 trestního zákoníku a zločin Neoprávněné opatření, padělání a pozměnění platebního prostředku podle ust. § 234 odst. 1, 3 trestního zákoníku.

S poškozenou byl následně sepsán protokol o podání vysvětlení podle ust. § 158 odst. 6 trestního řádu, kde uvedla veškeré jí známé skutečnosti a odpověděla na dotazy podané policejním orgánem. Uvedla tedy veškeré jména osob, kontakty, přezdívky a názvy profilů, ze kterých s ní podezřelá osoba komunikovala. Dále podrobně uvedla kdy ke komunikaci a přeposlání finančních prostředků z jejího účtu došlo. Policejnímu orgánu poskytla písemné a elektronické podklady důležité k trestnímu řízení, jako jsou screenshoty komunikace a další. Byl s ní sepsán souhlas s poskytnutím bankovních informací, kdy díky tomuto může policejní orgán požadovat po bance poškozené výpisy z jejího bankovního účtu, aby se zjistilo, kam byly finanční prostředky převedeny a také konkrétní dny a časy, kdy k převodu došlo.

Ve smyslu ust. § 8 odst. 1 zákona číslo 141/1961 Sb., trestního řádu bylo policejním orgánem požádáno o zaslání podkladů pro trestní řízení. Konkrétně bylo požadováno od bankovní společnosti Česka spořitelna, a.s. o zaslání identifikace bankovního účtu číslo 2307****93/0800 (číslo, datum založení, dispoziční práva, příp. další skutečnosti) a o výpis z bankovního účtu číslo 2307****93/0800 s uvedením, kdy byly zaúčtovány dvě platby ve výši 9.990,-Kč zadané dne 15. 04. 2024 a veškeré detaily plateb (IP logy autorizace a připojení k účtu, atd.).

Policejním orgánem byly následně vyhodnoceny informace, které obdržel od České spořitelny, jakožto bankovního ústavu, u které má poškozená zřízený svůj bankovní účet č. 2307****93/0800, který jí byl dne 15. 04. 2024 napaden dosud neznámým pachatelem. V odpovědi od bankovního ústavu se nachází výpis z uvedeného bankovního účtu, výpis IP logů a detaily obou zájmových transakcí. Z doručené odpovědi bylo zjištěno, že výše uvedená je jediným majitelem a disponentem uvedeného bankovního účtu. Z detailů obou zájmových plateb bylo zjištěno, že tyto byly provedeny dne 15. 04. 2024 v 9:57 hod. a 10:01 hodin pokaždé v částce 9.990,- Kč a to přes platební portál TransferGo. Obě platby byly zadány z IP adresy 2a03:***:420:a7:e850:****:7c7e:4178 a z mobilního zařízení Mozilla/5.0 (iPhone OS 15_8_2). Dále z výpisu IP logů k uvedenému bankovnímu účtu bylo zjištěno, že dne 15. 04. 2024 v době od 09:45 - 10:01 hod. se na účet někdo opakovaně připojil z IP adresy 4a03:***:410:a7:e850:****:7c7e:5984 a celkem osmkrát se pokoušel odeslat platbu ve výši 9.990,-Kč. Dle výpisu z uvedeného bankovního účtu, byla platba schválena pouze dvakrát. Uvedená IP adresa je shodná i s IP adresou, ze které se NP přihlašoval k účtu vedeném u společnosti TransferGo.

Dále policejní orgán obdržel na zaslanou žádost od společnosti TransferGo odpověď, kde byly uvedeny údaje k účtu, přes který prošly finanční prostředky poškozené. Z této odpovědi bylo zjištěno následující: jméno a příjmení majitele účtu: S.D, nar. 03.**.19**, bydliště: M****, 5** 01 L***č, telefonní číslo: +420733***948, e-mail: di***@gmail.com a IP adresy: 62.221.71.***, 4a03:***:410:a7:e850:****:7c7e:5984. Následně byla vyžádána lustrace těchto údajů Oddělením analytiky a kybernetické kriminality, SKPV, ÚO Rychnov nad Kněžnou.

Jelikož bylo šetřením policejního orgánu zjištěno, že se jedná o sériově páchanou trestnou činnost, byl spisový materiál na základě věcné příslušnosti dle PPP (pokynu policejního prezidenta) číslo 103/2013 postoupen ke společnému řízení na Obvodní oddělení Policie Frýdek Místek, kde bylo pokračováno v šetření výše uvedené trestného činu a jeho pachatele.

15.2 Případ číslo 2

Dne 15. 11. 2023 osobně na Obvodním oddělení Policie České republiky v Hostinném oznámil pan M. J. že si dne 5. 11. 2023 na internetovém portálu www.heureka.cz vyhledal a objednal sadu zimních pneumatik NOKIAN za částku 15.515.-Kč, kterou předem odeslal ze svého bankovního účtu číslo 31468****/0300 na bankovní účet 166774****/2700 společnosti PNEU a TRANS s.r.o. Do dnešního dne mu nebyly objednané pneumatiky doručeny, poškozený nemá vráceny peníze zpět a firma je nekontaktní.

Oznamovatel, pan M. J. byl řádně poučen podle zákona číslo 45/2013 Sb., o obětech trestných a poté sním byl sepsán Úřední záznam o podání vysvětlení podle ust.. § 158 odst. 6 tr. řádu, kde uvedl veškeré skutečnosti týkající se jeho případu. Na základě přijatého oznámení a předložených dokladů policejní orgán vyhodnotil, že se jedná o podezření ze spáchání přečinu Podvodu podle ust. § 209 tr. zákoníku. Byl sepsán Záznam o zahájení úkonů trestního řízení, čímž byla oficiálně zahájena fáze prověřování. Následně byl policejním orgánem podle ust. § 78 odst. 1 tr. řádu vyzván, aby vydal veškeré potřebné soubory a dokumenty týkající se podvodného jednání. Vydal tedy fakturu, která mu byla doručena při zaplacení objednaného zboží, dále výpis ze svého bankovního účtu a veškerou emailovou komunikaci s podezřelým.

Policejní orgán prověřil společnost PNEU a TRANS s.r.o. v obchodním rejstříku. Zjistil, že se jedná o tzv. „prázdnou schránku“ s nastrčeným jednatelem (bílý kůň), na kterou bylo v poslední době podáno více obdobných oznámení po celé České republice. Dále bylo provedeno šetření k bankovnímu účtu podle ust. § 8 odst. 2 tr. řádu policejní orgán zaslal přes Státního zástupce Okresního státního zastupitelství vyžádání bance k identifikaci majitele účtu a výpisu transakcí. Z výpisu vyplynulo, že finanční částka 15.515,-Kč byla ihned po připsání přeposlána na jiný účet nebo vybrána z bankomatu. Policejním orgánem bylo tedy požádáno provozovatele portálu

Heureka.cz a registrátora domény o sdělení IP adres, ze kterých byl e-shop spravován a ze kterých byla vedena komunikace se zákazníky. Lustrací v systému ETŘ bylo zjištěno, že pod stejným číslem účtu a názvem firmy figuruje dalších 45 poškozených z celé České republiky. Celková škoda tedy přesáhla hranici 500.000,-Kč, čímž došlo k překvalifikaci na Podvod se značnou škodou podle ust. § 209 odst. 4 písm. d) tr. zákoníku.

Díky analýze IP adres a kamerových záznamů z výběrů z bankomatů byl ztotožněn podezřelý pan A. B., který v inkriminované době ovládal bankovní účty i webové rozhraní e-shopu. Na základě příkazu soudu byla u podezřelého provedena domovní prohlídka, při které byl zajištěn notebook, mobilní telefony a SIM karty použité při páchání trestné činnosti. Zajištěná technika byla předána k analýze, která potvrdila přítomnost přístupových údajů k e-shopu a komunikaci s poškozenými.

Jakmile byly shromážděny dostatečné důkazy (výpisy z účtů, IP adresy, data z domovní prohlídky), policejní orgán vydal Usnesení o zahájení trestního stíhání proti panu A. B., jako obviněnému. Policejní orgán předal spis státnímu zástupci s návrhem na podání obžaloby. Okresní soud uznal pana A. B. vinným. Byl mu uložen úhrnný trest odnětí svobody v trvání 3 let s podmíněným odkladem na zkušební dobu 5 let a povinnost nahradit škodu všem poškozeným, včetně pana M. J. ve výši 15.515,-Kč.

15.3 Případ číslo 3

Dne 15. 01. 2025 se dostavil na Obvodní oddělení Policie České republiky v Kostelci nad Orlicí poškozený, pan J. M., bytem v přilehlé obci. Službu konajícímu policistovi uvedl, že se stal obětí podvodu na inzertním portálu Bazoš.cz.

Pan Jaroslav popsal, že si týden předtím vyhlédl inzerát na zánovní mobilní telefon iPhone 15 Pro za lákavou, nikoliv však nereálnou cenu 16.500,-Kč. S prodejcem komunikoval prostřednictvím e-mailu a aplikace WhatsApp. Po dohodě zaslal celou částku na bankovní účet prodejce, který přislíbil odeslání balíku přes Zásilkovnu. Předchozího dne si poškozený balík vyzvedl v boxu v Kostelci nad Orlicí. Po otevření krabice doma zjistil, že namísto telefonu obsahuje jeden kilogram krystalového cukru v originálním papírovém obalu, aby váha zásilky odpovídala předpokládanému obsahu.

Policista vyhodnotil, že popsané jednání naplňuje znaky skutkové podstaty trestného činu Podvodu podle ust. § 209 trestního zákoníku. Ihned po přijetí oznámení sepsal s poškozeným Úřední záznam o podání vysvětlení podle ust. § 158 odst. 6 tr. řádu. Poškozený policii předal veškerou dokumentaci:

- Vytištěnou e-mailovou komunikaci.
- Screenshoty z aplikace WhatsApp s telefonním číslem pachatele.
- Potvrzení o bankovním převodu (číslo účtu příjemce).
- Podací štítek ze Zásilkovny.
- Samotný „obsah“ zásilky (cukr) i s obalovým materiálem pro případné zajištění daktyloskopických stop či DNA.

Následně byl sepsán Záznam o zahájení úkonů trestního řízení podle ust. § 158 odst. 3 tr. řádu, čímž byla oficiálně zahájena fáze prověřování. Policejní orgán provedl „lustraci“ všech dostupných atributů. Tento proces zahrnoval zejména lustraci bankovního účtu podle ust. § 8 odst. 2 tr. řádu na bankovní ústav za účelem zjištění majitele účtu a historie transakcí (zasílá Státní zástupce). Dále lustraci telefonního čísla, tedy zjištění registrovaného uživatele u mobilního operátora (často jde o anonymní předplacenou kartu), prověření IP adres, tedy vyžádání dat od provozovatele inzertního portálu o tom, z jaké IP adresy byl inzerát vložen. Vzhledem k tomu, že se jednalo o trestnou činnost páchanou v kyberprostoru, byl spisový materiál a zjištěné atributy (číslo účtu, e-mail, telefon) postoupeny k analýze na Službu kriminální policie a vyšetřování – analytické pracoviště.

Analytici SKPV provedli kontrolu v systémech (například v databázi informací o trestné činnosti páchané na internetu). Zjistili, že stejné číslo účtu figuruje v dalších sedmi případech napříč celou Českou republikou (například v Ostravě, Praze a Plzni), kde bylo rovněž zasíláno znehodnocené zboží (cukr, rýže, staré časopisy). Dalším šetřením bylo zjištěno, že bankovní účet je veden na jméno tzv. „bílého koně“ – osoby bez domova, která účet založila za úplatu a k platební kartě nemá přístup. Výběry z bankomatu byly prováděny osobou v roušce a kapuci v místech mimo dosah kvalitních kamerových systémů. IP adresy pachatele vedly přes zahraniční VPN servery, což znemožnilo přímou identifikaci koncového zařízení.

Přes intenzivní snahu policejního orgánu a analytickou podporu SKPV (Služba kriminální policie a vyšetřování) se nepodařilo ustanovit konkrétní osobu, která

se za fiktivním prodejcem skrývala. „Bílý kůň“ nebyl schopen, nebo ochoten identifikovat osobu, která jej k založení účtu najala a digitální stopa skončila u anonymizačních nástrojů.

Vzhledem k tomu, že byly vyčerpány všechny dostupné operativní i procesní možnosti a nepodařilo se zjistit skutečnosti opravňující zahájit trestní stíhání proti konkrétní osobě, rozhodl policejní orgán o tom, že ne 10. 03. 2025 bude věc podle ust. § 159a odst. 5 tr. řádu odložena, neboť se nepodařilo zjistit pachatele. Poškozenému bylo doručeno Usnesení o odložení věci a byl telefonicky kontaktován, kdy mu vysvětleno, že pokud v budoucnu vyjdou najevo nové skutečnosti (například dopadení pachatele při jiné trestné činnosti, kde se přizná k těmto útokům), bude v prověřování neprodleně pokračováno.

16 Výsledky dotazníkového šetření

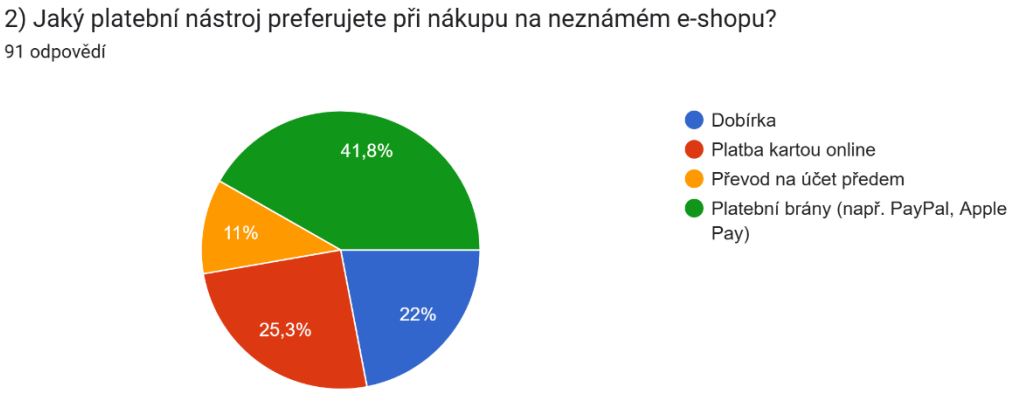
V této části jsou vyhodnocena data získaná prostřednictvím dotazníkového šetření. Výsledky jsou kvantitativně zpracovány a interpretovány s ohledem na formulované cíle. Dotazníkového šetření se účastnilo celkem 93 respondentů, kteří odpověděli na připravené otázky v dotazníkovém formátu.

Otázka č. 1 - Jak často nakupujete na e-shopech?

[51] Graf č. 1

Nejvíce respondentů nakupuje na e-shopech několikrát do měsíce (34,4 %), následuje druhá nejčastější odpověď, několikrát týdně (28 %), jednou do měsíce (22,6 %), jednou týdně (12,9 %) a vůbec na e-shopech nenakupuje minimální počet respondentů.

Otázka č. 2 – Jaký platební nástroj preferujete při nákupu na neznámém e-shopu?

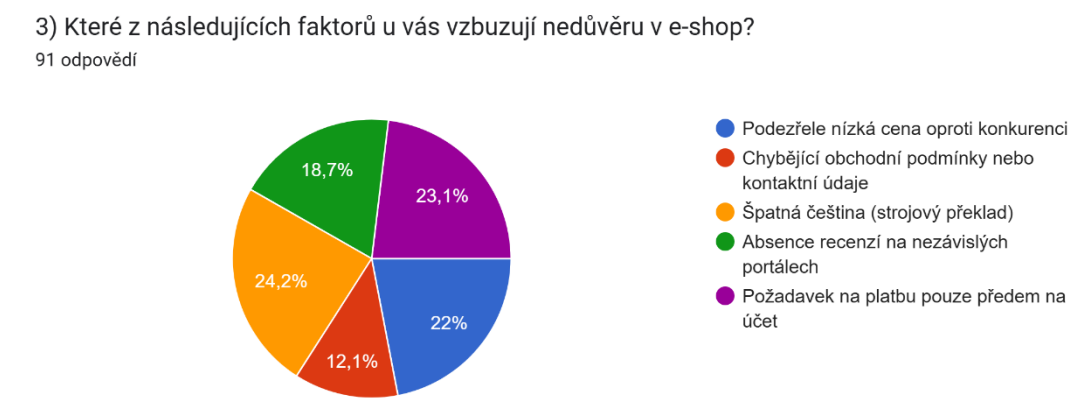


[52] Graf č. 2

[51] Google Forms

Nejvíce respondentů preferuje na e-shopech platbu přes tzv. platební brány, například PayPal, Apple Pay atd., (41,8 %), druhý nečastější způsob je platba kartou online (25,3 %), třetí nejčastější způsob je platba na tzv. dobírku (22 %) a poslední způsob je převod na účet předem (11 %).

Otázka č. 3 – Které z následujících faktorů u vás vzbuzují nedůvěru v e-shop?



[53] Graf č. 3

U oslovených respondentů vzbuzuje nejvíce nedůvěru faktor, pokud je e-shop tzv. strojově přeložen, tedy špatná gramatika apod. (24,2 %), druhý nejčastější faktor je požadavek na platbu předem na účet (23,1 %), třetím nejčastějším faktorem je podezřele nízká cena oproti konkurenci (22 %), dalším faktorem vzbuzujícím podezření je absence recenzí na nezávislých portálech (18,7 %) a posledním faktorem je chybějící obchodní podmínky, nebo kontaktní údaje na e-shopu (12,1 %).

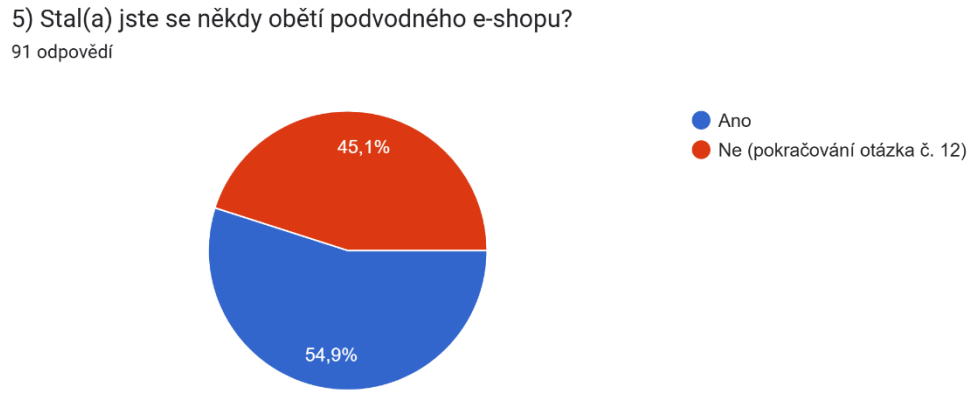
Otázka č. 4 – Prověřujete si e-shop před nákupem na stránkách ČOI (seznam rizikových e-shopů) nebo policie?

[52] Google Forms
[53] Google Forms

[54] Graf č. 4

Graf číslo 4 odpovídá na otázku, zda si oslovení respondenti prověřují e-shop na stránkách České obchodní inspekce. Nejčastější odpovědí bylo Nikdy (51,8 %), druhou nejčastější odpovědí bylo Výjimečně (24,2 %), třetí odpověď byla Vždy (15,4 %) a poslední odpověď, Skoro vždy (8,8 %).

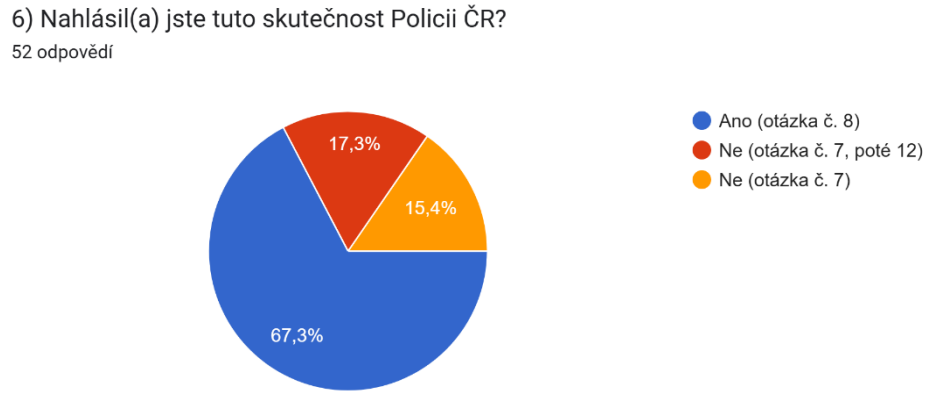
Otázka č. 5 – Stal(a) jste se někdy obětí podvodného e-shopu?



[55] Graf č. 5

Na otázku číslo 5 odpovědělo celkem 91 respondentů. Otázkou bylo, zda se respondent stal někdy obětí podvodného e-shopu. Ano odpovědělo 54,4 % respondentů a Ne odpovědělo 45,1 % respondentů.

Otázka č. 6 – Nahlásil(a) jste tuto skutečnost Policii České republiky?

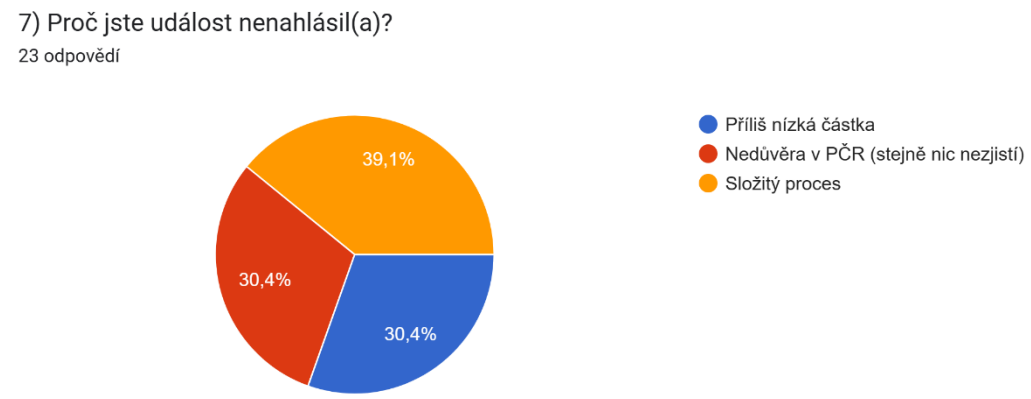


[56] Graf č. 6

Graf číslo 6 znázorňuje odpověď na otázku, zda respondent nahlásil skutečnost, že se stal poškozeným na Policii České republiky. Ano odpovědělo 67,3 % respondentů. Ne odpovědělo v součtu 32,7 % respondentů.

[54] Google Forms
[55] Google Forms
[56] Google Forms

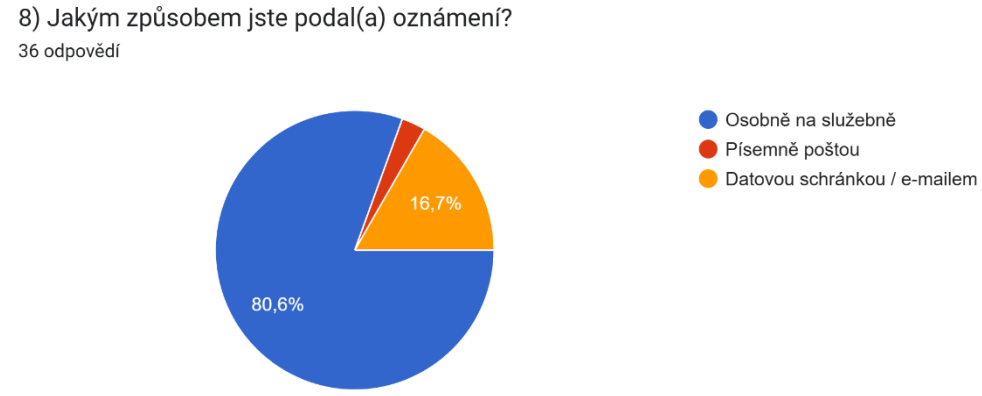
Otázka č. 7 – Proč jste událost nenahlásil(a)?



[57] Graf č. 7

Na otázku, proč nebyla událost nahlášena na Policii České republiky odpovědělo 39,1 % respondentů, že z důvodu složitého procesu. Shodně 30,4 % respondentů odpovědělo, že z důvodu nedůvěry v Policii a z důvodu příliš nízké částky, o kterou přišli.

Otázka č. 8 – Jakým způsobem jste podal(a) oznámení?



[58] Graf č. 8

Graf číslo 8 odpovídá na otázku, jakým způsobem bylo podáno oznámení o protiprávním jednání na Policii České republiky. Největší procento, tedy 80,6 % respondentů odpovědělo, že osobně na služebně Policie České republiky. Dále 16,7 % respondentů odpovědělo, že podání poslali datovou schránkou a minimální množství respondentů odpovědělo, že oznámení podali písmě poštou.

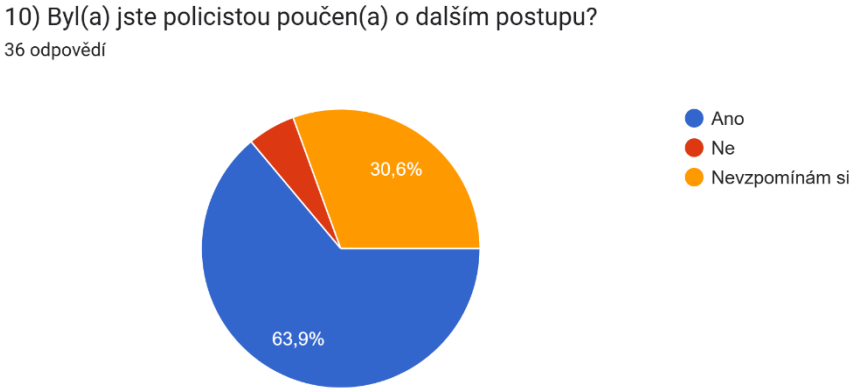
[57] Google Forms
[58] Google Forms

Otázka č. 9 – Byly ve Vašem případě zahájeny úkony trestního řízení?

[59] Graf č. 9

Graf číslo 9 odpovídá na otázku, zda byly v konkrétním případě dotazovaných respondentů zahájeny úkony trestního řízení. 63,2 % respondentů uvedlo, že ne, jelikož se jednalo o jednání v rovině přestupku a 36,8 % dotazovaných odpovědělo, že ano, jelikož se jednalo o trestný čin.

Otázka č. 10 – Byl(a) jste policistou poučen(a) o dalším postupu?

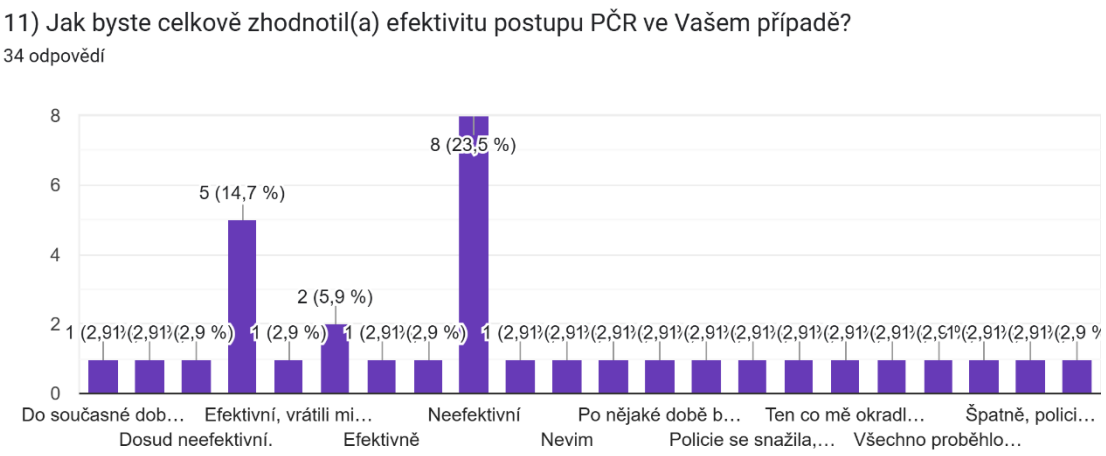


[60] Graf č. 10

Graf číslo 10 odpovídá na otázku, zda byl respondent poučen o dalším postupu v rámci šetření případu Policií, kdy 63,9 % respondentů odpovědělo, že ano. Dalších 30,6 % respondentů odpovědělo, že si již nevzpomíná a minimální množství dotazovaných odpovědělo na otázku, že ne.

[59] Google Forms
[60] Google Forms

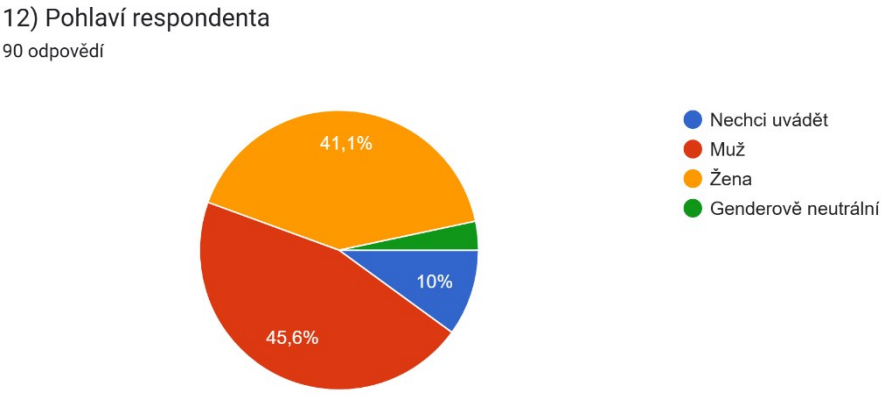
Otázka č. 11 – Jak byste celkově zhodnotil(a) efektivitu postupu Policie České republiky ve Vašem případě?



[61] Graf č. 11

Na otázku, jak by celkově dotazovaný respondent zhodnotil efektivitu postupu Policie České republiky, odpovědělo nejvíce dotazovaných, celkem 23,5 %, že postup byl neefektivní. Dalších 14,7 % respondentů odpovědělo, že postup byl efektivní, jelikož se jim vrátily finanční prostředky, o které přišli. Další odpovědi se pohybovaly okolo 3 %.

Otázka č. 12 – Pohlaví respondenta



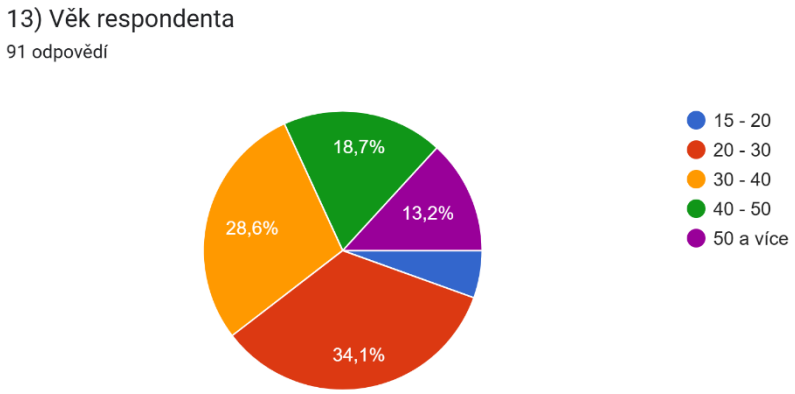
[62] Graf č. 12

Graf číslo 12 odpovídá na otázku pohlaví respondentů. Z 90 odpovědí bylo 45,6 % mužů, 41,1 % žen a 10 % respondentů nechtělo pohlaví uvést a minimální množství respondentů odpovědělo, že jsou genderově neutrální.

[61] Google Forms
[62] Google Forms

Otázka č. 13 – Věk respondenta

[63] Graf č. 13



Graf číslo 13 odpovídal na otázku věku oslovených respondentů, kdy 34,1 % respondentů bylo ve věku mezi 20 – 30 let, 28,6 % respondentů bylo ve věku mezi 30 – 40 let, 18,7 % respondentů bylo ve věku mezi 40 – 50 let, 13,2 % respondentů bylo ve věku mezi od 50 a více a minimální množství dotázaných respondentů bylo ve veku od 15 do 20 let.

[63] Google Forms

Závěr

Závěr této bakalářské práce představuje komplexní shrnutí poznatků o mechanismech prověřování podvodných e-shopů a chování uživatelů v kybernetickém prostoru. Hlavním cílem práce bylo posoudit postup Policie České republiky, což bylo realizováno skrze podrobnou analýzu legislativního rámce a následnou aplikaci v rámci tří vypracovaných kazuistik. Z nich vyplývá, že ačkoliv je procesní postup policie od přijetí oznámení až po případné zahájení trestního stíhání metodicky jasně definován, v praxi se potýká s vysokou mírou anonymity pachatelů a technologickým náskokem, který podvodníci často využívají. Kazuistiky potvrdily, že pro úspěšné prověřování je kritických prvních několik hodin po nahlášení, kdy je ještě reálná šance na zajištění finančních prostředků na účtech, než dojde k jejich vyvedení do zahraničí, nebo do kryptoměnových peněženek.

Vedlejší cíl práce se zaměřil na reflexi reality očima běžných uživatelů internetu. Dotazníkové šetření, do něhož se zapojilo 93 respondentů, odhalilo fascinující rozpor mezi subjektivním pocitem bezpečí a reálnou mírou opatrnosti. Přestože se většina účastníků považuje za informované, výsledky jasně identifikovaly rizikové faktory, které veřejnost systematicky přehlíží. Opatření, která by mohla současný stav zlepšit, se týkají zejména policejního postupu, kde jde především o nutnost zrychlení komunikace mezi orgány činnými v trestním řízení a bankovními institucemi.

Závěrem lze konstatovat, že stanovené cíle bakalářské práce byly naplněny. Práce poskytuje ucelený pohled na to, jak státní aparát reaguje na specifickou formu internetové kriminality, a zároveň varovně ukazuje, kde jsou nejslabší články řetězce bezpečnosti – tedy v našem vlastním chování. Boj proti podvodným e-shopům není jen otázkou výkonnosti policie, ale především otázkou kultivace digitální obezřetnosti každého z nás. Je zřejmé, že dokud bude poptávka po „zázračně levném“ zboží z pochybných zdrojů, bude existovat i nabídka ze strany sofistikovaných podvodníků, kteří se jen velmi těžko dopadají.

Seznam použitých zdrojů

Literární zdroje

1. DRAŠTÍK, Antonín a FREMR, Robert. Trestní zákoník: komentář. 1. díl. Praha: Wolters Kluwer, 2015. 1568 s. ISBN 978-80-7478-790-4.
2. DONÁT, Josef a TOMÍŠEK, Jan. Právo v síti: Průvodce právem na internetu. Praha: C. H. Beck, 2016. 350 s. ISBN 978-80-7400-610-4.
3. FEREBAUEROVÁ, R., PEKÁREK, O. Aplikovaná informatika. 1. vydání. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. 151 s. ISBN 978-80-87472-74-3.
4. JELÍNEK, Jiří. Trestní právo procesní. 7. aktualizované a doplněné vydání. Leges, 2023. 960 s. ISBN 978-80-7502-687-3.
5. JIRÁSEK, Petr. Cyber security glossary. Páté doplněné a upravené vydání. Centrum kybernetické bezpečnosti, z. ú., 2022. 352 s. ISBN 978-80-908388-4-0.
6. JIROVSKÝ, Václav. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2.
7. KOLOUCH, Jan. Cybercrime [online]. CZ.NIC, z. s. p. o., 2016. 511 s. ISBN 978-80-88168-16-4.
8. KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-271-9074-4.
9. Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech. Praha: Policejní akademie České republiky v Praze a kolektiv autorů, 2020. 214 s. ISBN 978-80-7251-505-9.
10. PORADA, Viktor a RAK, Roman. Kriminalita související s informačními a komunikačními technologiemi a identifikace osob na základě projevu lokomoce člověka. Druckvo, spol., 2007. 262 s. ISBN 978-80-254-0797-4.
11. SMEJKAL, V. Kybernetická kriminalita. 2. vydání. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.
12. SMEJKAL, Vladimír. Kybernetická kriminalita. Třetí rozšířené a aktualizované vydání. Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.
13. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Aleš Čeněk, 2019. 378 s. ISBN 978-80-7380-765-8.

14. ŠTĚDROŇ, B. JAŠEK, R.; SVÍTEK, M. a kol. Umělá inteligence a právo. Plzeň: Aleš Čeněk, 2024. 233 s. ISBN 978-80-7380-947-8.

15. VANTUCH, Pavel. Trestní zákoník s komentářem. ANAG, 2011. 1356 s. ISBN 978-80-7263-677-8.

16. ÚZ Trestní předpisy. Sagit, 2024. 511 s. ISBN 978-80-7488-634-8.

Elektronické zdroje

1. Jednotlivé druhy kyberkriminality. Online. Policie ČR. 2024. Dostupné z: https://policie.gov.cz/clanek/jednotlive-druhy-kyberkriminality.aspx. [cit. 2026-01-15].
2. Kybernetická kriminalita - fenomén dneška. Online. PRÁVNÍ PROSTOR. 2015. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/kyberneticka-kriminalita-fenomendneska. [cit. 2024-09-09].
3. MINISTERSTVO PRŮMYSLU A OBCHODU. *Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů* [online]. Praha: Ministerstvo průmyslu a obchodu, Odbor živností a spotřebitelské legislativy, 13. ledna 2025 [cit. 2026-01-27]. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--ktere-kopiruji-weby-znamych-obchodu--289453/
4. Kyberneticka_kriminalita.pdf. POKORNÝ, Pavel. Kyberkriminalita [online]. Zlín, 2016. Diplomová práce
5. KORMOŠOVÁ, I. Podvody na internetu [online].[cit. 2023-10-11]. Dostupné z WWW: https://www.policie.cz/clanek/podvody-na-e-shopech.aspx.
6. Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů. Online. 2025. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--ktere-kopiruji-weby-znamych-obchodu--289453/#:~:text=*%20Aktu%C3%A1ln%C3%AD%20informace.%20*%20Bezpe%C4%8Dnost%20v%C3%BDrobk%C5%AF. [cit. 2026-03-24].
7. POŽÁR, Josef. Specifické problémy boje s kybernetickou kriminalitou. Online. 2025. Dostupné z: https://mv.gov.cz/soubor/policejni akademie.aspx#:~:text=(Zdroj%20informac%C3%AD:%20resortn%C3%AD%20materi%C3%A1l%20%E2%80%9EAnal%C3%BDza%20aktu%C3%A1ln%C3%AD%20%C3%BArovn%C4%9B,kter%C3%A9%20se%20pod%C3%ADlej%

C3%AD%20na%20vy%C5%A1et%C5%99ov%C3%A1n%C3%AD%20kybernetick%C3%A9%20kriminality.. [cit. 2026-03-24].

8. Phishing. Online. Www.eset.com/cz/phishing. 2025. Dostupné z: https://www.eset.com/cz/phishing/#:~:text=Phishing%20je%20typ%20kybernetick%C3%A9ho%20%C3%BAtoku,nebo%20prod%C3%A1vaj%C3%AD%20na%20%C4%8Dern%C3%A9m%20trhu.. [cit. 2026-03-25].
9. Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád). Online. Zákony pro lidi. 2026. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141. [cit. 2026-03-25].
10. Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV. Online. 2026 Policie ČR. 2026. Dostupné z: https://policie.gov.cz/clanek/narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite.aspx. [cit. 2026-03-25].
11. Vishing a spoofing. Online. Policejní prezidium ČR. 2021. Dostupné z: https://policie.gov.cz/clanek/vishing-a-spoofing.aspx. [cit. 2026-03-25].
12. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: Zákony pro lidi.cz [online]. [cit. 2026-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40.
13. ČESKO. Zákon č. 370/2017 Sb., o platebním styku. In: Zákony pro lidi.cz [online]. [cit. 2026-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-370.

Seznam zkratek

ČOI -	Česká obchodní inspekce
DPD -	Dynamic Parcel Distribution
DPH -	daň z přidané hodnoty
ETŘ -	Evidence trestního řízení
IP adresa -	Internet Protocol (internetový protokol)
NP -	neznámý pachatel
NÚKIB -	Národní úřad pro kybernetickou a informační bezpečnost
PČR -	Policie České republiky
PPP -	Pokyn policejního prezidenta
SKPV -	Služba kriminální policie a vyšetřování
SIM karty -	Subscriber Identity Module (účastnická identifikační karta)
TČ -	trestný čin
Tr. řádu -	Trestního řádu
Tr. zák. -	Trestního zákoníku
TZ -	Trestní zákoník
URL adresa -	Uniform Resource Locator (v češtině jednotný lokátor zdrojů)
ÚO -	územní odbor
ZKB -	Zákon o kybernetické bezpečnosti

Seznam tabulek a grafů

Seznam příloh

PŘÍLOHY

Příloha – dotazník

Cílem mého výzkumu je zmapovat, jak se my, uživatelé internetu, chováme při online nákupech, a především zjistit, jaké jsou reálné zkušenosti s postupem policie v případech, kdy k podvodu dojde. Vaše odpovědi mi pomohou identifikovat slabá místa v prevenci i v následném procesu prověřování trestné činnosti.

- **Anonymita:** Dotazník je plně anonymní a získaná data budou použita výhradně pro účely mé bakalářské práce.
- **Časová náročnost:** Vyplnění vám zabere přibližně **5–8 minut**.
- **Pro koho:** Dotazník je určen pro každého, kdo nakupuje na internetu – i pro ty, kteří se (naštěstí) s podvodem zatím nesetkali.

Odkaz naleznete zde:

https://docs.google.com/forms/d/e/1FAIpQLSfUkHtZ2P26931FAEXZq_2U5rWh9SfR4HqRE0ronfaSRluYfQ/viewform?usp=dialog

Předem vám děkuji za vaši ochotu a čas. Velmi si vážím vaší pomoci při tvorbě mé závěrečné práce

1) Jak často nakupujete na e-shopech?

- Několikrát týdně
- Jednou týdně
- Několikrát měsíčně
- Jednou měsíčně
- Vůbec

2) Jaký platební nástroj preferujete při nákupu na neznámém e-shopu?

- Dobírka
- Platba kartou online
- Převod na účet předem
- Platební brány (např. PayPal, Apple Pay)

3) Které z následujících faktorů u vás vzbuzují nedůvěru v e-shop?

- Podezřele nízká cena oproti konkurenci
- Chybějící obchodní podmínky nebo kontaktní údaje
- Špatná čeština (strojový překlad)
- Absence recenzí na nezávislých portálech
- Požadavek na platbu pouze předem na účet

4) Prověřujete si e-shop před nákupem na stránkách ČOI (seznam rizikových e-shopů) nebo policie?

- Vždy
- Skoro vždy
- Výjimečně
- Nikdy

5) Stal(a) jste se někdy obětí podvodného e-shopu?

- Ano
- Ne (pokračování otázka č. 12)

6) Nahlásil(a) jste tuto skutečnost Policii ČR?

- Ano (otázka č. 8)
- Ne (otázka č. 7, poté 12)

7) Proč jste událost nenahlásil(a)?

- Příliš nízká částka
- Písemně poštou
- Datovou schránkou / e-mailem

9) Byly ve Vašem případě zahájeny úkony trestního řízení?

- Jednalo se o trestný čin (škoda nad 10.000,-Kč, popřípadě jiné okolnosti)
- Jednalo se o přestupek (škoda do 10.000,-Kč)

10) Byl(a) jste policistou poučen(a) o dalším postupu?

- Ano
- Ne
- Nevzpomínám si

11) Jak byste celkově zhodnotil(a) efektivitu postupu PČR ve Vašem případě?

- Otevřená otázka

12) Pohlaví respondenta

- Nechci uvádět
- Muž
- Žena
- Genderově neutrální

13) Věk respondenta

- 15 – 20
- 20 – 30
- 30 – 40
- 40 – 50
- 50 a více