Podvody na prodejních portálech a souvisejících službách

František Tragan

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**František Tragan**
Osobní číslo:	**A20489**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Podvody na prodejních portálech a souvisejících službách**
Téma práce anglicky:	**Fraud on Sales Portals and Related Services**

Zásady pro vypracování

1. Seznamte se s hrozbami, které jsou na obchodních portálech.
2. Vysvětlete způsoby a možnosti odhalení těchto hrozeb.
3. Identifikujte a popište metody, které podvodníci používají nejčastěji.
4. Proveďte průzkum, jak lidé reagují, pokud přijdou do styku s internetovým podvodníkem.
5. Navrhněte metodický postup, jak se vyhnout podvodům a nestát se obětí, případně jak postupovat, pokud se to stane.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. *Bezpečně na internetu průvodce chováním ve světě online*. 6137. U Průhonu 22, Praha 7: Grada, 2016. ISBN 978-80--271-9074-4.
2. *CyberCrime*. Praha: Edice CZ.NIC, 2016. ISBN 978-80-88168-15-7.
3. *EGovernment bezpečně*. Praha: Grada, 2008. ISBN 978-80-247-2462-1.
4. *Platby na internetu prostřednictvím platebních karet*. Praha, 2012. Diplomová práce. Bankovní institut vysoká škola Praha, Katedra bankovnictví a pojišťovnictví.
5. *Využití metod sociálního inženýrství pro etický hacking*. Hradec Králové, 2017. Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu.
6. 15 Examples of Real Social Engineering Attacks. *Tessian* [online]. London: Tessian Limited, 2022 [cit. 2022-10-18]. Dostupné z: https://www.tessian.com/blog/examples-of-social-engineering-attacks/

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **13. prosince 2022**
Termín odevzdání bakalářské práce: **5. června 2023**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 13. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 31.5.2023

František Tragan, v.r.
podpis studenta

ABSTRAKT

Cílem této bakalářské práce je poukázat na hrozby které se vyskytují na internetu v oblasti webových obchodních portálů, jak tyto hrozby hned na začátku odhalit a co udělat pro to, aby k nim nedošlo. Součástí teoretické části je popis hrozeb na internetu a kde se s nimi můžeme setkat. Dále je zde také uveden popis metod, které podvodníci využívají. Praktická část je rozdělena do dvou oblastí. První oblast je zaměřena na výzkum zkušeností uživatelů s internetovými podvody a jak uživatelé v případě zjištění reagují. Druhá oblast je zaměřena na vytvoření metodického návodu, jak se chovat, aby se člověk nestal objetí internetového podvodu.

Klíčová slova: Podvod, podvodník, obchodní portál, oběť, metody.

ABSTRACT

The aim of this bachelor's thesis is to point out the threats that occur on the internet in the area of web business portals, how to detect these threats at the very beginning and what to do to prevent them from happening. Part of the theoretical part is a description of threats on the internet and where we can encounter them. Furthermore, there is also a description of the methods used by fraudsters. The practical part is divided into two areas. The first area is focused on researching users' experiences with internet fraud and how users react in case of detection. The second area is focused on the creation of methodical instructions on how to behave so that one does not become a victim of internet fraud.

Keywords: Fraud, fraudster, business portal, victim, methods.

Děkuji vedoucímu práce panu Ing. Lukáši Králíkovi, Ph.D. za odborné vedení, čas a rady při zpracovávání bakalářské práce. Dále chci poděkovat svým rodičům a kamarádům za podporu, které se mi dostalo během celé doby studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V současné době se podvody na webových obchodních portálech a souvisejících službách stávají čím dál tím větším tématem. Jejich nárůst se oproti minulým rokům výrazně zvýšil. V roce 2011 bylo zaznamenáno 1502 prokázaných internetových podvodů a v roce 2022 již bylo zaznamenáno 18 554 prokázaných internetových podvodů[1][2][3]. Tyto čísla demonstrují to, jak závažným problémem tato problematika je. Podvodníci nejčastěji využívají pro oklamání svojí oběti techniku sociálního inženýrství, která je v jejich provedení velmi účinná. Pokud jim tato technika vyjde, tak se snaží od svojí oběti získat její citlivá data. Bývají to zpravidla její přihlašovací údaje do internetového bankovnictví, Google účtu nebo údaje o platební kartě. Zároveň pokud se oběť stane cílem internetového podvodu, je velmi těžké skoro až nemožné tyto podvodníky dopadnout. Z tohoto důvodu vznikla tato bakalářská práce, která má upozornit na metody podvodníků a seznámit s nimi obyvatele České republiky.

Teoretická část bakalářské práce se skládá z pěti částí. První část pojednává o webových obchodních portálech či jiných službách, které internetoví podvodníci využívají nejčastěji. Druhá část je zaměřena na způsoby plateb, kterými lze platit na webových obchodních portálech. Třetí část rozebírá cílové skupiny podvodníků a jak se případné pokusy o podvod u jednotlivých skupin liší. Čtvrtá část pojednává o popise metod sociálního inženýrství, které podvodníci využívají k provádění podvodů. Poslední pátá část je zaměřena na webové obchodní portály a konkrétně na to, jak případně odhalit falešný obchodní portál.

Praktická část se dělí na dvě části. Obsahem první části je zpracování výsledků dotazníkového šetření, které je vedené za účelem zjištění, jaké mají obyvatelé České republiky zkušenosti s internetovými podvody. Vytvořený dotazník se skládá ze čtyř základních okruhů. První okruh se týká obchodních portálů a jejich využívání, druhá část je zaměřena na způsoby plateb na obchodních portálech, třetí část pojednává o výzkumu zkušeností respondentů s internetovými podvodníky a čtvrtá část zkoumá reakce respondentů na internetový podvod. Druhá polovina praktické části obsahuje metodický návod, jak se bezpečně chovat v internetovém prostředí obchodních portálů, aby se člověk nestal obětí internetových podvodníků.

I. TEORETICKÁ ČÁST

1 OBCHODNÍ PORTÁLY, KDE NEJČASTĚJI DOCHÁZÍ K POKUSŮM O PODVOD

V dnešní době většina obyvatel ČR využívá pro nákup případně prodej zboží webové obchodní portály. Bohužel s velkým vytížením těchto portálů přichází i velký počet podvodů na těchto stránkách. V níže uvedené kapitole jsou popsány webové obchodní portály, kde se s podvodníky lze setkat.

1.1 E-commerce

E-commerce zahrnuje všechny obchodní transakce, které se uskutečňují pomocí internetu nebo elektronických komunikačních prostředků. Může se týkat různých typů obchodu jako jsou internetové obchody, online reklama, affiliate marketing a online tržiště. Může se také rozdělit podle zaměření na typ zákazníka jako je B2B (podniky mezi sebou), B2C (podniky a spotřebitelé), C2B (spotřebitelé a podniky) nebo C2C (spotřebitelé mezi sebou). Prodej a nákup zboží a služeb se uskutečňují pomocí počítačových sítí, zatímco platba a dodání mohou být provedeny online nebo offline. Obchodní portály, které do této skupiny můžeme zařadit, jsou např. Alza nebo Mall. [4][5]

1.2 Aukční a Inzertní portály

Mezi tyto portály lze zařadit většinu webových obchodních portálů, které zákazníci pro své nákupy používají. Níže jsou tyto portály blíže vysvětleny.

1.2.1 Aukční stránky

Aukční stránky jsou internetové portály, které umožňují lidem prodávat a nakupovat zboží pomocí aukčního systému. Prodejci na aukčních stránkách nabízejí své zboží k prodeji a zájemci o předmět mohou začít licitovat, což znamená, že nabízejí vyšší a vyšší ceny za předmět. Licitace trvá určitou dobu a po jejím skončení vítězný licitátor získá předmět za nejvyšší cenu, kterou nabídl. Aukční stránky obvykle také umožňují prodejcům prodávat předměty za fixní cenu, což je cena, za kterou se předmět prodává bez ohledu na to, kolik lidí se o něj uchází. Mezi známější světové aukční stránky patří eBay, Amazon a mnoho dalších. Na území České republiky jsou nejvíce používané stránky jako Aukro, Sbazar. [4][5]

1.2.2 Inzertní stránky

Inzertní portály jsou internetové stránky, které slouží jako prostředek pro zveřejňování inzerátů. Jsou určené pro lidi, kteří hledají různé typy zboží nebo služby. Inzertní portály se mohou zabývat různými tématy, jako je prodej a nákup osobních věcí, práce, bydlení atd. Mezi nejznámější české inzertní portály patří Aukro, Bazoš, Sbazar, Heureka nebo zboží.cz. [6]

1.3 Sociální sítě

Sociální sítě jsou internetové platformy, které umožňují lidem vytvářet a udržovat online kontakty s přáteli. Sociální sítě poskytují uživatelům možnost sdílet fotografie, videa, vytvářet inzeráty a další obsah s ostatními uživateli. Uživatelé si také mohou vytvářet skupiny nebo stránky s různými tématy, která jsou zaměřená na konkrétní oblasti zájmu nebo komunity. Mezi nejznámější sociální sítě patří například Facebook, Instagram, Twitter či WhatsApp.

1.3.1 Facebook Markeplace

Facebook Marketplace je služba Facebooku, která umožňuje uživatelům prodávat a kupovat zboží a služby v jejich okolí. Tato služba je zdarma a je k dispozici na webu nebo v aplikaci pro iOS a Android. [7]

1.3.2 Instagram Marketplace

Instagram Marketplace je platforma na Instagramu, která umožňuje uživatelům prohlížet a nakupovat produkty přímo z Instagramu. Instagram Marketplace lze použít k nalezení produktů, které zákazníka zajímají a k procházení kategorií, jako jsou oblečení, móda, doplňky, šperky a mnoho dalšího. I tato služba je zdarma a je k dispozici v aplikaci pro iOS i Android. [7]

1.4 Běžné obchodní portály

Do této skupiny patří především obchodní portály využívané na denní bázi. Je možné tyto portály dělit podle typu produktů, které prodávají. Jedná se zejména o obchody s elekronikou (Alza, CZC, TSBohemia …), oblečením (Vinted, About You, Adidas …), jídlem (Dáme jídlo, Wolt, KFC …), kosmetikou (Notino …), hrami (xZone, JRC …) atd. Mezi portály lze

také považovat streamovací platformy jako např. Twitch, ale i Netflix, HBO, Voyo či Disney+.

1.5 Přepravní společnosti

Nejen na obchodních portálech se můžeme setkat s podvody. Podvodníci se zaměřují i na přepravní společnosti, které objednané zboží přepravují a vydávají se za ně. Níže je uvedeno několik známějších a často využívaných přepravců.

1.5.1 Česká pošta

Česká pošta je nejstarším českým přepravcem zásilek. V dnešní době je ale méně využívaná. Nabízí služby přepravy dopisů, balíků, platební a finanční služby či možnost koupě elektronické dálniční známky a eGovernment.[8]

1.5.2 PPL, DHL, DPD, Zásilkovna

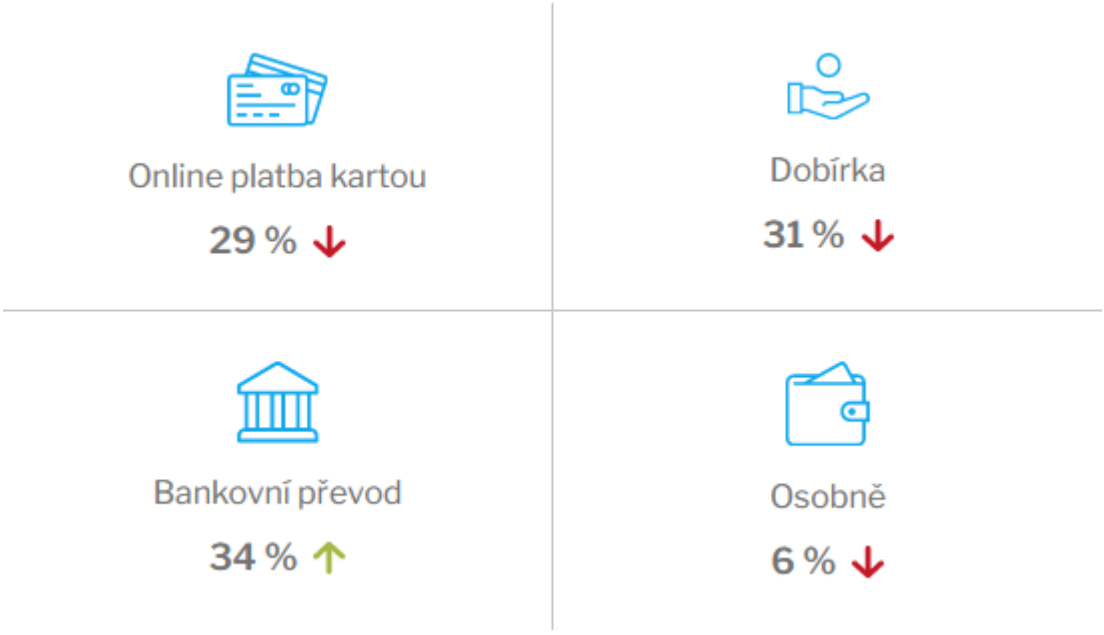
Tyto přepravní společnosti patří mezi nejvíce rozšířené a nejvíce využívané na území České republiky. Zaměřují se především na přepravu balíků. Svoje služby provozují nejen na území Česka, ale i v zahraničí.[9]

2 PLATBY NA INTERNETU

Platba přes internet je charakteristická především tím, že provedená platba se uskutečňuje přímo přes internetové rozhraní a probíhá okamžitě. Tento typ platby především využívá pro provedení platby platební bránu nebo bankovní převodem. Tyto platby umožňují zákazníkům platit za nákupy na webových obchodních portálech a ušetřit tak čas a úsilí. Přesto však mohou být spojeny s určitými riziky, jako je možnost zneužití osobních údajů nebo ztráta peněz při podvodných transakcích.

2.1 Způsoby plateb přes internet

Při nákupu přes internet máme na výběr hned z několika možností plateb. Mezi nejběžnější způsoby patří dobírka, bankovní převod či platební karta. Na níže uvedeném obrázku jsou aktuální statistiky jednotlivých druhů platebních metod (Obrázek 1) [10][11]

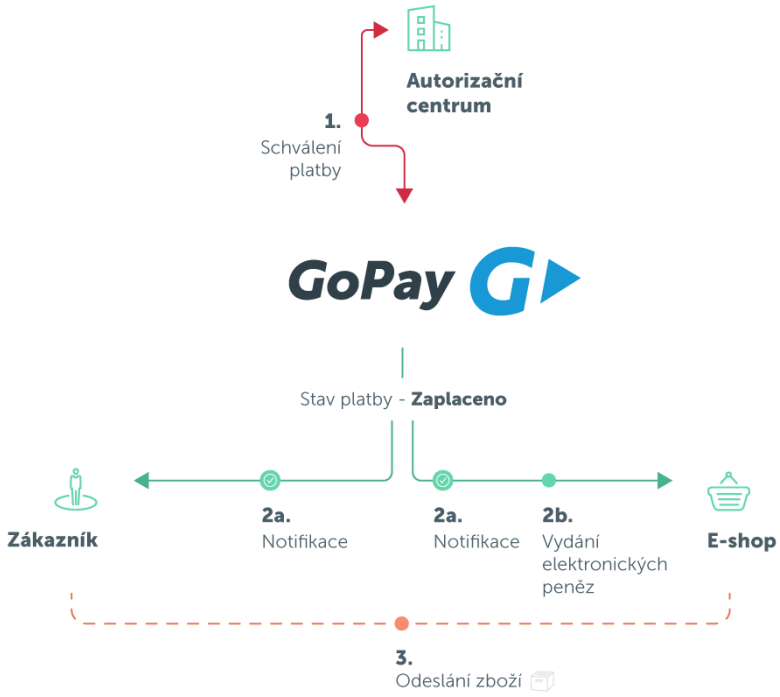


Obrázek 1. Statistiky platebních metod [1]

2.1.1 Platební karta

Platba kartou přes internet umožňuje zákazníkům platit za zboží pomocí kreditní, debetní nebo virtuální karty kdykoliv a odkudkoliv. Je to velmi jednoduchá a bezpečná platba díky použití zabezpečeného protokolu HTTPS, který šifruje údaje z karty. Pro provedení platby systém vyžaduje zadání čísla karty, datumu platnosti a CVC kódu, který je umísěn na zadní straně platební karty. Pokud se platba provádí v systému 3 D Secure, zákazník potvrzuje

platbu pomocí mobilní aplikace dané banky, která mu pošle upozornění o prováděné platbě a zákazník tuto platbu musí v mobilní aplikaci potvrdit, aby platba úspěšně proběhla. Poté systém GoPay posílá e-shopu notifikaci o přijaté platbě a současně informuje zákazníka e-mailem o provedené platbě (Obrázek 2).[10][11][12][13]



Obrázek 2. Schéma průběhu platby kartou [12]

2.1.2 Bankovní převod

Aby bylo možné provést bankovní převod, je nutné mít zřízené elektronické bankovnictví. Výhodou je, že platba je bezhotovostní a s minimálními náklady, ale nevýhodou je, že prodejce zboží expeduje až po připsání platby na jeho účet. Převod lze provést kdykoliv po potvrzení objednávky, ale aby byla částka připsána na účet prodejce, musí být proveden nejpozději do pěti pracovních dnů od potvrzení objednávky, jinak je objednávka zrušena. Rizikem je, že platba nemusí být spárována nebo že obchodník je podvodník.[10][11]

2.1.3 Dobírka

Platba na dobírku je stále nejpoužívanější a nejstarší metodou placení při nákupu na internetu v České republice. Její výhodou je, že si zboží můžeme objednat a zaplatit až při jeho fyzickém převzetí od přepravní společnosti (PPL, Česká pošta, DPD) a tak má zákazník jistotu,

že k němu jeho objednávka dorazila. Nevýhodou je, že i když je již balík doručený, zákazník ho nemůže otevřít, dokud zásilku kurýrovi nezaplatí. [10][11][14]

2.1.4 Zabezpečení plateb kartou

Česká národní banka reguluje platební brány jako platební instituce, proto ke svému provozu musí mít schválenou licenci. Ministerstvo financí je nadřízeným orgánem, který se stará o dohled nad těmito institucemi. Platební brány jsou tedy podrobeny přísným regulacím a kontrolám, aby byly zajištěny jejich bezpečnost a spolehlivost. Pro zabezpečení plateb se také vztahuje zákon č. 370/2017 Sb. o platebním styku. [12] [13] [15]

2.1.4.1 3D secure

3D secure je systém zabezpečení plateb přes internet, který byl vytvořen společnostmi Visa a Mastercard. Tento systém funguje tak, že při platbě přes internet je platící zákazník přesměrován na zabezpečenou platební stránku své banky, kde po zadání údajů z karty mu banka zašle upozornění do mobilní aplikace dané banky, ve které je nutné platbu odsouhlasit, aby byla schválena a provedena. [11]

2.1.4.2 Bezpečnostní standard PCI DSS

PCI DSS je standard, který stanovuje pravidla pro zpracování citlivých dat platebních karet. Jeho cílem je zajistit bezpečnost těchto dat a chránit je před zneužitím. Tento standard musí dodržovat každá instituce, která se zabývá zpracováním platebních karet. Standard obsahuje různé stupně přísnosti, přičemž nejvyšší stupeň Level 1 je nejpřísnější a vyžaduje zavedení náročných technických opatření. Jediná nebankovní služba, která splňuje PCI DSS Level 1, je služba GoPay. [12] [13]

2.1.4.3 Možnost reklamace

Pokud e-shop nedodrží obchodní podmínky, má zákazník právo reklamovat platbu kartou.

2.1.5 Druhy platebních karet

Existují různé druhy platebních karet, které se liší v několika aspektech, jako je například typ, způsob použití, poskytované benefity nebo cílová skupina. Nejčastější druhy platebních karet, jsou uvedeny níže.

2.1.5.1 Kreditní karty

Díky kreditní kartě může zákazník platit za svoje zboží, nicméně prostředky, které k platbě používá, nejsou jeho nýbrž banky, která kartu vydala. Kreditní karty jsou obvykle vydávány s nabídkami různých benefitů. [10][11] [13]

2.1.5.2 Debetní karty

Debetní karta je nejvíce používanou platební kartou. Pokud zákazník platí touto kartou, platí vlastními penězi, které má na svém účtu v bance. Její platnost vždy určuje banka, která ji vydala. Při použití této karty se peníze okamžitě odečtou z účtu a není nutné je tedy splácet. [10][11][13]

2.1.5.3 Virtuální karty

Virtuální karta je druh platební karty, která neexistuje ve fyzické podobě. Virtuální karty se využívají především pro placení na internetu nebo v aplikacích a nevyžadují fyzické vydání karty. Držitel virtuální karty obdrží informace o kartě, které potřebuje k jejímu použití, obvykle jsou tyto informace k dispozici v mobilní aplikaci banky nebo internetovém bankovnictví. [13]

2.1.5.4 Charge karta

Tento typ karty se vyznačuje tím, že uživatelé nemusí platit za nákupy ihned, ale mohou si je rozložit do několika splátek. Charge karty se často používají k nákupu dražšího zboží nebo služeb, ale uživatelé musí splácet určitou částku každý měsíc a také platit poplatky za používání karty. Charge karty jsou často zaměňovány s kreditními kartami. Zatímco kreditní karty poskytují uživatelům půjčku, charge karty jim umožňují rozložit náklady nákupu na několik splátek[10][11] [13]

2.2 Nebankovní poskytovatelé platebních služeb

Nebankovní poskytovatelé platebních služeb jsou společnosti nebo organizace, které poskytují platební služby, aniž by byly bankou. Níže jsou uvedeny jednotlivé příklady těchto systémů.

2.2.1 Mobilní platby

Tyto platby jsou obvykle realizovány pomocí aplikace na telefonu, která je spojena s účtem platby. Mezi příklady společností poskytujících mobilní platby patří Apple Pay a Google

Pay. Tyto společnosti poskytují bezpečný a rychlý způsob platby prostřednictvím mobilního telefonu.[13]

2.2.2 PayPal

Jedná se o jednu z nejvíce používaných bezpečných platebních metod přes internet. PayPal si můžeme představit jako elektronickou peněženku. Po založení uživatelského účtu, který je propojený s platební kartou uživatele, lze provádět bezpečné platby přes tento portál. Pokud je pak založený účet propojen pomocí platební karty uživatele, je možné převádět peníze mezi jednotlivými účty. [16]

3 CÍLOVÉ SKUPINY

Věkové skupiny, na které se útočníci zaměřují, nelze vymezit. Útočníci se totiž snaží podvést veškeré věkové skupiny. Jediné, co se liší, je forma komunikace a druh podvodu, který je uzpůsoben dané věkové kategorii. Pokud by se ale měla zvolit věková skupina, na kterou se útočníci nejvíce zaměřují, tak dle výzkumu od společnosti ESET se jedná o lidi ve věku od 30 do 40 let [17]. Hlavním důvodem je, že tato věková skupina nejvíce využívá webové obchodní portály. V níže uvedené kapitole je popsáno rozdělení populace do věkových kategorií a případné komunikační cesty, díky kterým se k nim útočníci pokoušejí dostat.

3.1 Mladiství

Pokud se bavíme o mladistvých (14-18 let), tak ti se v dnešní době pohybují hlavně v online prostoru. Především na Instagramu, Tik Toku, Facebooku, různých streamovacích platformách atd. Proto se útočníci přizpůsobují tomuto trendu a snaží se komunikovat a okrást je těmito kanály. Samozřejmě i mladiství navštěvují různé obchodní portály, ale primárně jen kvůli tomu, aby se podívali na zboží a následně už dané produkty pořizují především jejich rodiče. Jedna z nejlepších metod, jak mladistvého přimět kliknout na falešnou reklamu, je přislíbení finanční odměny. To samozřejmě platí i pro starší věkové kategorie, nicméně mladší lidé jsou více nezkušení a mohou na rozdíl od starších tomuto podvodu uvěřit.

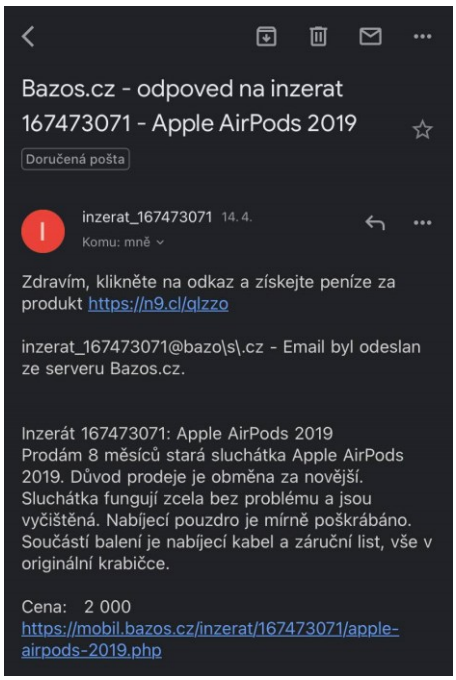
Obrázek 3. Podvod na sociálních sítích[18]

Na výše uvedeném Obrázek 3 je příklad falešné reklamy na platformě Facebook, kdy po prokliku přes odkaz se oběť přesměruje na falešné stránky MBank, kde je nabádána k tomu, aby se přihlásila do svého internetového bankovnictví. Takovýto typ reklam se samozřejmě nemusí vyskytovat jen na Facebooku. V jiné podobě se může objevovat na Instagramu, kdy oběti přijde do DM zpráv.[19]

3.2 Dospělí v raném věku

V této věkové skupině se bavíme o lidech ve věku od 19 do 40 let. Tato věková skupina stejně jako mladiství četně využívají sociální sítě a jiné platformy tohoto druhu, proto se na ně samozřejmě vztahují hrozby, které jsou zmíněné u mladistvých. Každopádně jak bylo zmíněno v úvodu této kapitoly, tak do této skupiny patří také lidé ve věku od 30 do 40 let, kteří jsou nejčastějšími adresáty potenciálních útoků. Dospělí v raném věku využívají prostředí na internetu na maximum. Neboli brouzdají nejen po sociálních sítích, ale v dnešní době začínají využívat služeb online obchodních portálů naplno. Proto se také stávají nejčastějšími adresáty útoků.

Forma útoku je však transformována. Oproti předešlému prokliku přes reklamu je teď hlavní formou kontakt útočníka s obětí. Oběť např. prodává zboží přes Bazoš a podvodník začne předstírat zájem o jeho zboží.



Obrázek 4. Podvod na Bazoši [Vlastní]

Na výše uvedeném Obrázek 4 je znázorněná e-mailová komunikace podvodníka. Který doufá, že oběť se proklikne přes odkaz na jím vytvořené falešné stránky Bazoše. [19]

Více o této a podobných technikách je uvedeno níže v práci. Dalším způsobem jak útočníci kontaktují oběť může být využití sociálních sítí nebo telefoního hovoru. [19]

3.3 Lidé středního věku

Do této věkové skupiny řadíme lidi od 40 do 60 let. Tito lidé se již příliš nepohybují na sociálních sítích a ani v takové míře jako předešlá skupina nevyužívají webové obchodní portály. Samozřejmě pro tuto skupinu platí hrozby uvedené výše, každopádně zde je důležité zmínit formu komunikace podvodníku přes telefonní hovor. Kdy tato forma komunikace je pro tuto věkovou skupinu přijatelnější než chatování přes sociální sítě. Obvykle se útočník vydává za někoho z banky a požaduje citlivé údaje od oběti. Podrobněji je tento útok popsán níže v práci.[19]

3.4 Lidé důchodového věku

V této věkové skupině jsou lidé od 60 let a výše. Tito lidé krom několika výjimek nevyužívají jakékoliv sociální sítě ani webové obchodní portály, proto si podvodníci volí jinou cestu. V drtivé většině případů, kdy je důchodce podveden podvodníky z online prostoru, je využitá forma telefonátu. Tato věková skupina je bohužel velmi naivní a důvěřivá, protože nemá dostatečné informace o tom, co jim v těchto případech hrozí. Proto se mohou stát snadným terčem podvodníků.[19]

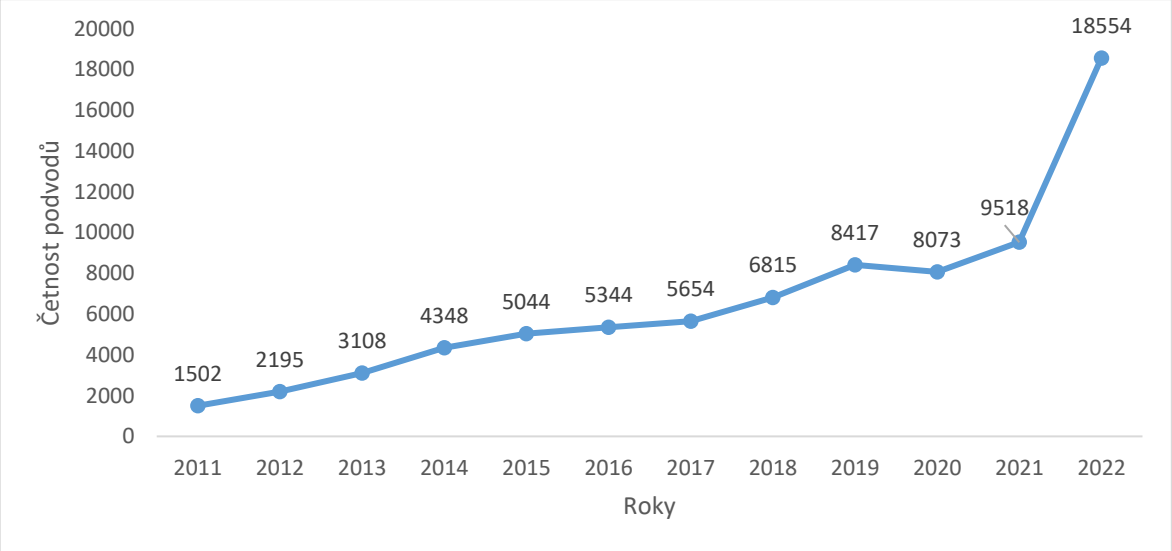
4 METODY VYUŽÍVANÉ PŘI INTERNETOVÝCH PODVODECH

Tato kapitola je zaměřena na historický vývoj útoků a jejich příklady. Dále se zabývá bližšímu upřesnění metod využívaných podvodníky a jak tyto podvody lze odhalit.

4.1 Vývoj podvodů v České republice

V České republice byl v posledních letech zaznamenán značný nárůst internetových podvodů. V níže uvedené kapitole je popsán vývojový trend těchto událostí. Data použitá v Graf 1 jsou použita ze stránek policie České republiky. Hodnoty kyberkriminality však nebylo možné ověřit. Hlavním důvodem byly především neshodné statistiky mezi jednotlivými články na internetu, policií, ministerstvem vnitra a dalšími subjekty, které se o tuto problematiku zajímají. Proto byla kontaktována policie, aby objasnila statistiku podvodů. Bohužel policie sdělila, že tento druh informací nemůže poskytnou. Následně byli kontaktovány podpory jednotlivých internetových portálů i přepravcích společností, nicméně ani od nich se nepodařilo získat přesná data podvodů.

4.1.1 Četnost podvodů na internetu



Graf 1.Četnost podvodů na internetu [1][2][3]

Ve výše uvedeném grafu je vidět, jak se v průběhu let měnila četnost podvodů na internetu. Na první pohled je patrné že v roce 2011 byla četnost podvodů okolo 1,5 tisíc. Nicméně v průběhu let se četnost podvodů rapidně zvětšoval. Největší skok proběhl mezi lety 2021 a 2022, kdy se počet podvodů zdvojnásobil. To značí, jak velké nebezpečí tyto podvody znamenají a zároveň jak jsou lidé zranitelní.

4.2 Sociální inženýrství

Sociální inženýrství slouží jako psychicky vedená manipulace člověka za účelem zisku citlivých informací jako např. přihlašovací údaje, důležitá osobní data nebo bankovní údaje. Útok lze provést přes veškeré známé technologie (mobil, tablet, počítač…). Nejčastější forma útoku sociálního inženýrství je pomocí metody zvané phishing, nicméně těchto metod je o hodně více.

4.2.1 Phishing

Slovo phishing vychází ze slova fishing neboli rybolov. Jde tedy o nahození pomyslného háčku, který „hází“ útočník např. velmi výhodnou nabídku a čeká na svoji oběť. V reálném světě se nejčastěji stává, že se útočník vydává za zaměstnance buď nějaké internetové služby, banky, firmy, a tím se snaží získat citlivá data oběti. Už jen díky tomu, jak je lehké v dnešní době někoho pomocí phishingu podvést, je tato metoda jednou z nejvíce používaných útoků v oblasti sociálního inženýrství.[20][21][22][23]

Nejčetnějšími útoky za pomocí phishingu je pokus o odcizení citlivých informací o kreditní kartě, případně internetovém bankovnictví. Tento útok nejčastěji probíhá zasláním buď pomocí e-mailu, textové zprávy nebo přes sociální sítě. V těchto zprávách většinou oběť najde URL odkaz, který jí přesměruje na naoko totožné webové stránky a na základě buď dodání zásilky, zrušení předplatného nebo jen „ověření“ uživatele je oběti předložen formulář, který vyžaduje zadání čísla, datumu a CVV kódu uvedených na kartě. Poté, co člověk zadá údaje o své kartě, jsou po něm většinou dále vyžadovány přihlašovací údaje k jeho internetovému bankovnictví. Pokud tyto údaje oběť vyplní správně a potvrdí, otevírá podvodníkovy svůj bankovní účet. Poté je také více než možné, že útočník navrhne oběti, aby si nainstalovala aplikaci z jeho webu. V dnešní době totiž drtivá většina bank používá k ověření či autorizaci platby svého uživatele potvrzení v její aplikaci. Ale pokud oběť nainstaluje tuto aplikaci, tak ztrácí i tuto ochranu a útočník má plný přístup nejen k internetovému bankovnictví a kartě uživatele, ale nyní může provádět platby, měnit heslo atd. [20][21][22][23]

Obrázek 5. Příklad phishingového e-mailu[24]

4.2.2 Spear - phishing

Tento poddruh phishingu je v podstatě jeho o dost více radikální forma. Jde v ní o to, že si útočník dopředu zjistí veškeré důležité informace o oběti, jejím okolí a poté pomocí těchto informací sestaví phishingovou zprávu, která je konkrétně pro jeho oběť. Je tedy patrné, že je velmi obtížné odhalit takto důsledně propracovaný phishing. Tento poddruh se nejvíce používá při útocích na větší společnosti. Útočník si předem zjistí, např. jaká firma dováží do dané společnosti komponenty do jejich výroby. Zašle dovozci e-mail pod záminkou spolupráce, ale ve skutečnosti jen potřebuje vědět, jak daná firma komunikuje a jak graficky její e-mail vypadá. Následně vytvoří zcela identický phishingový e-mail a pošle ho společnosti. Zaměstnanec většinou na první pohled nepozná, že se jedná o podvrh a nechtěně poskytne útočníkovi informace nebo finance, které požaduje. [20][23][25]

4.2.3 Whaling

Jde o phishingový útok, který je zaměřený na vyšší management firem. Útočník se pomocí e-mailu začne vydávat za jejich vedoucího a požaduje po nich interní citlivé informace, peněžní převody nebo stažení dokumentu, což je ve skutečnosti malware. Pro provedení tohoto útoku se používá techniky phishing a odkazy na webové stránky neboli web spoofing (viz níže). Díky tomu, že e-mail vypadá velmi věrohodně, jsou v něm minimální vizuální nesrovnalosti, a ještě k tomu oběti píše její šéf, tak se tyto útoky stávají úspěšné. Oběť se totiž bojí nevyhovět svému nadřízenému.[25]

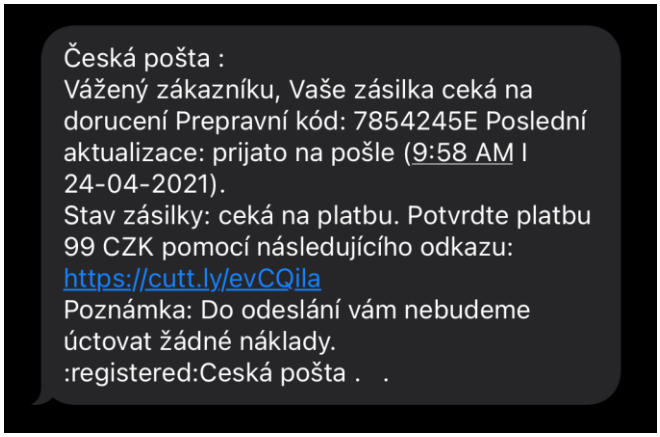
4.2.4 Vishing

Vishing je další možnou formou phishingu. Jeho princip a účel je víceméně stejný, ale liší se především použitými prostředky. Vishig nejčastěji využívá telefonní hovor neboli mluvené slovo. Cílem tohoto hovoru je vytáhnou z oběti její citlivé informace jako přihlašující údaje do internetového bankovnictví, číslo kreditní karty a její CVC. V roce 2021 byla tato technika úspěšná ve 14 % případů. [21][23][26]

Při zahájení telefonátu jsou nejčastěji použitá takováto slovní spojení: „Volám z vaší banky/pojišťovny, Jsem policista, Jsem váš dodavatel“. Dále útočník pokračuje větami „Zjistil jsem podvod, Vaše karta byla zneužita“. Následně útočník vyzve oběť, aby mu sdělila osobní údaje“ Budu potřebovat údaje o vaší kartě, Musím vás ověřit, Z bezpečnostních důvodů, Abychom mohli zablokovat vaši kartu“. Poslední, co útočník potřebuje, je ověřovací kód, který dojde oběti na její mobilní telefon „Potvrďte prosím heslo k účtu, Potvrďte prosím svůj kód do internetového bankovnictví, Přijde vám SMS, Nadiktujte mi kód, který vám přijde“. Poté má útočník již veškerá podstatná data, která od oběti potřeboval a může oběť okrást. [23][26]

4.2.5 SMShing

Jedná se o formu phishingového útoku za pomocí textových zpráv. Cílem útočníka je dostat z oběti její citlivé údaje, např. přihlašovací ID, hesla k jejím účtům nebo údaje z její kreditní karty či 3D Secure kód. Útočník rozešle hromadně SMS zprávu, kde se vydává za nějakou společnost, např. Českou poštu a čeká kdo odpoví. Součástí této zprávy je odkaz, který oběť přesměruje na vytvořené stránky, které jsou identické s originální stránkou a na první pohled není vidět rozdíl. Druhou možností je, že odkaz oběť přiměje si stáhnou škodlivý software a po instalaci může sbírat informace o oběti dlouhodobě, aniž by o tom věděla. [23]



Obrázek 6. Příklad SMShingu [27]

4.3 Spoofing

Tato metoda se většinou kombinuje s předchozími uvedenými metodami (phishing, vishing). Jedná se tedy o situace, kdy se útočník rozhodne vydávat za někoho, koho oběť zná, nebo s ním spolupracuje a následně buď pomocí telefonního hovoru, e-mailu či webové stránky se snaží z oběti vytáhnout citlivé informace. Spoofing se rozděluje hned do několika skupin, které jsou níže popsány.

4.3.1 E-mail spoofing

Jde o zasílání podvodních emailů s falešnou adresou odesílatele, nejčastěji tento útok probíhá společně s prishingovým útokem. Cílem je ukrást cenná data uživatele, infikovat jeho počítač malwarem nebo požadovat peníze. U těchto e-mailů bývají nejčastěji použity typy malwaru jako ransomware, adware, cryptojackers, trojské koně nebo malware, který přebírá kontrolu nad počítačem uživatele. [28][29][30]

Nejčastějším případem spoofingu je jeho používání u sexuálních podvodů. Základ podvodu je jednoduchý, útočník se snaží přesvědčit svoji oběť o tom, že dostal přístup k jeho web kameře a že má nahrávku, jak se oběť kouká na filmy pro dospělé. Podvodník pak po oběti požaduje většinou platbu v Bitcoinech nebo jiné kryptoměně nebo údajné video rozešle všem kontaktům oběti. Aby e-mail nabyl ještě větší věrohodnosti, může obsahovat také nějaké předešlé používané heslo tohoto uživatele, které útočník odcizil dříve. Spoof pak nabyde také dojmu, že e-mail, který oběť dostala, je odeslán z jejího vlastního účtu, a to má demonstrovat to, že má útočník přístup k e-mailu oběti a může dané video rozeslat. Nicméně většinou to není pravda a e-mail, ze kterého byla zpráva odeslána, je většinou nepatrně

pozměněn a útočník jen zkouší, jak moc je jeho oběť pozorná. To samé se týká i údajného videa, kdy ve většině případů nemá útočník vůbec nic. [28][29][30]

Obrázek 7. Příklad e-mail Spoofingu [31]

4.3.2 Spoofing webových stránek

Tento útok spočívá v tom, že si útočník předem vytvoří totožné webové stránky, např. stránky seznamu, nebo nějaké banky. Můžou se lišit jen velmi nepatrně, např. změnou umístění tečky, písmena bez háčku atd. Útočník pak sází na to, že oběť zapíše špatně adresu stránky do vyhledávače a přesměruje se na jeho podvodný web. Jelikož stránka vypadá doslova identicky jako originální stránka, tak oběť zadá svoje přihlašující údaje nebo přes stránku zaplatí (útočník dostane údaje o platební kartě) anebo si oběť stáhne do svého počítače škodlivý malware. Pokud útočník vytvoří podvodný web, nebude jen čekat, než se někdo přepíše, ale spojí ho s e-mailovým spoofem, ve který bude obsahovat odkaz na tento web. [28][29][30]

4.3.3 Spoofing ID volajícího

U tohoto útoku jde o to, že útočník obejde ID volajícího a jeho hovor pak vypadá, jako by volal buď kamarád oběti nebo někdo jiný známý. Útočník spoléhá na to, že když zavolá pod přezdívkou někoho, koho oběť zná, nebude již kontrolovat číslo, ze kterého se doopravdy volá. Pokud tento hovor oběť zvedne, může se z ní útočník pokusit dostat citlivá data, ale hlavně se oběti může začít odečítat kredit ze sim karty a útočník tak z oběti dostane hodně peněz. [28][29] [30]

4.3.4 SMS Spoofing

Jako u předešlé metody se útočník začne vydávat za někoho, koho jeho oběť zná nebo spolupracuje, akorát mu nevolá, ale napíše. Opět obejde ID odesílatele a zašle oběti zprávu pod jménem jejího přítele nebo spolupracovníka. Pokud si oběť nevšimne, že se jedná o jiné číslo (což není moc obvyklé), tak většinou udělá, co podvodník požaduje. Tedy buď se nechá přesměrovat na falešný web a zadá na něj své přihlašující údaje nebo si stáhne malware. [28][29]

4.3.5 GPS Spoofing

Je spojen především se hrou Pokémon GO. Jde o to, že oklamu svoje zařízení, aby si myslelo, že jsem někde jinde na světě, než doopravdy jsem. Proč to ale podvodníci dělají? Je to kvůli hře Pokémon GO. Díky tomu, že oklamají zařízení o svojí poloze, tak získávají herní měnu nebo chytají velký počet pokémonů. Zní to opravdu velmi neškodně (což víceméně momentálně je), ale tento typ podvodu by se mohl v blízké budoucnosti objevit u něčeho mnohem závažnějšího, než je získávání pokémonů a herní měny ve hře. [28][29]

4.4 Další typy podvodů

Ve výše uvedených kapitolách byly uvedeny známější způsoby, jaké podvodníci využívají. V níže uvedené kapitole jsou popsány další formy podvodů, které podvodníci využívají.

4.4.1 Man-in-the-Middle

Jedná se o útok, díky kterému je útočník schopen nabourat cizí komunikaci mezi dvěma účastníky, a aniž by o tom věděli, převezme kontrolu nad jejich komunikací. Informace může číst, ale i modifikovat Na typu komunikace v podstatě nezáleží, může se jednat o komunikaci mezi dvěma uživateli nebo mezi bankou a uživatelem nebo serverem a uživatelem. Získané informace pak může útočník použít např. k vydírání nebo krádežím, teroristickým útokům atd. [32]

Nejčastější místo pro tento typ útoku jsou veřejná místa neboli místa s free WI-FI. Útočník si nakonfiguruje svoji vlastní WI-FI a nezahesluje ji ani jí nepřidělí bezpečnostní certifikát (TLS/HTTPS). Jestli se oběť přihlásí pomocí této sítě ke svému internetovému bankovnictví, útočník pomocí softwaru snadno tyto údaje získá. Ke spoofu dochází při tomto útoku v momentě, kdy útočník začne měnit komunikaci mezi stranami a přesměrovává je na svoje stránky, aby získal citlivá data oběti. [23][32]

4.4.2 Watering hole

Tato technika sociálního inženýrství se zaměřuje na konkrétní skupinu lidí, např. lidi, kteří se zajímají o investice. Útočníci napadnou zranitelné stránky, které jsou zaměřené na investice a pomocí těchto stránek je přesměrují na svoje stránky obsahující škodlivý obsah nebo malware. Následně pak od obětí, které se přihlásí pod svým účtem na falešný portál, získají jejich přihlašovací údaje nebo údaje platební karty. Také se může zaměřit na počítač oběti, nevědomky donutí oběť stáhnout škodlivý software a napadnou přes něj firmu, kde oběť pracuje. [33]

4.4.3 Quid pro Quo

V překladu „něco za něco“. Jedná se o návnadu, díky které útočník nabízí nějakou službu či výhody, ale aby ji mohl provést potřebuje přístup nebo informace od oběti. Např. útočník zavolá nebo napíše e-mail, že pracuje v Avastu, a že vaše verze má chybu a potřebuje neprodleně přístup k vám do počítače, aby mohl zamezit případným útokům. Vyděšená oběť předá své údaje nebo vzdálený přístup na svůj počítač a útočník už může dělat co si jen zamane. [34]

4.5 Odhalení internetového podvodu

Vy výše uvedených kapitolách byly popsány metody, jaké internetoví podvodníci využívají. V níže popsané kapitole je vypracován postup inspirovaný internetovými zdroji, jak úspěšně odhalit nejčastější formy internetových podvodů.

4.5.1 Phishingový Spoofingový podvod

U phishingových i spoofingových útoků se v drtivé většině případů jedná o e-mailovou zprávu. Dále je tento e-mail upraven graficky podle toho, koho se snaží útočník oklamat. První náznak, že se může jednat o phishingový či spoofingový e-mail, je neočekávaný e-mail. Jako první je u takového e-mailu dobré podívat se na adresu odesílatele. Pokud se jedná o podvodný e-mail, většinou se v nepatrném detailu oproti originální adrese liší. Může se jednat např. o prohození nebo vynechání písmen či přidání tečky. Následně je dobré zaměřit se na oslovení oběti v samotném e-mailu. Pokud dostáváme e-maily od bank, úřadů či jiných společností, oslovují zákazníka personifikovaným oslovením. Následně pokud seriózní společnost či banka obepisuje lidi, nepožaduje po nich žádný druh citlivých informací (hesla, ověření čísla karty, telefonní číslo) nebo nepřikládá odkazy na „svoje“ webové stránky.

Pokud se jedná o podvodný e-mail je velice pravděpodobné, že se v něm bude vyskytovat nespočet gramatických chyb. To je z důvodu, že nespočet těchto zpráv je generováno v angličtině a následně automaticky překládáno do češtiny. Zpozornit by měla oběť také pokud se v e-mailu vyskytuje nepřiměřený nátlak. Útočník totiž potřebuje, aby jeho oběť byla vystrašená, neměla čas moc přemýšlet a provedla požadovaný úkol v co nejkratším čase. Proto oběť nepřiměřeně vystraší, může jí také dát časový limit pro splnění úkolu a následně umístí pod naléhanou zprávu webový odkaz, pomocí kterého by měla oběť řešit daný problém. Pokud se v e-mailu neobjeví nátlak může se naopak objevit pro oběť velmi výhodná nabídka. Může se jednat o výhru v loterii, smrt vzdáleného příbuzného, který oběti daroval velké množství peněz nebo se může jednat o elektroniku či jiné zboží zadarmo. Útočník také může nabízet službu za velmi výhodnou cenu. Posledním důvodem, proč se může jednat o podvodný e-mail je doména. Pokud mám např. účet u české banky, neměl bych používat zahraniční domény pro přihlášení se do internetového bankovnictví. [22][25][29]

4.6 Příklady internetových podvodů

V této kapitole jsou uvedeny některé známější případ podvodů na internetu. Podvody jsou rozděleny podle toho, zda se jedná o útok na firmu nebo na jednotlivce.

4.6.1 Příklady útoků na firmy

Google a Facebook

Tento podvod zasáhl společnosti Google a Facebook pomocí phishingových e-mailů. Podvodníci se vydávali za velkou firmu, které prodává počítače. Rozeslali phishingové e-maily konkrétním zaměstnancům uvedených společností. V e-mailech je požádali o převod prostředků za objednané počítače. Mezi lety 2013 až 2015 si podvodníci vydělali něco přes 100 milionů amerických dolarů.[35]

Microsoft

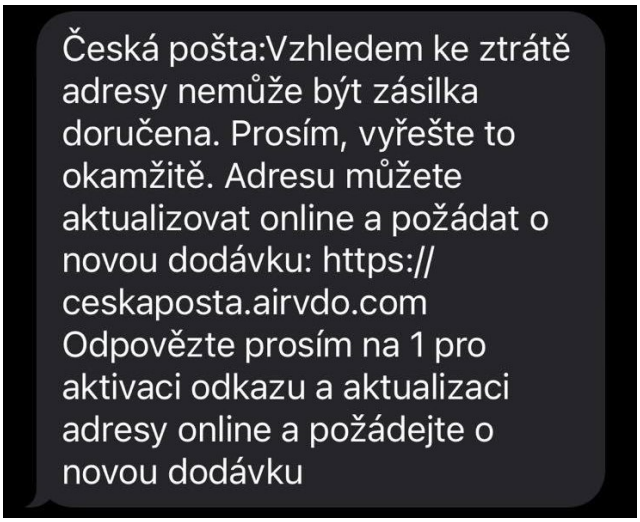
Uživatelé Microsoftu dostávali falešné e-maily s přílohou, která vypadala na excelovské tabulky. Ve skutečnosti se ale jednalo o html soubor. Po rozkliknutí byla oběť přesměrována na falešné stránky Microsoftu, kde byly navedeni k tomu, aby se přihlásili ke svému účtu. Po zadání se údaje odeslali podvodníkům.[35]

FACC

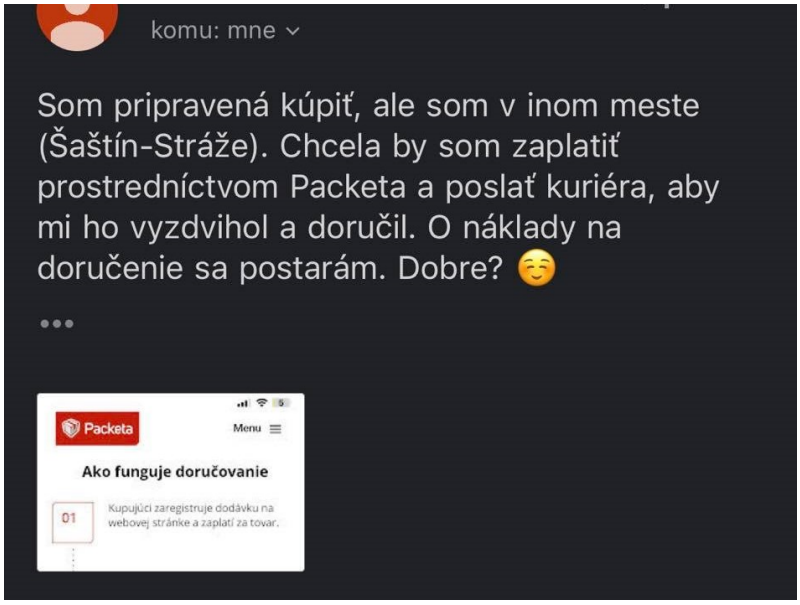
U tohoto podvodu se podvodníci vydávali za velmi vysoko postavené manažery ve firmě. Přiměli zaměstnance Čínské firmy k převodu 60 milionů dolarů.[35]

4.6.2 Příklady útoků na jednotlivce

Níže uvedené obrázky jsou typickými příklady podvodníků, kteří se snaží získat citlivá data obětí. Většinou se o to snaží buď pomocí podvodných SMS zpráv, jako u Obrázek 8 nebo pomocí podvodného e-mailu, jako u Obrázek 9. Pro úspěšné podvedení obětí nejčastěji využívají sociální inženýrství.



Obrázek 8. Příklad podvodu_1 [Vlastní]



Obrázek 9. Příklad podvodu_2 [Vlastní]

5 IDENTIFIKACE PODVODNÉHO OBCHODNÍHO PORTÁLU

Podvodných obchodních portálů je na internetu opravdu velké množství. V níže uvedených bodech se zaměříme na to, jak tyto stránky rozpoznat a nenechat se podvést podvodníkem. Na tyto stránky se můžeme dostat především dvěma způsoby. První je přes sociální inženýrství. Druhý způsob je prokliknutí přes internetový vyhledávač.

5.1 Ověření pravosti obchodního portálu

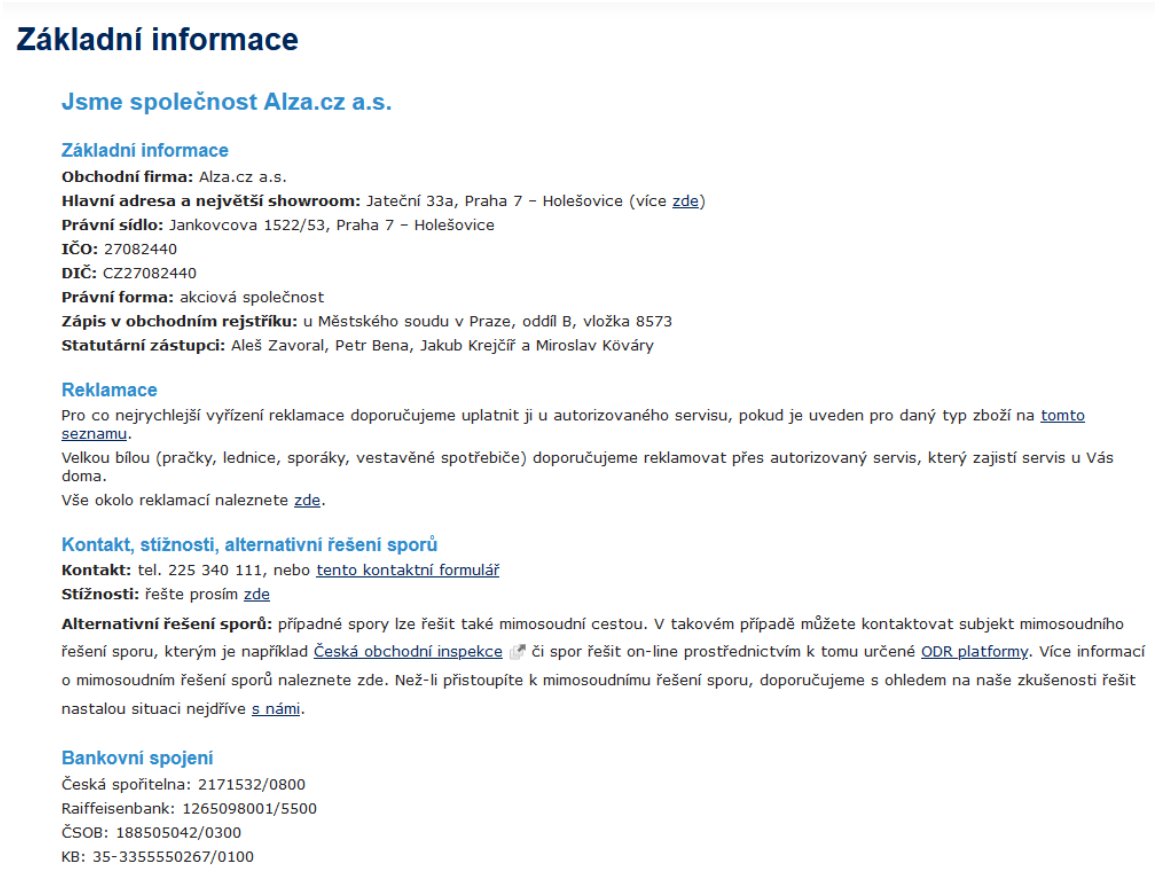
Níže uvedené signály, podle kterých lze kategorizovat pravost webového obchodního portálu, nám mohou pomoci odhalit podvodný portál, nicméně i když bude web splňovat vícero níže uvedených upozornění, nemusí se vždy jednat o podvodný web.[36][37]

5.1.1 Kontakt

Jako jedna z prvních věcí, které by si měl člověk začít všímat, pokud má podezření, že se nejedná o legální web, je totožnost provozovatele. Ten má totiž legislativní povinnost uvést svoji totožnost. Může uvést buď fyzickou nebo právnickou osobu. Nicméně měl by obsahovat název podnikatele, kontaktní adresu, IČ (unikátní identifikační číslo podnikající osoby) a DIČ (identifikace osoby, a to z placení daní z přidané hodnoty). [37]

Mezi další znamení se také řadí seznam kamenných poboček či výdejních míst. Další drobnost, díky které se lze ujistit o pravosti webu, je např. uvedení linek MHD či parkovišť v okolí jejich kamenné prodejny. Nicméně pokud je webová obchodní stránka chudá na výše uvedené informace, může se jednat o potenciálně nebezpečnou stránku.

Níže přiložené obrázky demonstrují správně uvedené kontaktní údaje (Obrázek 10) a neúplně uvedené kontaktní údaje (Obrázek 11). [36][37]



Základní informace

Jsme společnost Alza.cz a.s.

Základní informace

Obchodní firma: Alza.cz a.s.
Hlavní adresa a největší showroom: Jateční 33a, Praha 7 – Holešovice (více zde)
Právní sídlo: Jankovcova 1522/53, Praha 7 – Holešovice
IČO: 27082440
DIČ: CZ27082440
Právní forma: akciová společnost
Zápis v obchodním rejstříku: u Městského soudu v Praze, oddíl B, vložka 8573
Statutární zástupci: Aleš Zavoral, Petr Bena, Jakub Krejčíř a Miroslav Kováry

Reklamace

Pro co nejrychlejší vyřízení reklamace doporučujeme uplatnit ji u autorizovaného servisu, pokud je uveden pro daný typ zboží na tomto seznamu.
Velkou bílou (pračky, lednice, sporáky, vestavěné spotřebiče) doporučujeme reklamovat přes autorizovaný servis, který zajistí servis u Vás doma.
Vše okolo reklamací naleznete zde.

Kontakt, stížnosti, alternativní řešení sporů

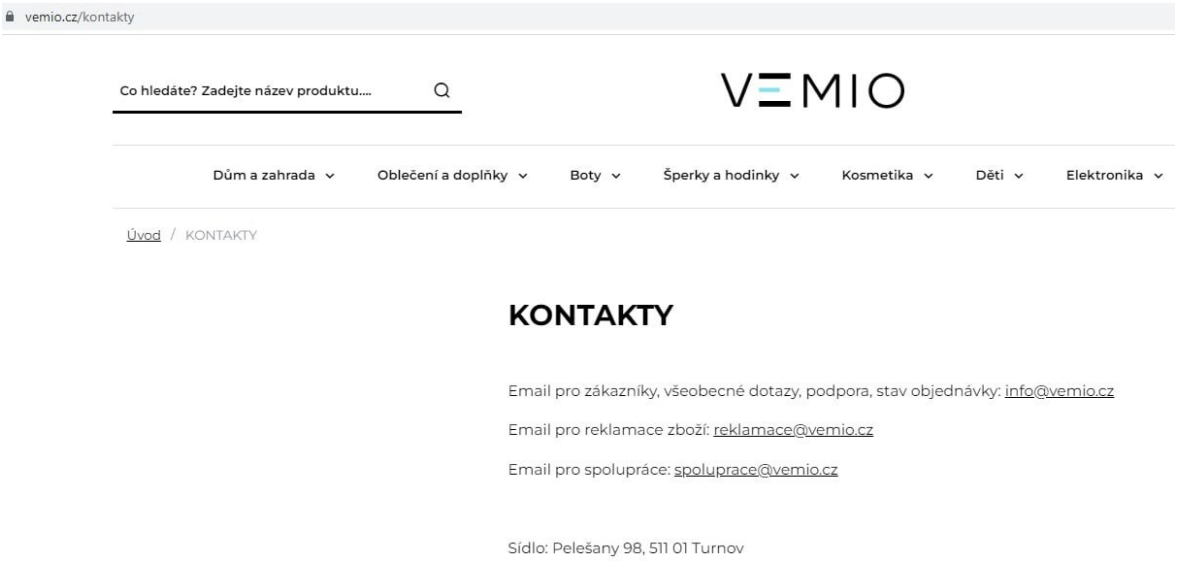
Kontakt: tel. 225 340 111, nebo tento kontaktní formulář
Stížnosti: řešte prosím zde

Alternativní řešení sporů: případné spory lze řešit také mimosoudní cestou. V takovém případě můžete kontaktovat subjekt mimosoudního řešení sporu, kterým je například Česká obchodní inspekce či spor řešit on-line prostřednictvím k tomu určené ODR platformy. Více informací o mimosoudním řešení sporů naleznete zde. Než-li přistoupíte k mimosoudnímu řešení sporu, doporučujeme s ohledem na naše zkušenosti řešit nastalou situaci nejdříve s námi.

Bankovní spojení

Česká spořitelna: 2171532/0800
Raiffeisenbank: 1265098001/5500
ČSOB: 188505042/0300
KB: 35-3355550267/0100

Obrázek 10. Příklad dobře zpracovaných kontaktních údajů [38]



Obrázek 11. Příklad neúplně zpracovaných kontaktních údajů [36]

5.1.2 Obchodní podmínky

Další podmínka, kterou má ze zákona o ochraně spotřebitele [39], kdy každý e-skop musí uvést obchodní podmínky. Ty by měly být velmi snadno na stránce dohledatelné a přístupné. Nicméně u mnoha e-shopů se může stát, že nejdou ihned najít. To však nemusí nutně znamenat, že se jedná o podvodný e-shop. Může se jednat čistě o neznalost provozovatelů stránek, a proto mohou být hůř dohledatelné. Nicméně pokud e-shop nevykazuje buď výše nebo níže uvedené nedostatky, může být web zcela v pořádku. Pokud však obchodní podmínky na webu vůbec nejsou nebo jsou napsané nekvalitní češtinou, jedná se o velmi podezřelý signál. [36][37]

5.1.3 Fotografie

Fotografie jsou u webů víceméně jen podpůrné znaky. Někdo je přesvědčen, že by každý web měl mít nafocené veškeré své nabízené produkty, a to i s uvedením loga společnosti na obrázku, aby byla jasně prokázaná pravost fotografie. Problém však je, že web může mít i tisíce produktů k prodeji, a tudíž není schopen u všech pořídit jejich originální fotografie jak z finančních nebo kapacitních důvodů. Proto, pokud na webu není vyfocená originální fotka daného produktu, nemusí se ihned jednat o podvodný web. [36][37]

5.1.4 Špatná čeština

U valné většiny podvodných webů je styl, slovosled či gramatika vygenerovaná a není tudíž ručně psaná. Důležité je tedy zaměřit se především na skladbu vět, gramatické chyby, spojení jednotlivých vět a souvětí nebo velká a malá písmena. Na tyto znaky je tedy dobré dát si pozor, a pokud web vykazuje tyto známky špatné češtiny, s největší pravděpodobností se může jednat o podvodný web. [36][37]

5.1.5 Netradiční název domény

První, čeho je dobré si u domény všimnout, je její obsah. Pokud se nacházím na webu, kde se primárně nakupuje oblečení, neměla by doména vypadat např. www.levnepecivo.cz. Neboli název domény by měl odpovídat nabízenému sortimentu.

Většina podvodných webů využívá takzvané expirované domény. To jsou domény, které nejsou již nějaký čas využívány a vlastník se již rozhodl, tuto doménu dále nepoužívat. Pokud útočník takovýto web najde, může si ho legálně zakoupit a tím pádem získal web, který má již nějakou historii nebo na ni vedou odkazy z jiných webových stránek a díky tomu se

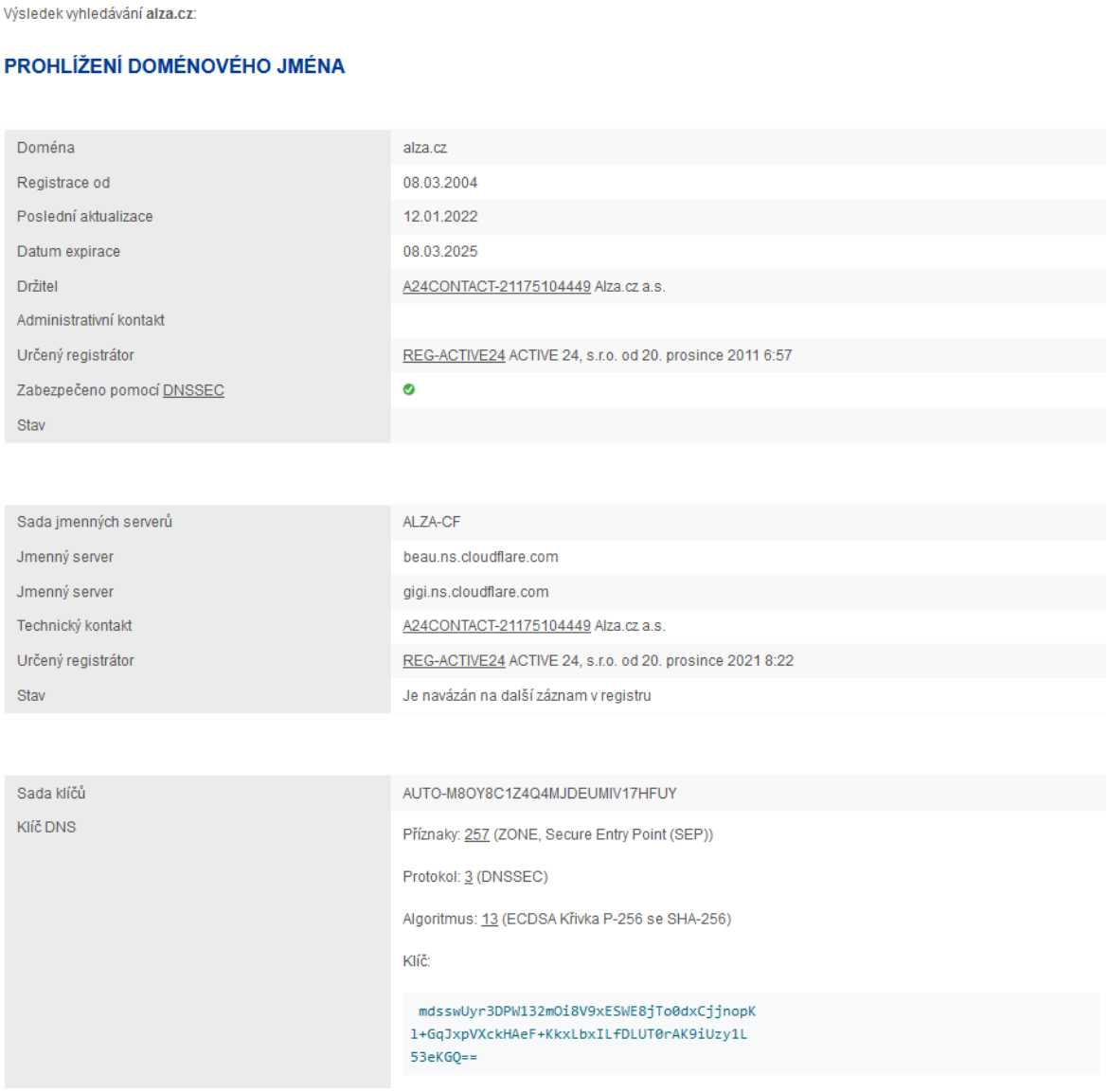
lépe dohledává a doporučuje. Tím pádem již útočníkovi nebrání nic v tom, aby web přetvořil na podvodný. Další možný důkaz podvodného webu může být rozkliknutí českého webu, např. pro nákup bot, ale doména je tvořena nesmyslnými znaky a jejich koncovka není typická pro Českou republiku, tedy ne cz, ale např. ru nebo shop. Na těchto stránkách je důležité dbát větší opatrnosti a určitě do nich nezadávat svoje citlivé údaje. [36][37]

Nicméně na světě existují i weby, které jsou v pořádku, ale mají nezvyklý název své domény. Hlavním důvodem může být odlišení od konkurence. [36][37]

5.1.6 Vlastník domény

Pro ověření vlastníka domény existuje seznam veškerých držitelů českých domén. Tento seznam je uveden na stránkách cz nic. Výpis vlastníka domény je uveden níže (Obrázek 12). Pokud jsou u výpisu vlastníka uvedeny tyto informace, jedná se pravděpodobně o bezproblémový web. Nicméně i útočník si může vymyslet falešnou totožnost a další informace, které při kontrole nedokážeme určit, avšak většina útočníků si s vymýšlením informací na oko nedělá příliš těžkou hlavu a je tedy velmi snadno ověřitelné, zda je doména pravá anebo není. Registr by měl tedy obsahovat jméno buď fyzické nebo právnické osoby, kontakt či zabezpečení. [36][37]

Pokud tedy nakupuji např. na českém webu s ponožkami a chtěl bych ověřit jeho pravost, zkopíruji doménu a vložím ji do registru cz nic. Pokud se jedná o web s českou doménou, očekává se, že vlastník bude buď z Česka nebo okolních států. Pokud bude web registrován např na jméno Sergej Kolarov, je dobré si toto jméno dále detailněji prověřit a ověřit, že se nejedná o vymyšlené jméno a příjmení. [36][37]



Výsledek vyhledávání **alza.cz**:

PROHLÍŽENÍ DOMÉNOVÉHO JMÉNA

Doména	alza.cz
Registrace od	08.03.2004
Poslední aktualizace	12.01.2022
Datum expirace	08.03.2025
Držitel	A24CONTACT-21175104449 Alza.cz a.s.
Administrativní kontakt	
Určený registrátor	REG-ACTIVE24 ACTIVE 24, s.r.o. od 20. prosince 2011 6:57
Zabezpečeno pomocí DNSSEC	
Stav	

Sada jmenných serverů	ALZA-CF
Jmenný server	beau.ns.cloudflare.com
Jmenný server	gigi.ns.cloudflare.com
Technický kontakt	A24CONTACT-21175104449 Alza.cz a.s.
Určený registrátor	REG-ACTIVE24 ACTIVE 24, s.r.o. od 20. prosince 2021 8:22
Stav	Je navázán na další záznam v registru

Sada klíčů	AUTO-M8OY8C1Z4Q4MJDEUMIV17HFUY
Klíč DNS	Příznaky: 257 (ZONE, Secure Entry Point (SEP)) Protokol: 3 (DNSSEC) Algoritmus: 13 (ECDSA Křivka P-256 se SHA-256) Klíč: mdsswUyr3DPW132mOi8V9xESWE8jTo0dxCjjnopK l+GqJxpVXckHAeF+KkxLbxILfDLUT0rAK9iUzy1L 53eKGQ==

Obrázek 12. Kontrola domény [40]

5.1.7 Podezřele nízké ceny

Věc, která spojuje veškeré podvodné weby, je až příliš nízká cena nabízeného zboží. Díky snížení ceny pak lidé často nedbají na výše uvedené body a kupují produkty jedna radost, jelikož nízká cena je dobrá motivace pro nákup. Nicméně každý web s nízkými cenami nemusí být ihned podvodný. Je dobré dbát výše uvedených bodů a ideálně, pokud si i tak chce zákazník na webu nakoupit neměl by zboží platit dopředu a zaplatit ho na dobírku. [36][37]

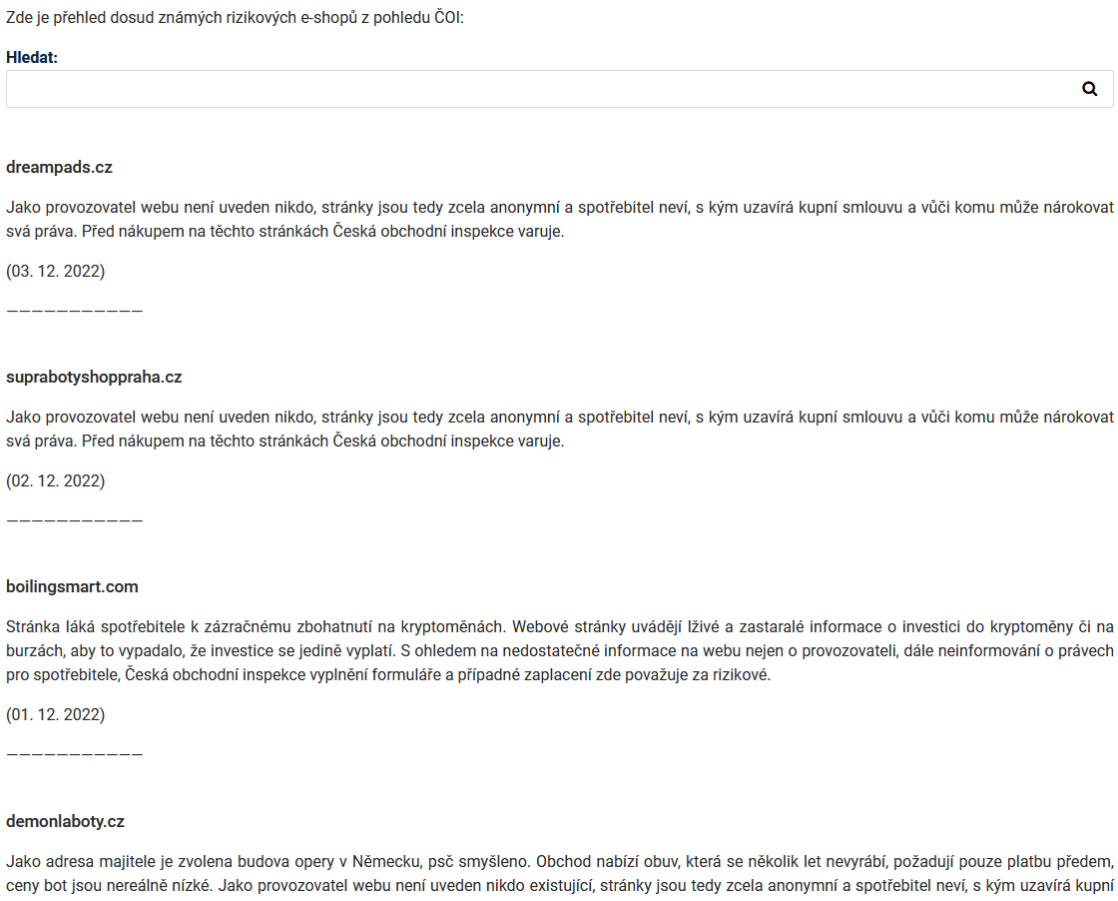
5.1.8 Další možnosti ověření pravosti webu

Web si lze ověřit i pomocí jiných webových stránek. První z nich jsou webové stránky České ochotní inspekce konkrétně v podsložce Rizikové obchody. Jako druhý způsob ověření webu

lze považovat různé typy testů, které ověří weby za nás a my jakožto uživatelé nemusíme vše dohledávat, ale všechny podstatné informace dostaneme na jednom místě. [36][37]

5.1.8.1 Česká obchodní inspekce

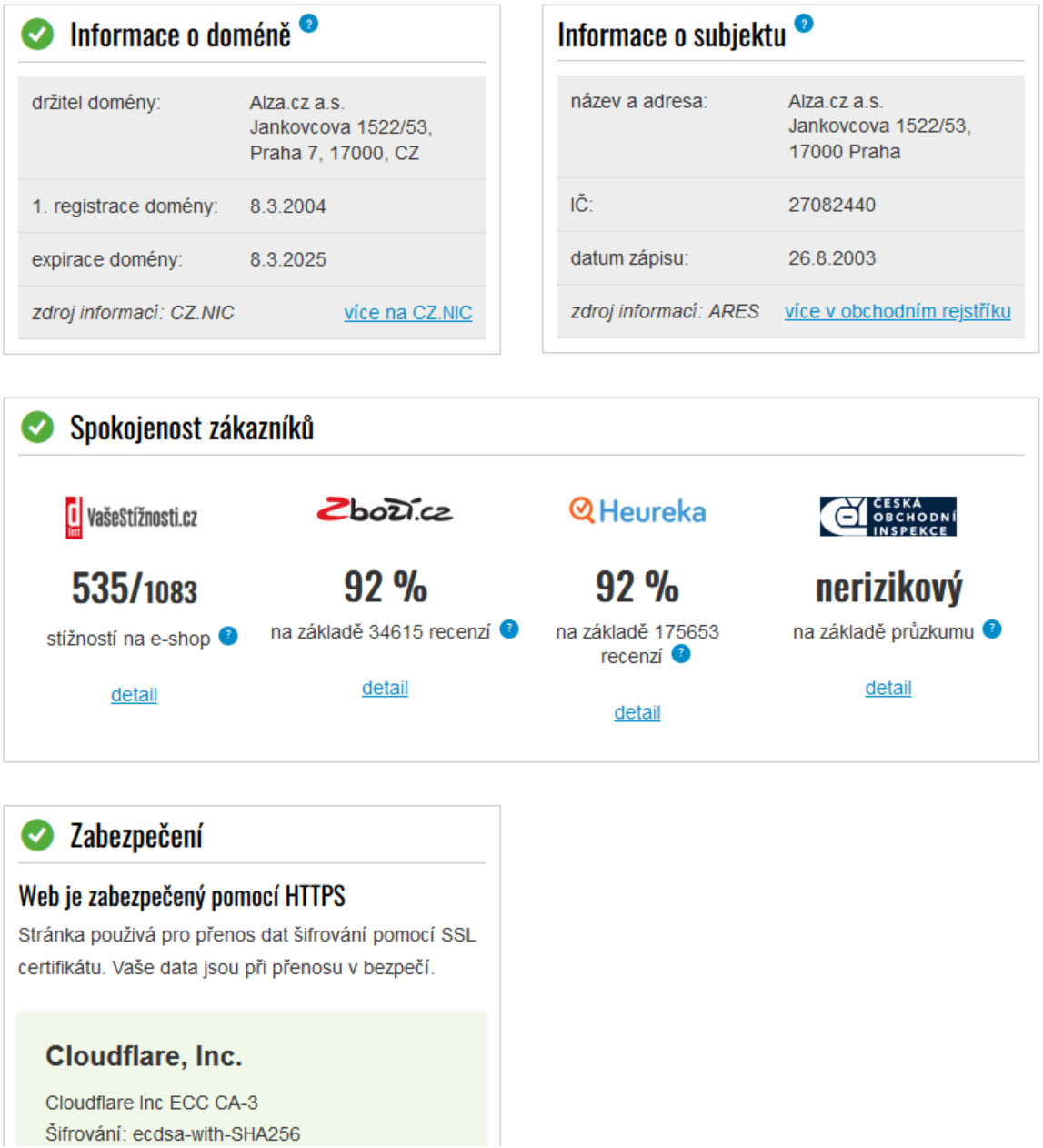
Na této stránce, jak je výše zmíněno, si lze pomocí IČ dohledat danou webovou stránku. Pokud ji však na této stránce najdeme, nemusí se opět jednat o podvodný web. Česká obchodní inspekce jen u toho webu upozorňuje na jeho nedostatky. Tento seznam je každopádně každý den aktualizován. Níže uvedený Obrázek 13 demonstruje, jak to na webu České obchodní inspekce vypadá. [36][37]



Obrázek 13. Příklad databáze České obchodní inspekce [37]

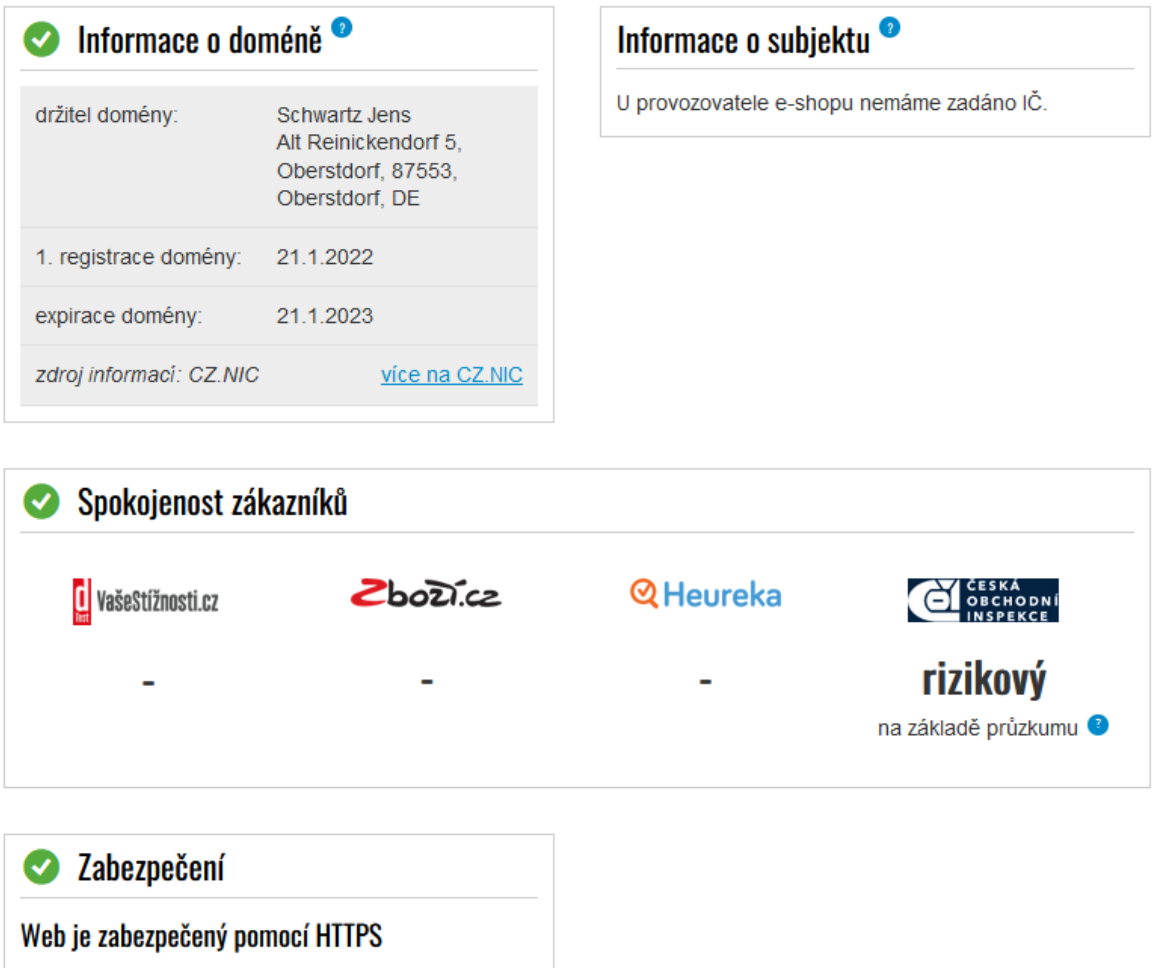
5.1.8.2 dTest

Toto je jeden z mnoha webů, kde si lze zdarma ověřit pravost webu. Po zadání URL odkazu se spustí test, který vyhodnotí na jedné stránce veškeré dostupné informace o zadaném webu (Obrázek 14). [36][41]



Obrázek 14. Příklad dTestu [41]

Na výše uvedeném obrázku je vidět, že internetový obchod Alza splňuje veškeré požadavky, které zákazník potřebuje vědět k tomu, aby poznal, že tento internetový obchod je v pořádku. Má uvedeného držitele domény a adresu jejich hlavní pobočky a také má doménu zaregistrovanou přes 20 let, což u běžného podvodného webu většinou neplatí. Podvodníci si svoji doménu předplácí na velmi krátkou dobu. Poté je také vidět, že má uvedené IČO společnosti a na recenzích uvedených níže je patrné, že na tomto e-shopu již nakoupily statisíce lidí.



Obrázek 15. Příklad dTestu [41]

U tohoto příkladu internetového obchodu již není jisté, zda se jedná o podvodný e-shop či nikoliv. Zřizovatel má na svých stránkách uvedeny jen ty nejdůležitější údaje nutné k provozu této stránky. Jedná se o obchod, který působí v česku, nicméně držitel domény uvádí, že je z jihu Německa, a to konkrétně z Oberstdorfu. Toto město je velmi malé a je především známé jako lyžařské středisko. Registrace domény tohoto obchodu je jen na jeden rok a následně na svých stránkách neuvádí žádné pořádné kontakty jako e-mail či telefonní číslo. Ani není jasné, jestli přes tento obchod lidé nakupují, protože jak je vidět na Obrázek 15 nejsou k dispozici žádné recenze zákazníků. Dokonce i web České obchodní inspekce upozorňuje na tento web, že může být rizikový. Nicméně i přes toto všechno se pořád může jednat o spolehlivý web, na kterém se může bez problému nakupovat. Majitel může teprve začínat s podnikáním, a tak nemusí být obeznámen s informacemi o správném provozování webu. Pak je již na každém zákazníkovi, jestli na daném e-shopu nakoupí, nicméně pokud by se jednalo o takto podezřelý typ internetového obchodu, ideálně by měl volit platbu dobírkou.

II. PRAKTICKÁ ČÁST

6 DOTAZNÍKOVÉ ŠETŘENÍ

Cílem dotazníkového šetření byla analýza zkušeností obyvatel České republiky s internetovými podvody. Dotazník byl vyhotoven a rozeslán respondentům v elektronické podobě, kdy veškeré odpovědi respondentů byli anonymní. Pro samotnou tvorbu dotazníku byla použita stránka www.survio.cz. Data získána z odpovědí respondentů, byla dále zpracována v Microsoft Excelu, a to buď ve formě grafu nebo tabulky. Celý dotazník je uveden v příloze práce.

Dotazník obsahoval 25 otázek, které byly rozděleny na 4 okruhy. První okruh se týkal webových obchodních portálů, druhý plateb přes internet a třetí se týkala internetových podvodů a technik, které podvodníci využívají a poslední reakci respondentů na podvod. Z 25 otázek bylo 23 otázek uzavřených a 2 otázky otevřené. Obě otevřené otázky byly nepovinné. Kdy otázka číslo 24 umožnila, pokud respondent chtěl, se podělit o svou vlastní zkušenost s internetovými podvody. Otázka číslo 25 měla čistě edukativní účel, protože součástí dotazníku byly otázky, na které existovaly správné odpovědi a pokud měl respondent zájem, mohl u této nepovinné otevřené otázky uvést svoji e-mailovou adresu. Po ukončení sběru dat mu pak byly na jeho e-mailovou adresu zaslány správné odpovědi na tyto otázky.

U tvorby dotazníku byl kladen důraz také na to, aby respondenta příliš nezdržoval, pokud s řešenou problematikou neměl zkušenosti. Proto byla u každé otázky, která měla zásadní vliv na případné další odpovědi respondenta vytvořena podmínka. Výsledkem podmínek bylo to, že existovalo několik variant, jak úspěšně vyplnit dotazník. Zároveň, aby se daly odhalit případné odpovědi respondentů, kteří při vyplňování dotazníku neodpovídali seriózně, byly v dotazníku u některých otázek takové možnosti, jak odpovědět, aby při vyhodnocování odpovědí bylo možné podle těchto odpovědí vyselektovat vyplněné dotazníky, které byly zodpovězeny neseriózně a dále je nepožívat při vyhodnocení celého dotazníku.

6.1 Stanovení hypotéz

H1: Drtivá většina respondentů již využila služeb webových obchodních portálů.

H2: Více jak polovina respondentů preferuje platbu online kartou.

H3: Jen málo respondentů využívá pro platbu přes internet virtuální kartu.

H4: Alespoň polovina respondentů se domnívá, že se stali obětí internetového podvodu.

H5: Většina respondentů se nepodlehne prvnímu falešnému e-mailu.

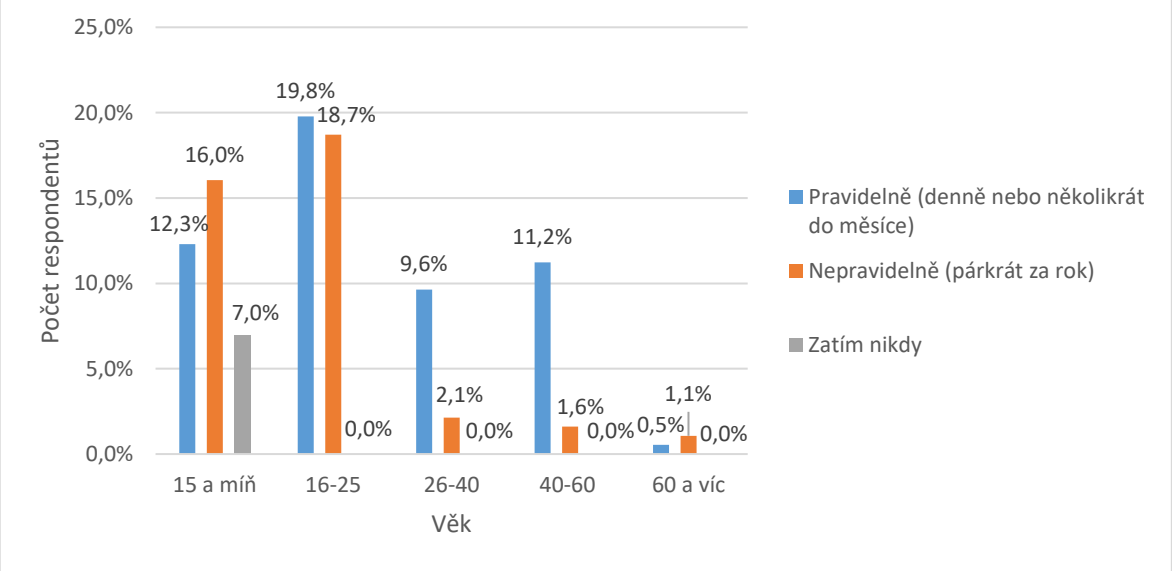
6.2 Analýza a vyhodnocení dotazníku

Vybrané otázky, byly voleny a analyzovány, aby bylo možné po vyhodnocení dotazníku definovat jaké zkušenosti mají respondenti s internetovými podvody, na jaké věkové kategorie jsou podvodníci nejvíce zaměřeni, ale také jak jsou respondenti obezřetní, pokud jsou kontaktováni podvodníkem. Data respondentů byly zpracovávány pomocí grafů a tabulek.

6.2.1 Využívání obchodních portálů

Jak často využívají respondenti obchodní portály?

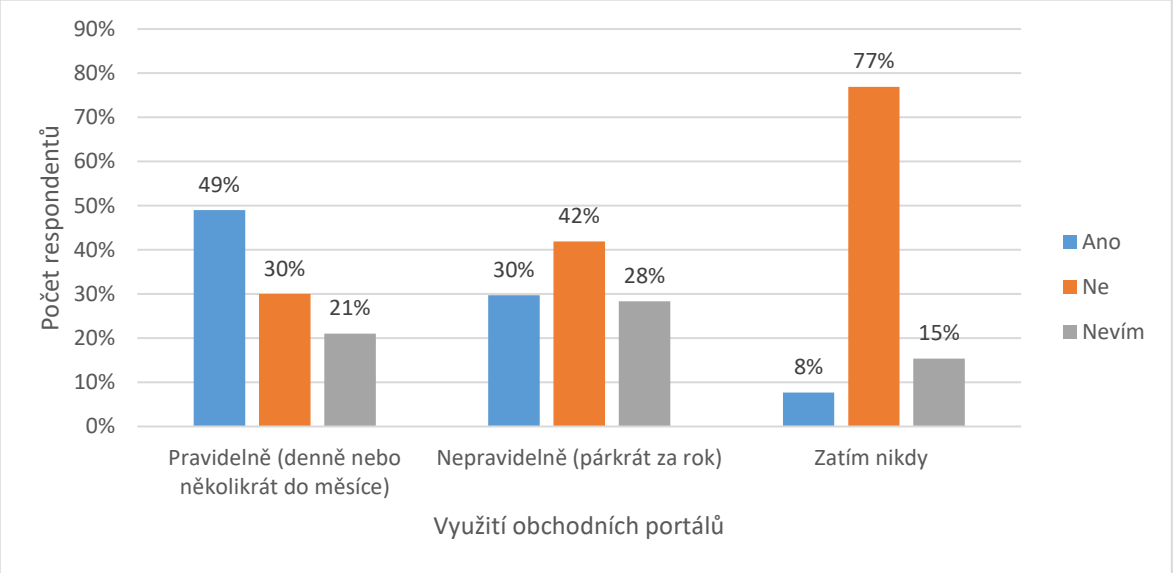
U této otázky byl hlavní cíl zjistit podle věku respondentů, jak často využívají obchodní portály. Podle označené odpovědi se respondentovi následně upravila skladba dotazníku.



Graf 2. Využití webových obchodních portálů

Výčet respondentů podle využití obchodních portálů v souvislosti s podvody

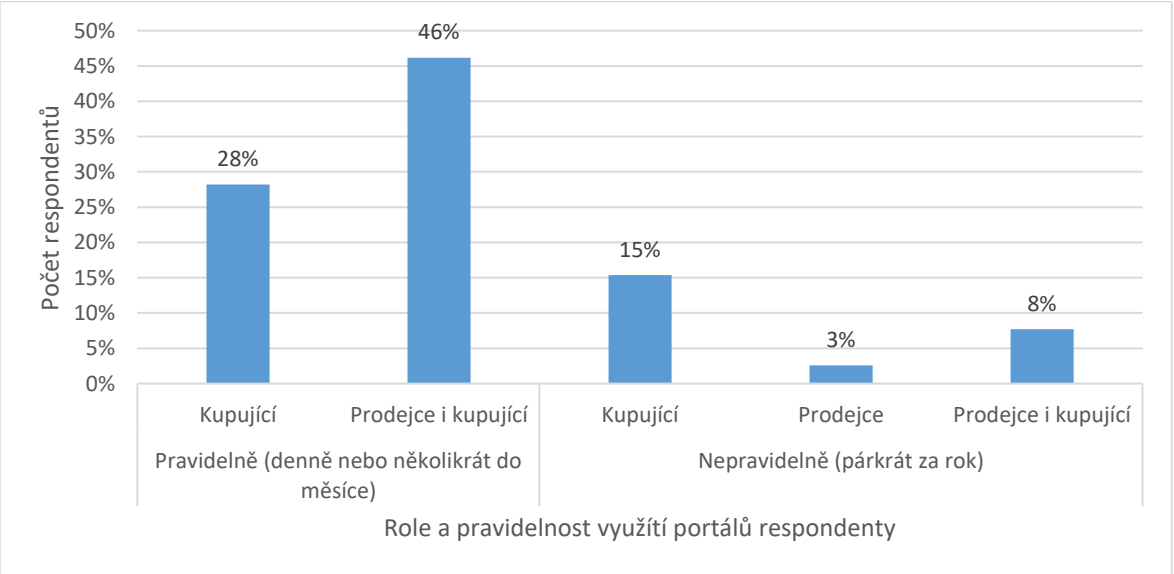
U této otázky mohli odpovídat všichni respondenti. Důvodem otázky bylo zjistit, jak často využívají obchodní portály nehledě na jejich věk. Podle odpovědi respondentů se jim následně přizpůsobily otázky v dotazníku.



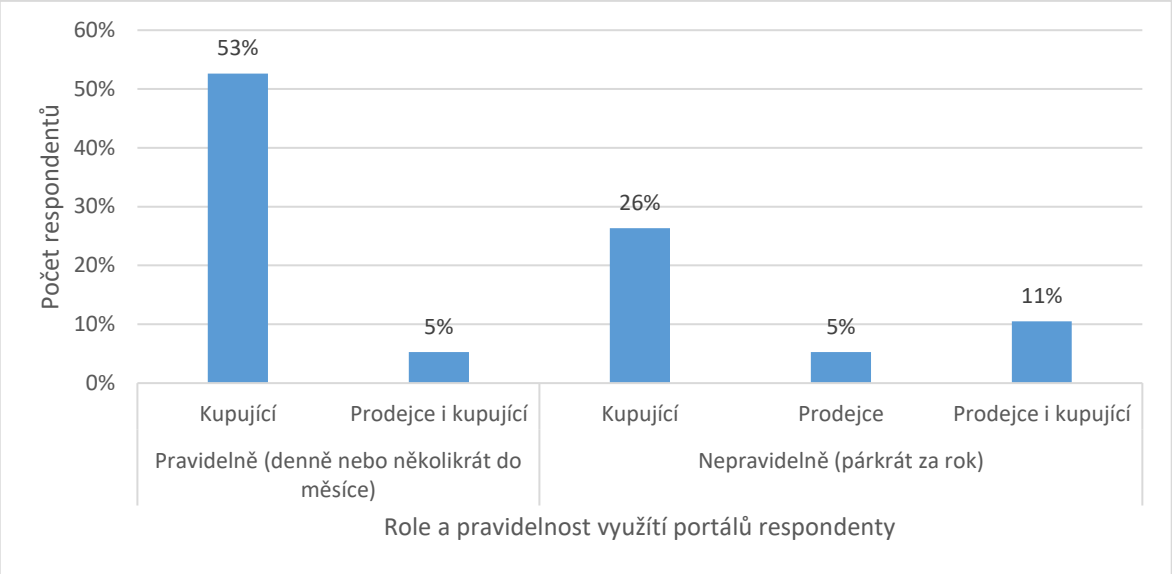
Graf 3. Využití obchodních portálů v závislosti na zkušenosti respondentů s podvody

Využití sociálních sítí respondenty

Na tuto sadu otázek 4, 5 a 6 mohli odpovídat pouze respondenti, kteří v dřívější otázce odpověděli, že využívají obchodní portály, alespoň nepravidelně. Níže uvedené dva grafy se dělí podle využití sociálních sítí, skrz jejich možné využití k obchodování.



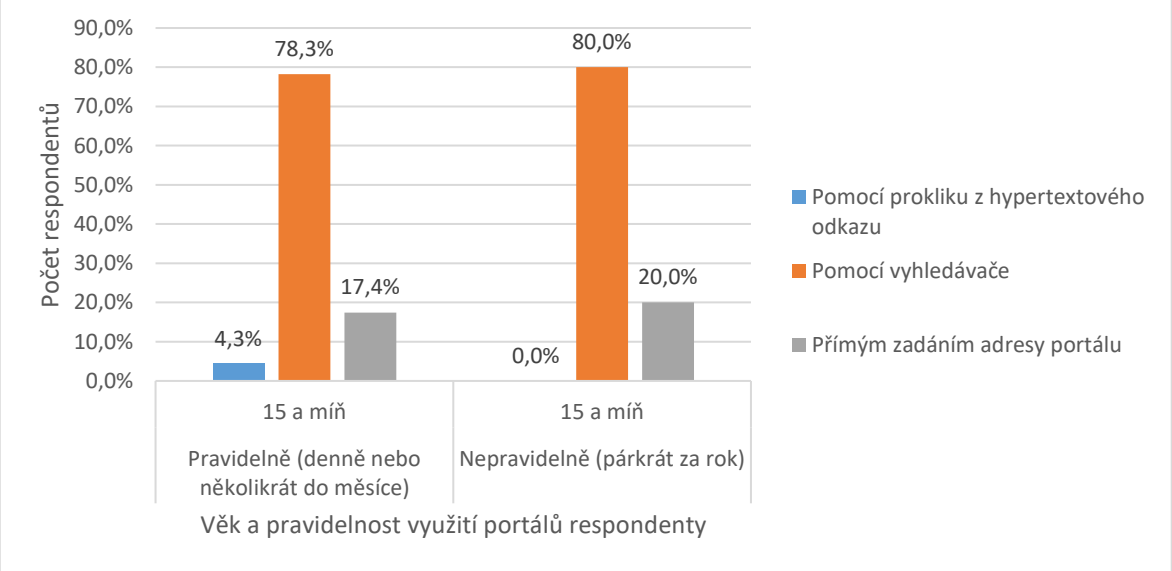
Graf 4. Facebook Marketplace



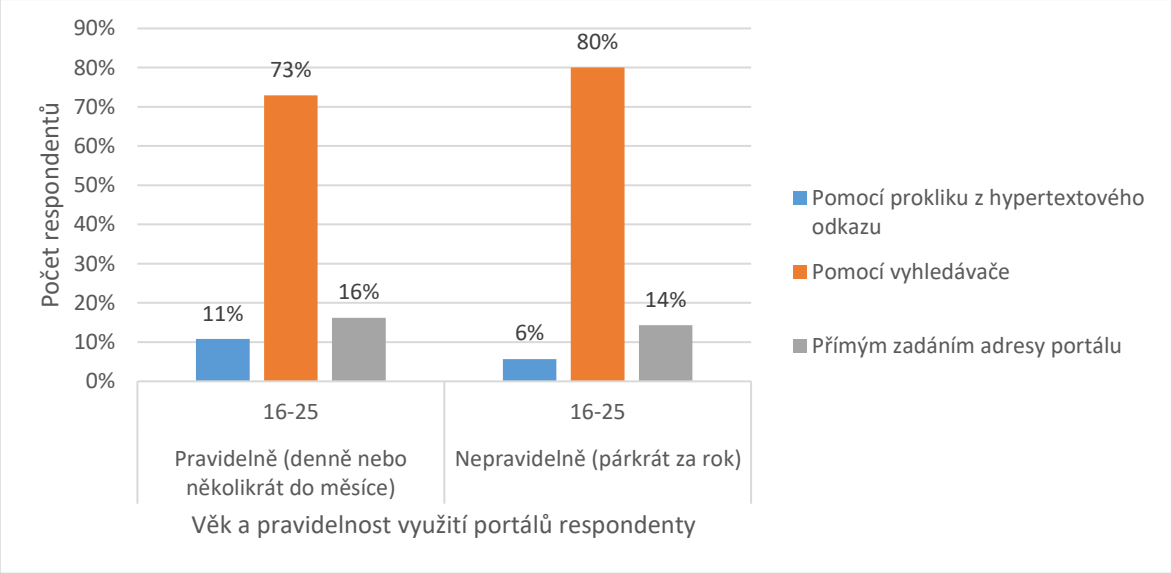
Graf 5. Instagram (DM zprávy)

Jak respondenti vyhledávají obchodní portály na internetu?

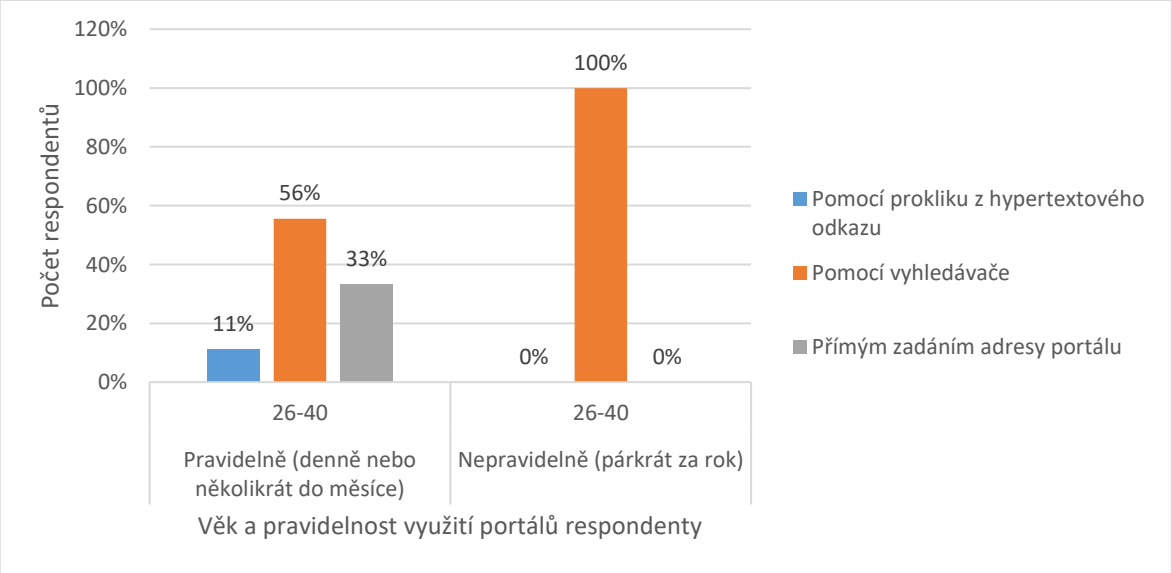
Na tuto otázku mohl respondent odpovědět, pokud v otázce 4 odpověděl, že využívá obchodní portály alespoň nepravidelně. Jednotlivé odpovědi se dělí podle věku, z důvodu srovnání, mezi jednotlivými věkovými skupinami. Hlavní důvod položení této otázky je zjištění, jaká forma vyhledávání obchodních portálů na internetu je respondentům nejbližší.



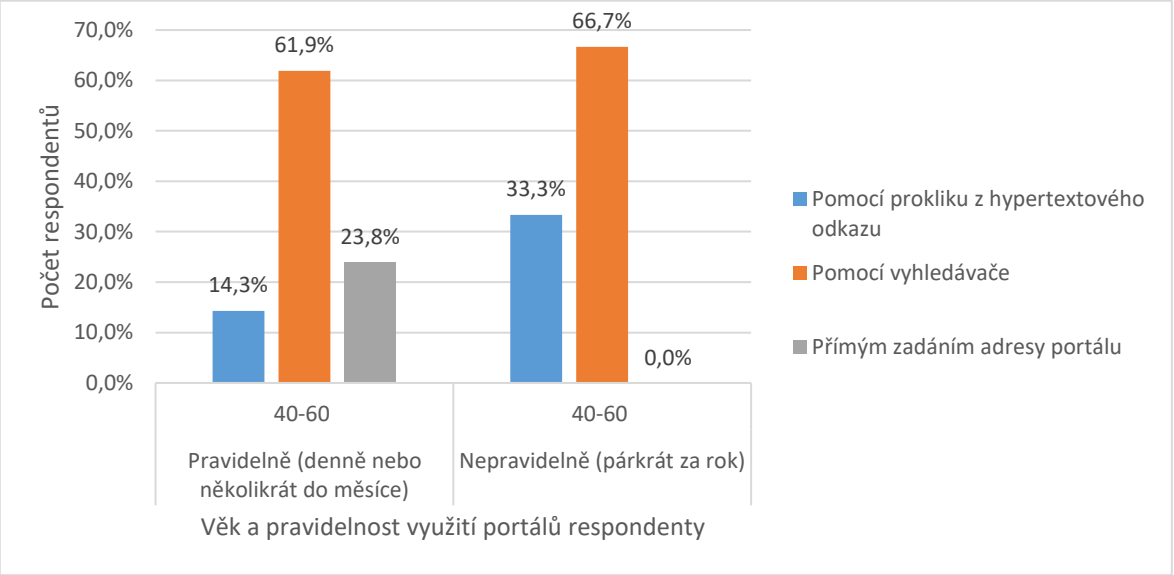
Graf 6. Věková kategorie 15 a míň let



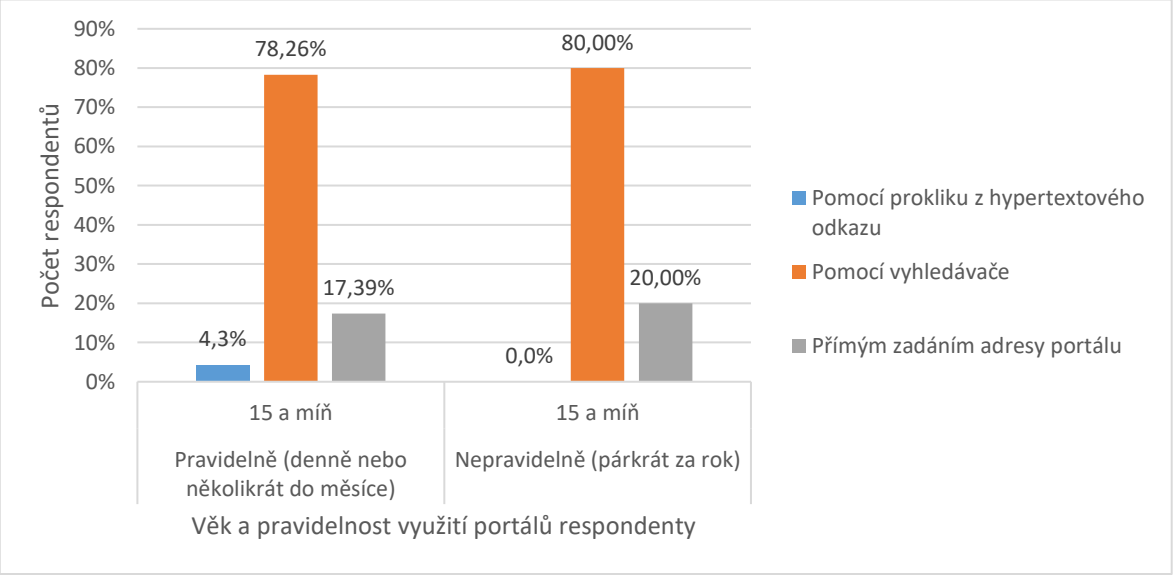
Graf 7. Věková kategorie 16-25 let



Graf 8. Věková skupina 26-40 let



Graf 9. Věková skupina 40-60 let



Graf 10. Věková skupina 60 a víc let

Jaké indikátory jsou podle respondentů důležité k rozpoznání podvodného e-shopu?

K této otázce měli respondenti opět jako u předešlých otázek přístup, pokud odpověděli u otázky číslo 4, že využívají obchodní portály alespoň nepravidelně. Níže uvedená Tabulka

1 znázorňuje co je pro respondenty nejvíce důležité, vzhledem k rozpoznání podvodného obchodního portálu.

Tabulka 1. Indikátory, které vedou k rozpoznání podvodného e-shopu

	Indikátory							
Věk	Recenze zákazníků	Sídlo firmy či společnosti	Nespisovný jazyk	Neuvedení obchodních podmínek na webu	Ceny produktů	Jméno provo-zovatele	Název a vlastník domény	Fotografie produktů
15 a míň	35	22	22	15	24	15	11	26
16-25	56	39	38	48	27	32	26	23
26-40	17	11	13	12	10	8	11	3
40 a víc	20	18	17	12	7	10	11	4
Celkem	128	90	90	87	68	65	59	56

6.2.1.1 Dílčí shrnutí kapitoly

Kapitola byla zaměřena na využití webových obchodních portálů respondenty. Jak často je respondenti využívají, jak své oblíbené portály vyhledávají a co je podle nich důležité k rozpoznání podvodného webového obchodního portálu. Níže jsou uvedeny nejdůležitější informace.

Nejčastějšími uživateli obchodních portálů je věková skupina od 16 do 25 let (Graf 2).

Pokud respondent v minulosti využil obchodní portály tak se s podvodníky v drtivé většině případů již setkal (Graf 3).

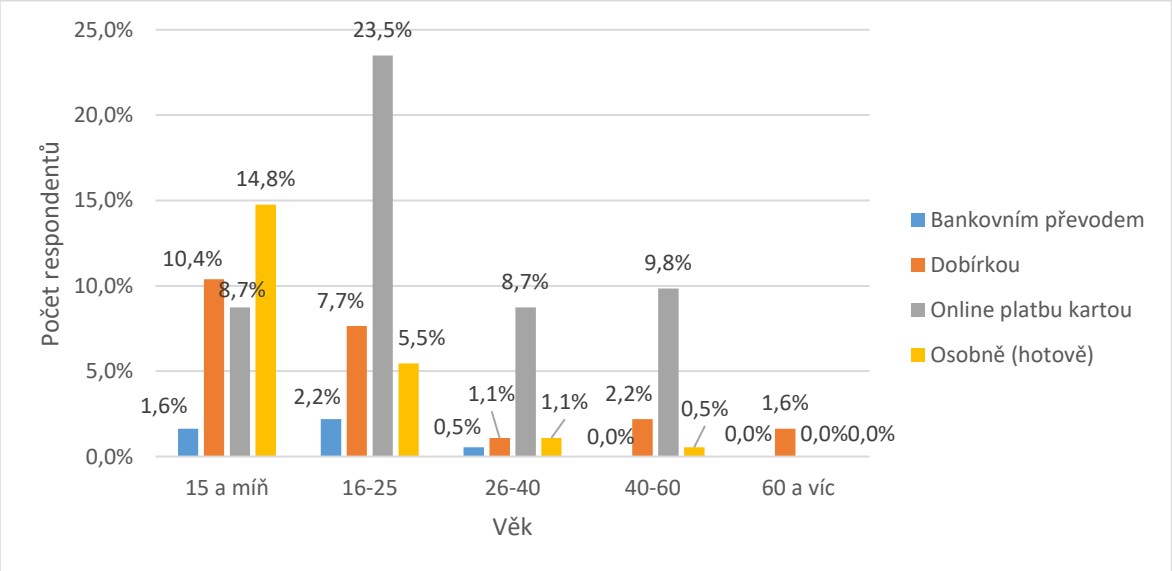
Pokud si respondenti chtějí něco nakoupit přes obchodní portály tak je vyhledávají jednoznačně pomocí vyhledávače (Graf 6, Graf 7, Graf 8, Graf 9 a Graf 10).

Pokud si respondent není jistý s pravostí obchodního portálu, tak dá především na recenze ostatních zákazníků (Tabulka 1).

6.2.2 Platby na obchodních portálech

Jakou formu platby respondenti nejčastěji využívají?

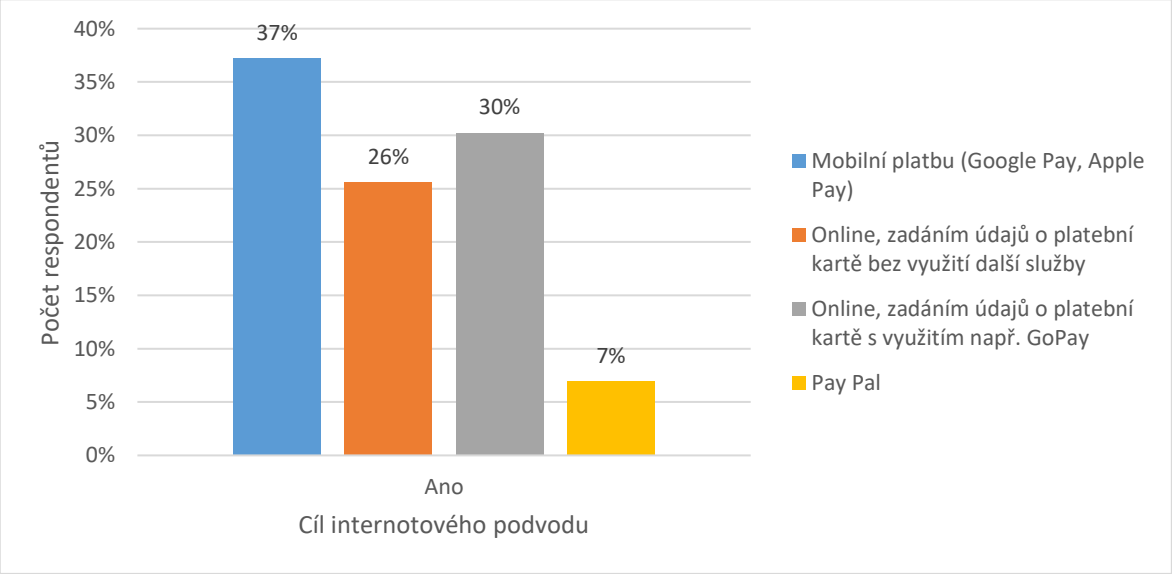
Na tuto otázku odpovídali všichni respondenti. Nicméně podle jejich odpovědi se jim pak následně upravil dotazník do příslušné podoby. Význam této otázky spočívá v tom, jak se jednotlivé věkové skupiny liší při placení na online obchodních portálech.



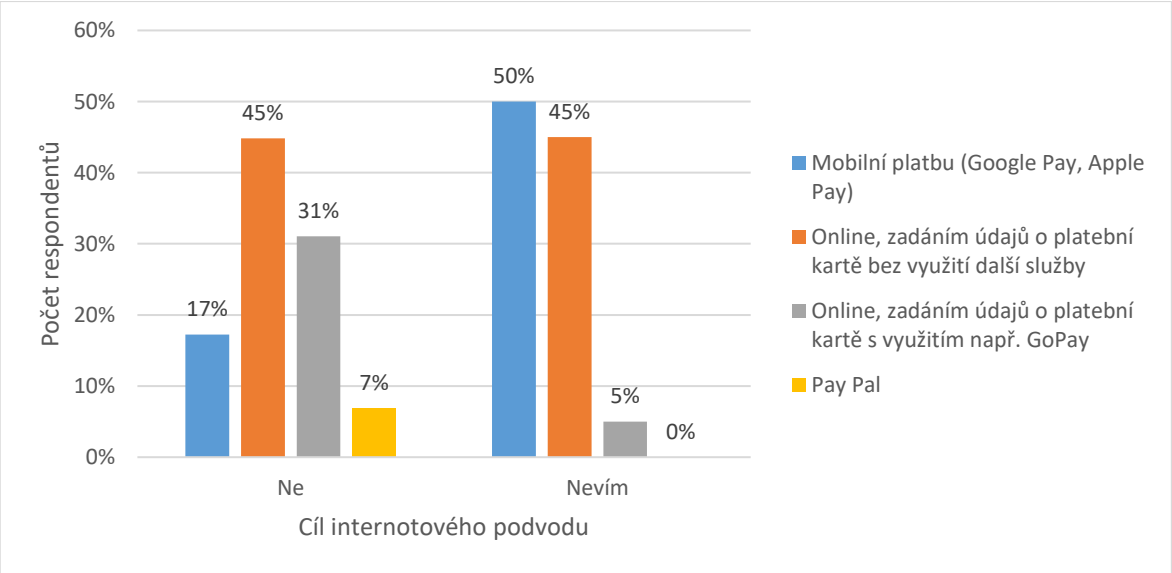
Graf 11. Forma platby

Jaká forma online platby je nejvíce nebezpečná?

Na tuto otázku mohli odpovědět pouze respondenti, kteří v předešlé otázce vybrali odpověď: Online platba kartou. Tato navazující otázka zkoumá, jakým způsobem respondenti platí pomocí karty na internetu. K této otázce byla přidána ještě otázka, zda se respondent domnívá, jestli se v minulosti stal cílem internetového podvodu. Výsledkem tedy je statistika toho, která platební metoda je nejvíce nebezpečná pro platby na internetových obchodních portálech.



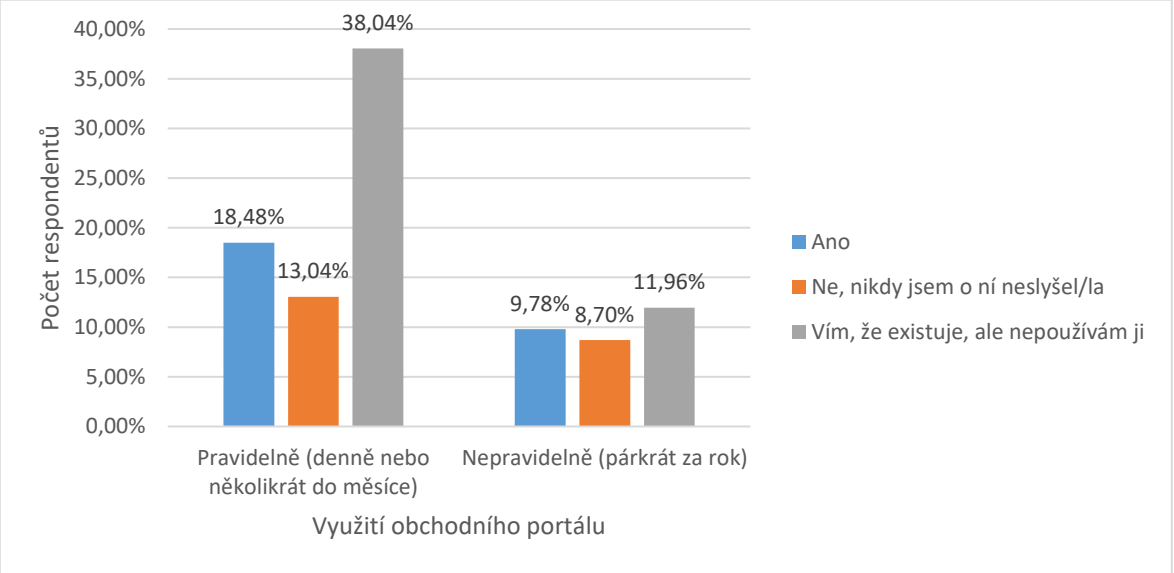
Graf 12. Ano domnívám se, že jsem se stal cílem internetového podvodu



Graf 13. Ne nebo nevím, zda jsem se stal cílem internetového podvodu

Využívá respondent pro platbu na internetu virtuální kartu?

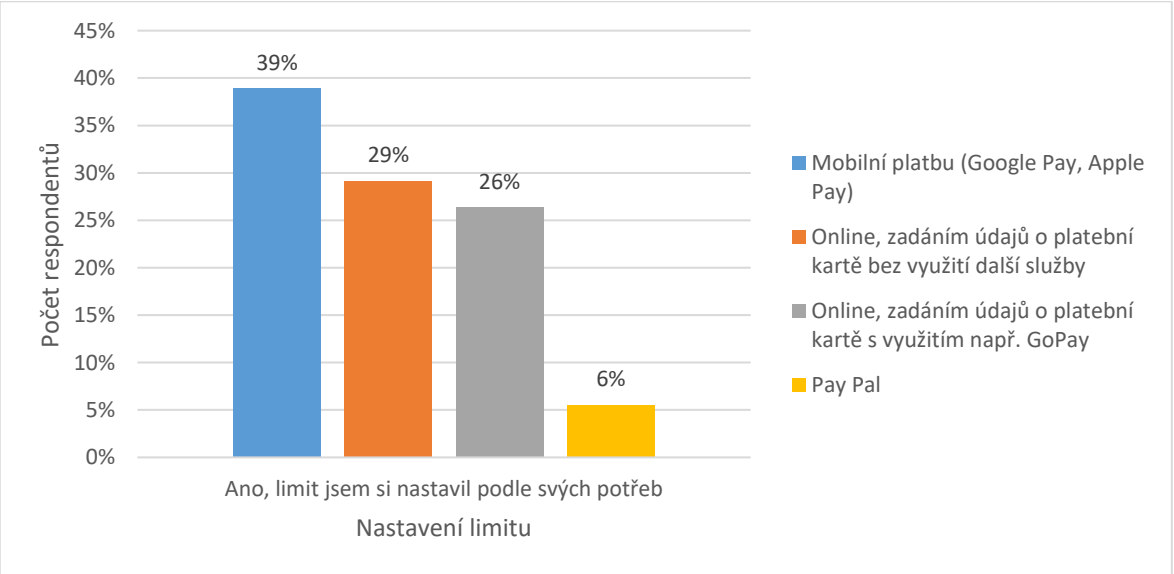
Na tuto otázku mohl respondent opět odpovědět jen v případě, že u otázky 10 označil možnost online platby kartou. Z grafu by mělo vyplynout, jak respondenti využívají virtuální kartu, podle pravidelnosti využívání obchodních portálů.



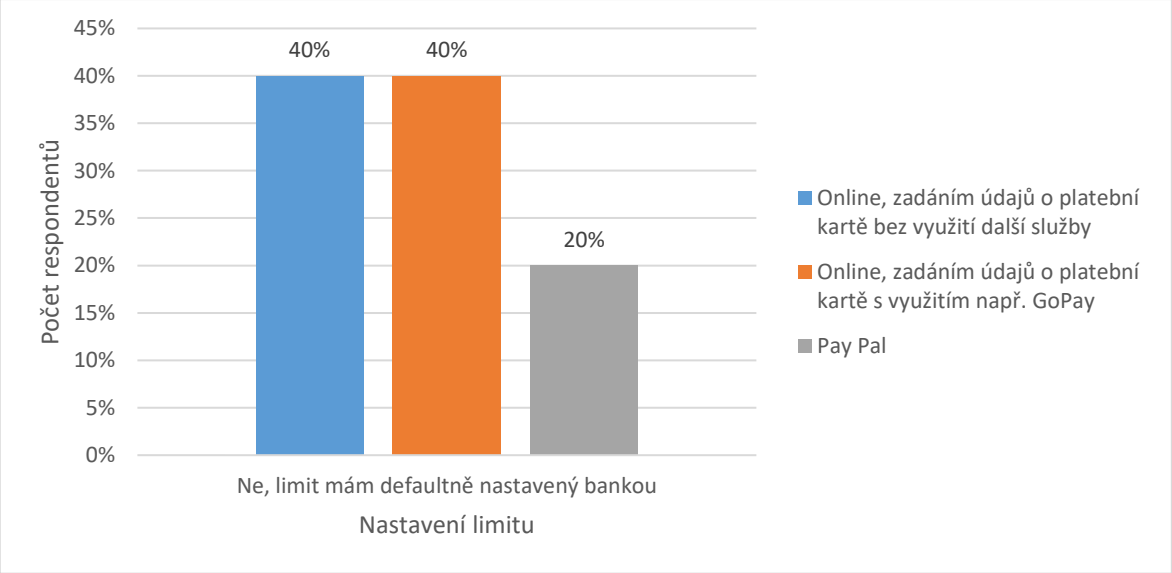
Graf 14. Platba virtuální kartou

Má respondent nastavený limit pro platby přes internet?

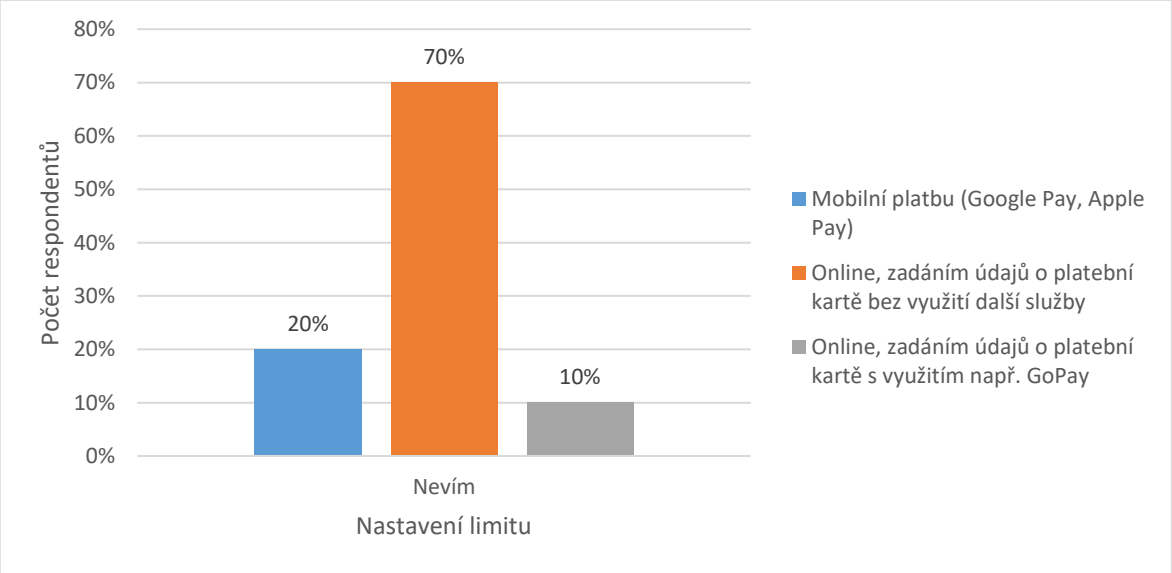
Odpovědět na tuto otázku odpověděli všichni tázaní respondenti. Pokud respondent neměl zřízené internetové bankovnictví, měl možnost označit odpověď tomu uzpůsobenou. Otázka je čistě zaměřena na to, jestli mají respondenti nastavený limit v internetovém bankovnictví.



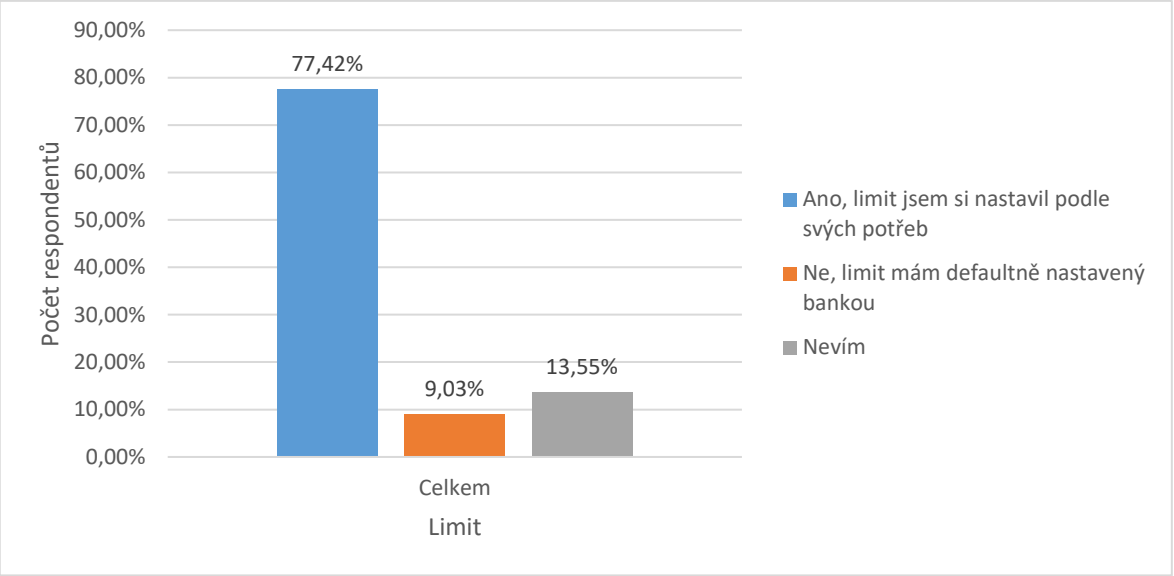
Graf 15. Ano, limit jsem si nastavil podle svých potřeb



Graf 16. Ne, limit mám defaultně nastavený bankou



Graf 17. Nevím, jak mám limit nastavený



Graf 18. Celkový souhrn odpovědí u nastavení limitu v internetovém bankovnictví

6.2.2.1 Dílčí shrnutí kapitoly

Tato kapitola se týkala plateb na webových obchodních portálech. Respondenti odpovídali na otázky zaměřené na jejich nejoblíbenější způsob platby, využívání virtuální platební karty, nebo nastavení limitu na jejich platebních kartách. Níže jsou uvedeny nejdůležitější informace, které z této části vyplynuly.

Pro platbu na obchodních portálech se respondenti dělí podle věku do dvou základních skupin. Mladí respondenti nejčastěji platí hotově, ostatní respondenti preferují online platbu (Graf 11).

Typ platby, při které se respondenti nejvíce setkali s podvodníky je platba mobilním telefonem (Graf 12,Graf 13).

Respondenti, kteří využívají obchodní portály pravidelně nevyužívají pro platbu virtuální kartu tak často jako ti, kteří nenakupují pravidelně (Graf 14).

Velké množství respondentů má v internetovém bankovnictví nastavený limit (Graf 18).

6.2.3 Podvody na prodejních portálech

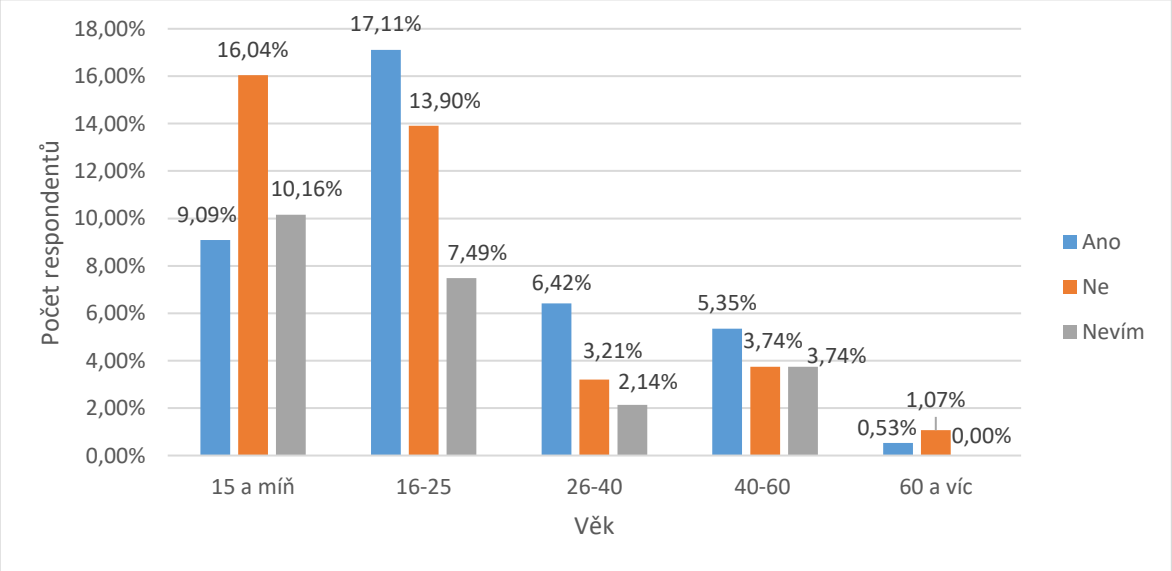
Kolik se dle respondentů událo v roce 2022 prokázaných internetových podvodů?

Tabulka 2. Prokázané internetoví podvody

Věk	Četnost podvodů				
	100–1000	1000–5000	5000 - 15 000	15 000 - 20 000	20 000 a víc
15 a míň	5	18	18	14	11
16-25	1	11	31	19	10
26-40	0	2	5	6	9
40-60	2	3	8	3	8
60 a víc	0	1	0	1	1
Celkový součet	8	35	62	43	39

Stal se respondent cílem internetového podvodu?

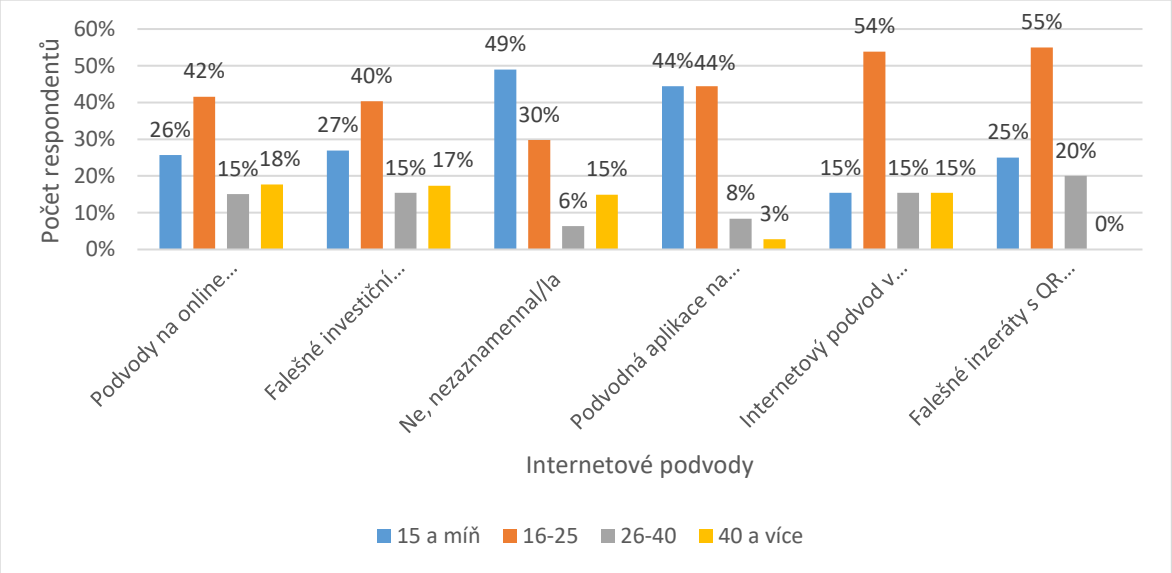
Tuto otázku zodpovídali všichni respondenti. Cílem bylo zjistit která věková skupina respondentů zaznamenala nejvíce podvodů na obchodních internetových portálech.



Graf 19. Podvody na obchodních portálech

Zaznamenal respondent některý z uvedených internetových podvodů?

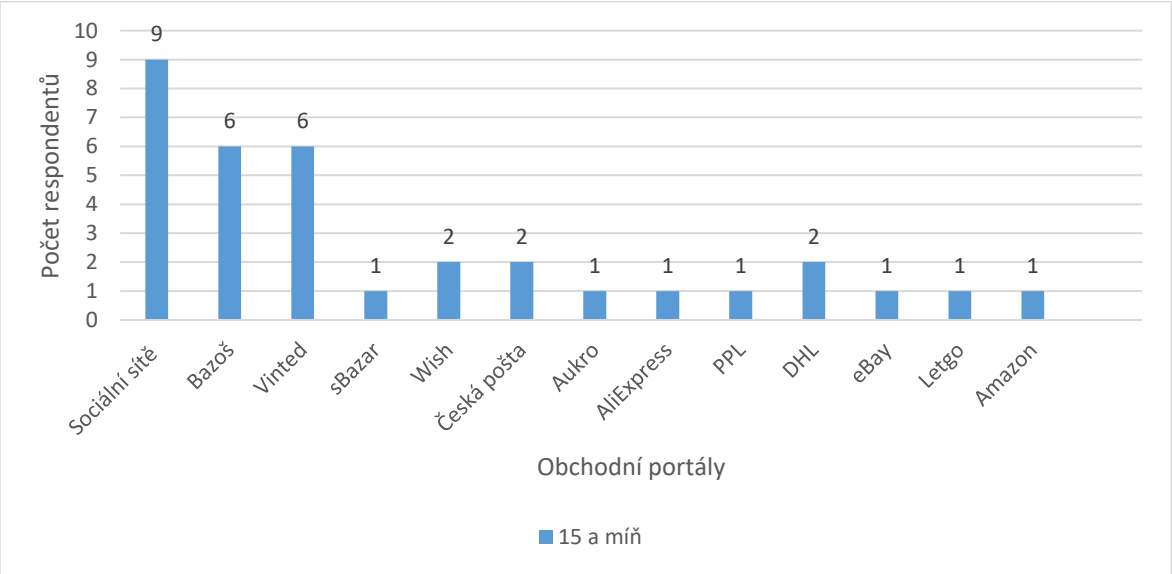
Na tuto otázku mohli odpovídat všichni respondenti. Odpovědi obsažené v Graf 20 jsou seřazeny podle toho, kolikrát se respondentům jednotlivé podvody stali. Zároveň u této otázky byly opět přidány dva internetová podvody, které se nestaly.



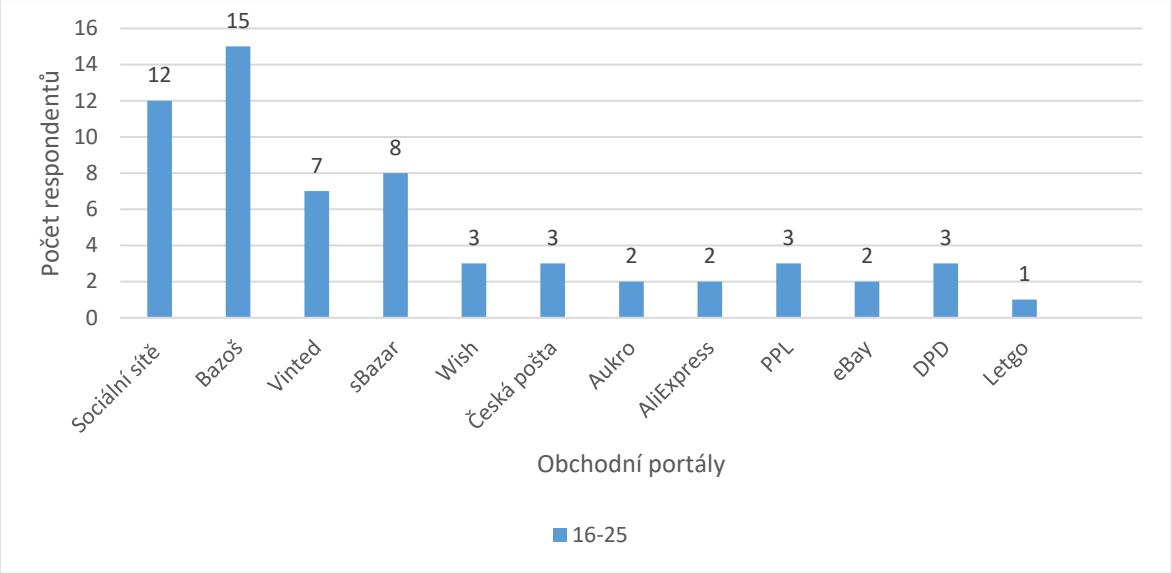
Graf 20. Příklady internetových podvodů

Na jakém druhu webové stránky se respondent s podvodníky setkal?

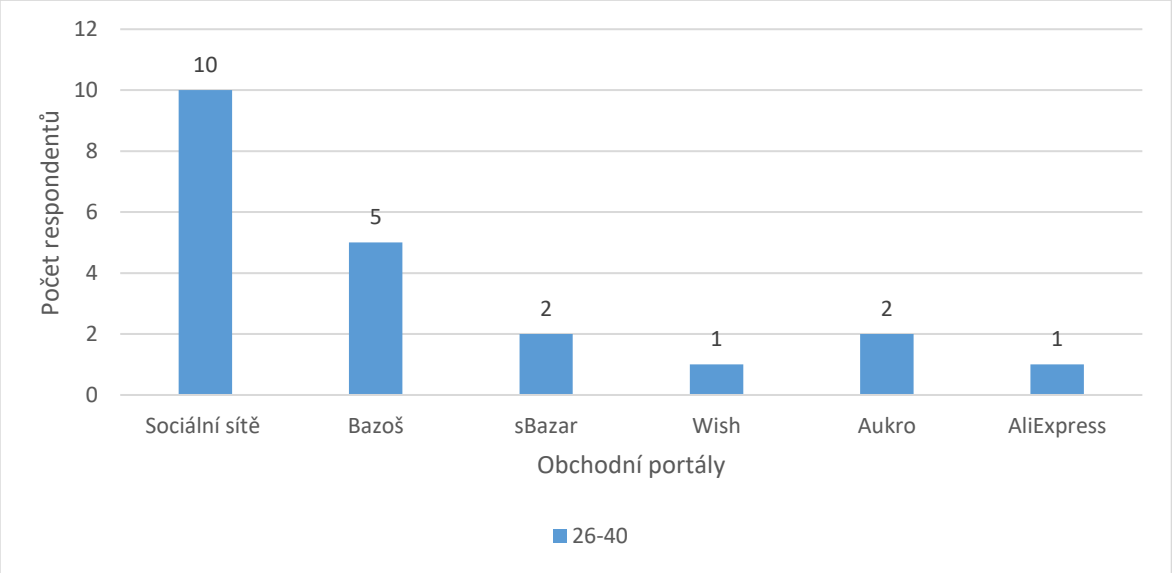
Na tuto otázku mohl odpovědět jen respondent, který u otázky 16 odpověděl, že se pravděpodobně stal v minulosti cílem internetového podvodu. Smysl této otázky spočívá v tom, aby bylo možné určit portály, kde se respondenti nejčastěji setkali podvodníky.



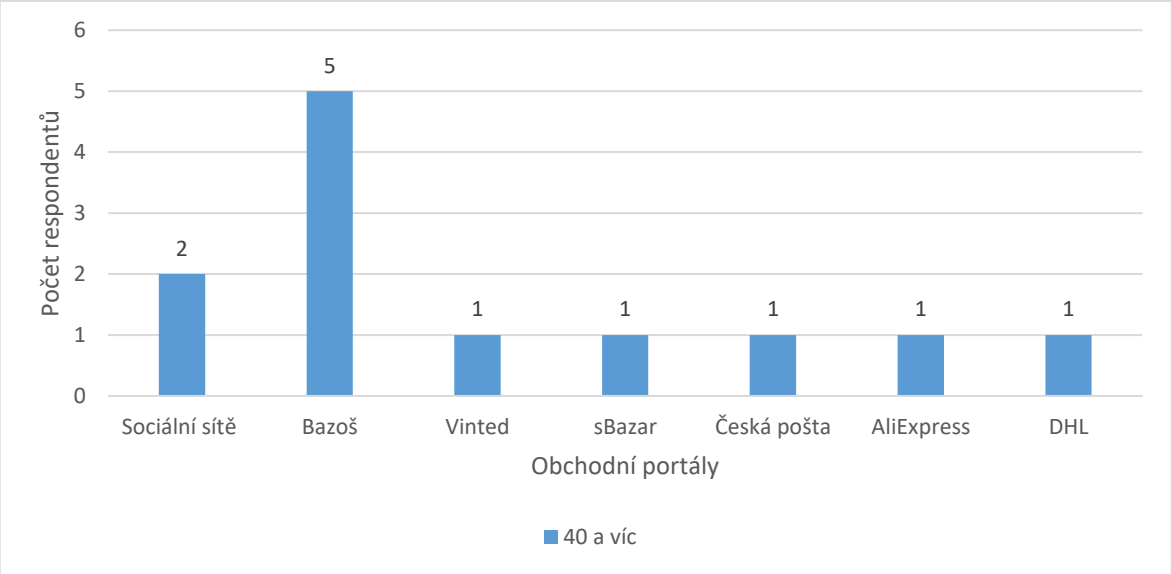
Graf 21. 15 a míň let



Graf 22. 16 až 25 let



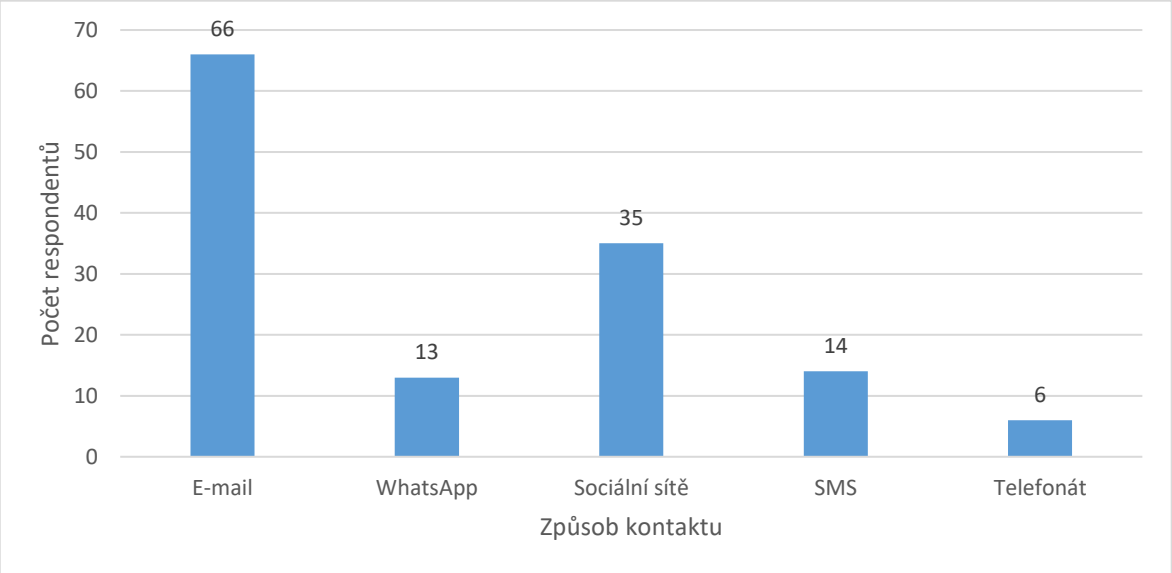
Graf 23. 26 až 40 let



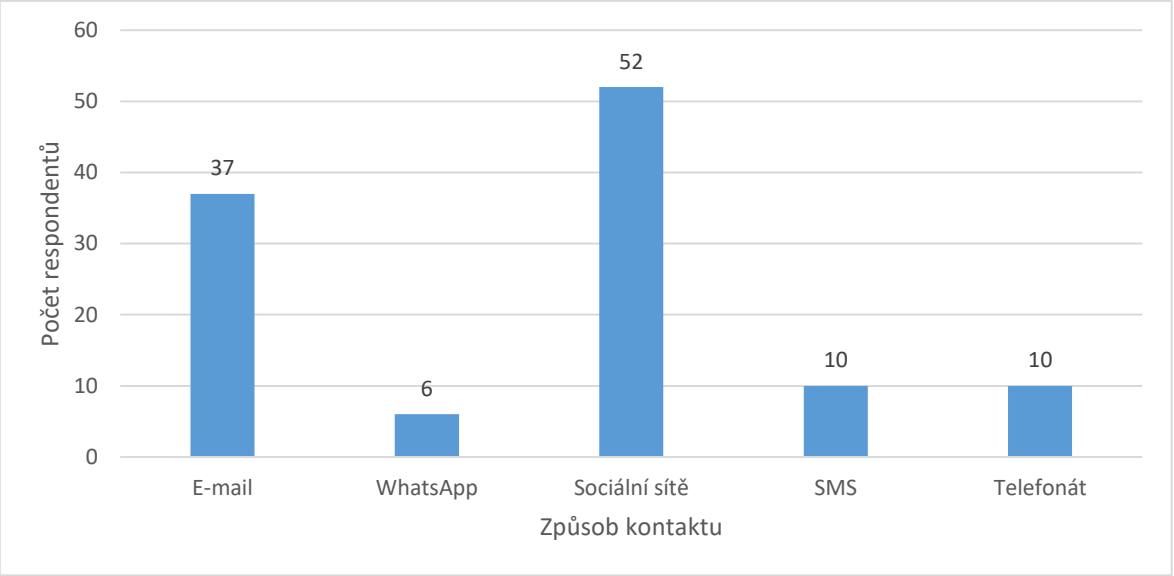
Graf 24. 40 a více let

Jakým způsobem podvodníci respondenty kontaktovali?

Obsahem této části je srovnání toho, jak podvodníci kontaktovali respondenty. První graf znázorňuje respondenty, kteří si myslí, že se stali cílem internetového podvodu. Druhý graf představuje odpovědi respondentů, kteří se buď nestali cílem internetového podvodu, případně o tom nevědí.



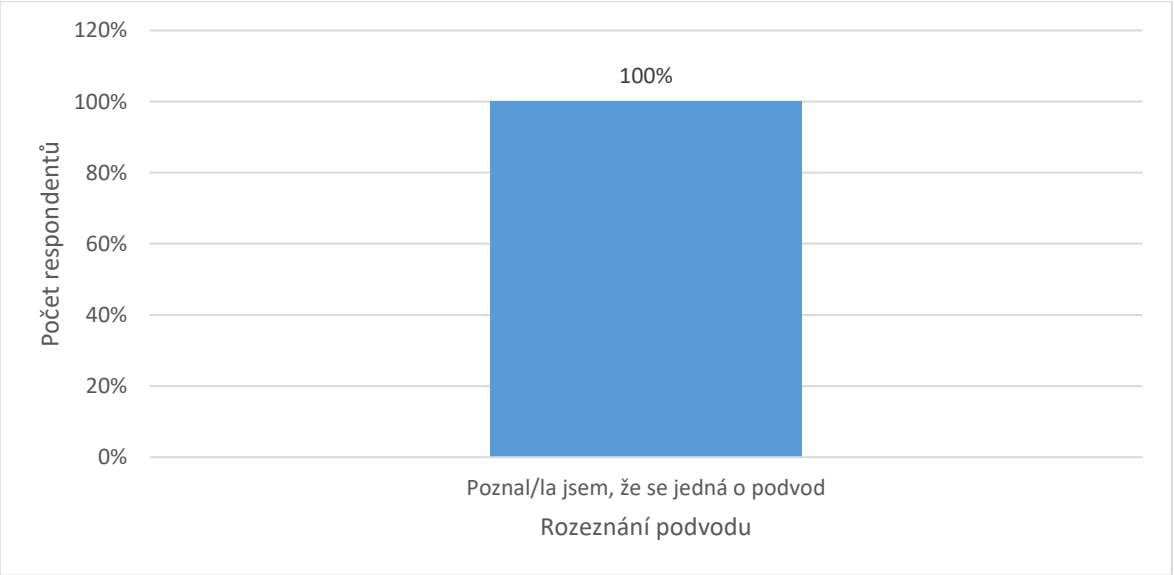
Graf 25. Jakým způsobem Vás podvodníci kontaktovali



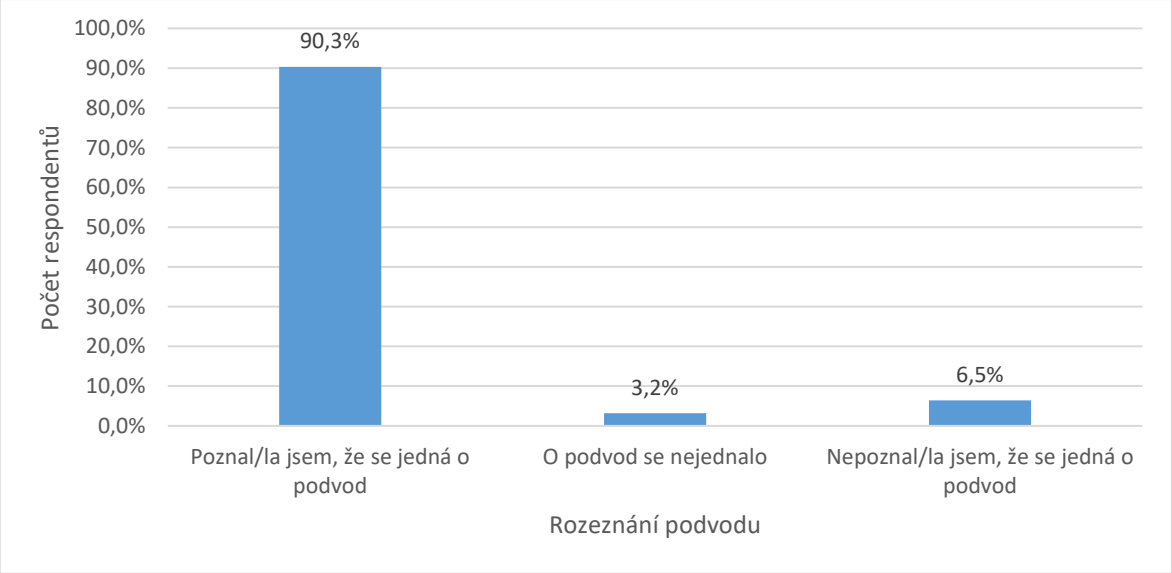
Graf 26. Jakou komunikační formu podle Vás útočníci nejčastěji využívají?

Stala se respondentovy některá z uvedených situací?

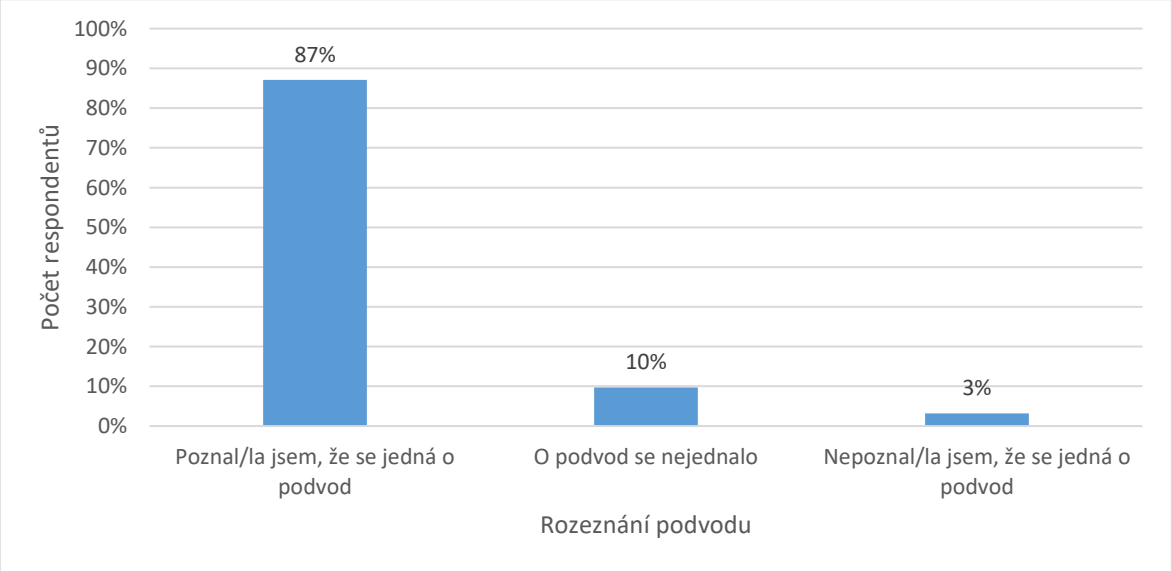
Na tuto otázku odpovídali všichni respondenti, nehledě na jejich předešlé odpovědi. Tato otázka byla položena především z důvodu toho, aby si respondenti například dodatečně uvědomily, že se stali cílem podvodu, pokud v otázce 16 odpověděli, že se zatím s podvodníky nesetkali nebo o tom nevědí. Zároveň tato otázka je zároveň spojena s následují otázkou, která se respondentů ptá, zda poznali že se jednalo o podvod, pokud se jim nějaká z uvedených situací stala.



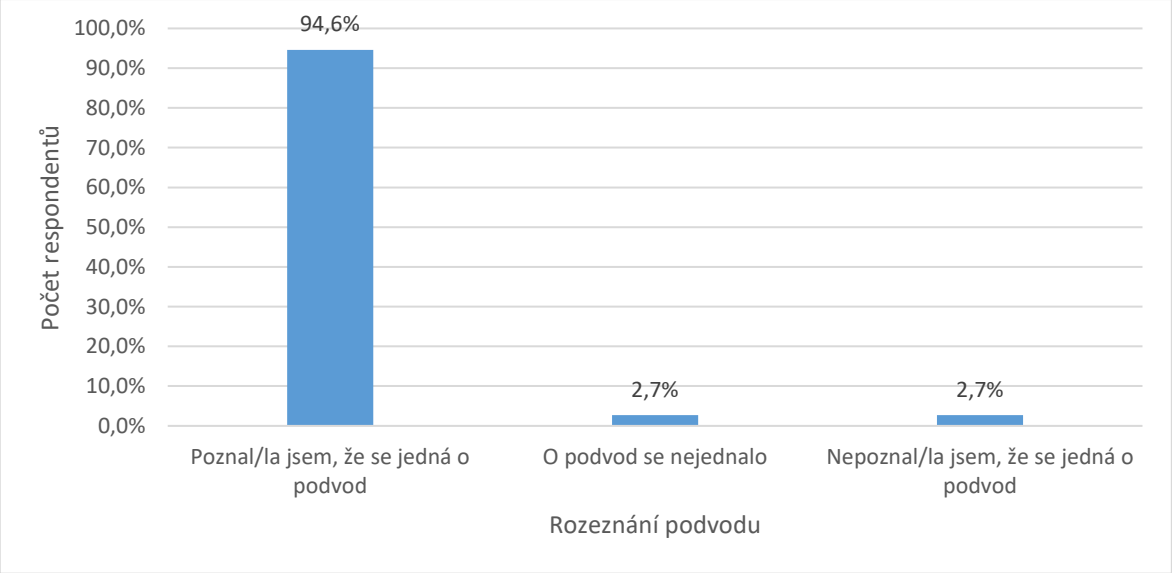
Graf 27. Napsal mi e-mail můj vedoucí z práce s prosbou buď o zaslání firemních dokumentů, citlivých informací o firmě či finančního převodu, normálně však tyto informace řeší přes jiné lidi.



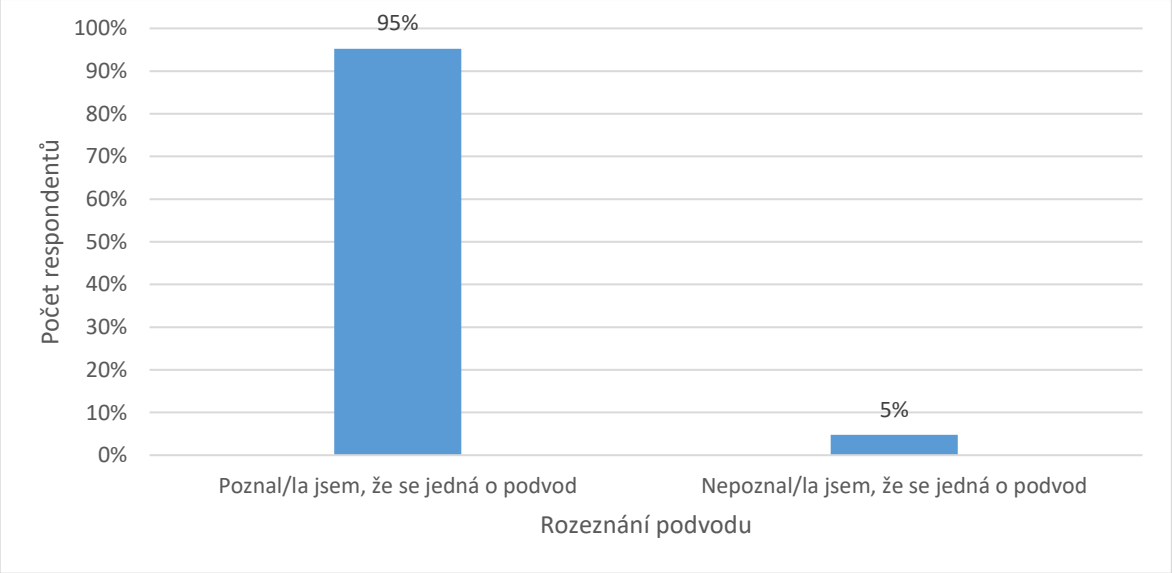
Graf 28. Využil/la jsem služby internetových obchodních portálů k prodeji (nebo nákupu) produktu, kupující či prodejce po mě chtěl zaplatit dopravu přes jím navrženou cestovní společnost.



Graf 29. Zavolal mi někdo neznámý, oznámil mi, že je buď z e-shopu nebo banky a potřeboval ode mě moje osobní údaje.



Graf 30. Někdo neznámý mi napsal e-mail, že jsem vyhrál/la větší finanční obnos, ale pro dokončení transakce se musím přihlásit přes jejich odkaz na jejich stránky.



Graf 31. Došla mi SMS s informací, že moje zásilka je připravená k expedici, nicméně není zaplacená její doprava, součástí SMS byl odkaz pro její zaplacení.

6.2.3.1 Dílčí shrnutí kapitoly

Obsahem této kapitoly bylo zjištění, jaké mají respondenti zkušenosti s internetovými podvody. Respondenti odpovídali na otázky ohledně počtu prokázaných internetových podvodů. Zda se stali cílem internetového podvodu a pokud ano, tak jestli zaznamenali zmíněné podvody. Na jakém druhu webové stránky se s podvodníky setkali a jak je podvodníci kontaktovali. Nebo jestli se respondenti setkali s nějakou z uvedených situací a jak na ni reagovali. Níže jsou uvedeny důležité poznatky.

Podle respondentů se na území České republiky v roce 2022 stalo mezi 5000 až 15000 prokázanými internetovými podvody (Tabulka 2).

Nejvíce se s internetovými podvody setkává věková skupina 16-25 let (Graf 19).

Internetový podvod, který byl respondenty nejvíce zaznamenán, byl spojený s obchodním portálem Bazoš (Graf 20).

Nejčastějším místem, kde se respondenti setkávají s podvody jsou sociální sítě (Graf 21, Graf 22, Graf 23 a Graf 24).

Respondenti, kteří se stali cílem podvodu označili e-mail jako způsob navázání komunikace mezi nimi a podvodníkem. Respondenti, kteří se nestali cílem internetového podvodu si myslí, že podvodníci ke kontaktu nejčastěji využívají sociální sítě (Graf 25, Graf 26).

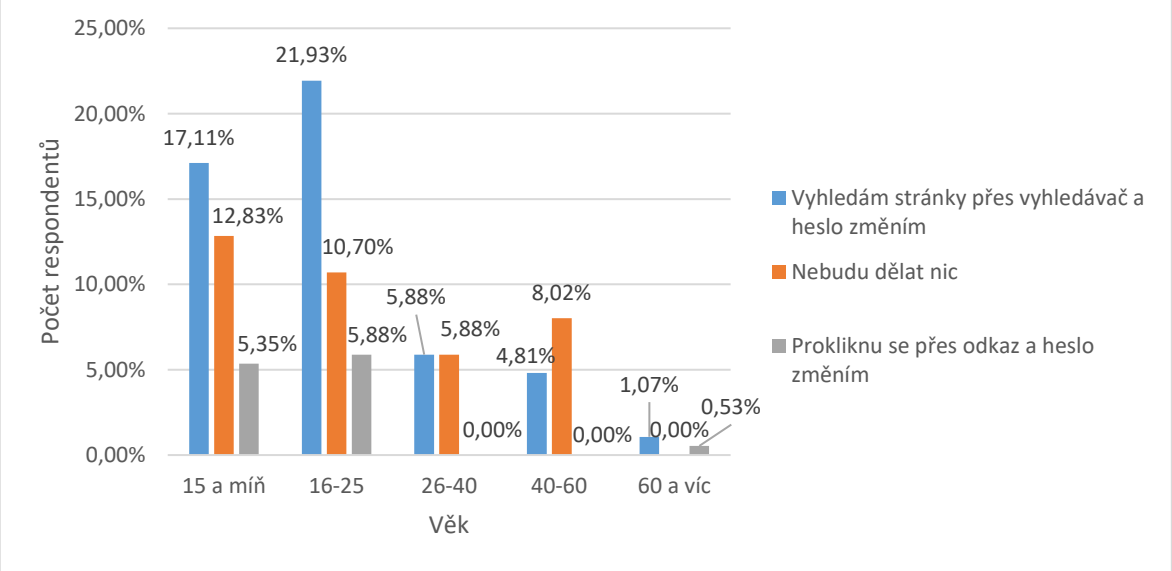
Pokud se respondentům stala některá z výše uvedených situací, byli schopni poznat, že se jedná o podvod (Graf 27, Graf 28, Graf 29, Graf 30 a Graf 31).

6.2.4 Podvodné e-maily

Respondentovi došel přiložený e-mail, jak se zachová?

Na tuto otázku mohli opět odpovídat všichni respondenti. Tento typ otázky měl za úkol prověřit respondenty v tom, jak jsou všímaví, pokud by jim přišel přiložený falešný e-mail od společnosti Facebook a jak by se v dané situaci zachovali.

Tento e-mail byl vytvořen tvůrcem dotazníku, který si vytvořil falešný e-mail Facebooku, konkrétně jejich bezpečnostního týmu, který tento typ zpráv má na starost. Pokud byl tedy respondent pozorný, tak si mohl všimnou netradičního formátu a obsahu u odesílatele zprávy a podle toho bylo možné určit, že se jedná o podvodný e-mail. E-mail je obsažen v příloze práce.



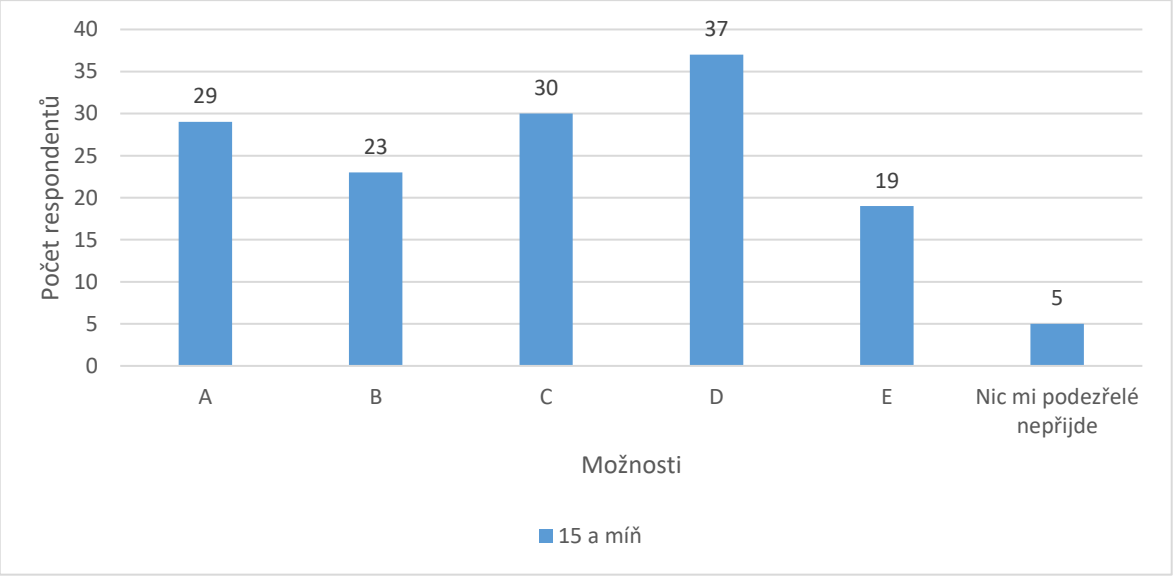
Graf 32. E-mail od Facebooku

Respondentovi došel přiložený e-mail, které části označí za podezřelé?

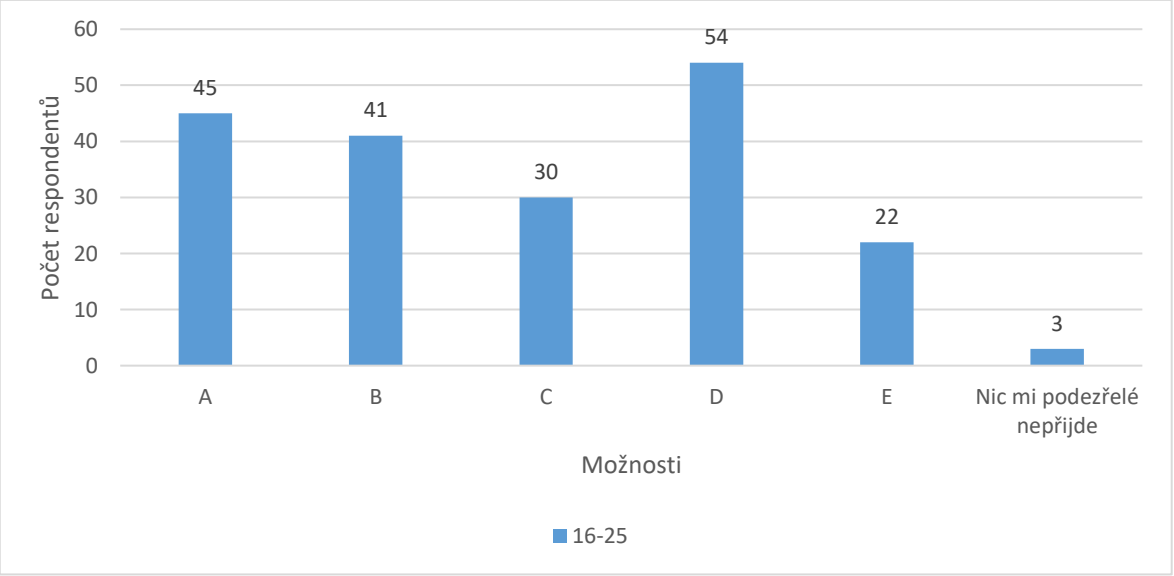
Na tento dotaz mohl opět odpovědět každý respondent. Účelem této otázky bylo zjistit, jak jsou respondenti všímaví, pokud jim přijde běžný e-mail a co považují za podezřelé, a naopak čemu vůbec nevěnují pozornost.

E-mail byl vytvořen tvůrcem dotazníku. Zpráva se rozdělovala do pěti částí: Předmět e-mailu, informacích o odesílateli, textu zprávy, prokliku na odkaz, štítku společnosti. Nicméně struktura samotného e-mailu byla udělána tak, aby respondentům nabídla části, které jsou úplně v pořádku a ničím nevyčnívají a pak na části, kde by měli určitě zpozornět. Tyto části, u kterých měli respondenti zpozornět byly: A, B a D, zbylé byly nezávadné. U

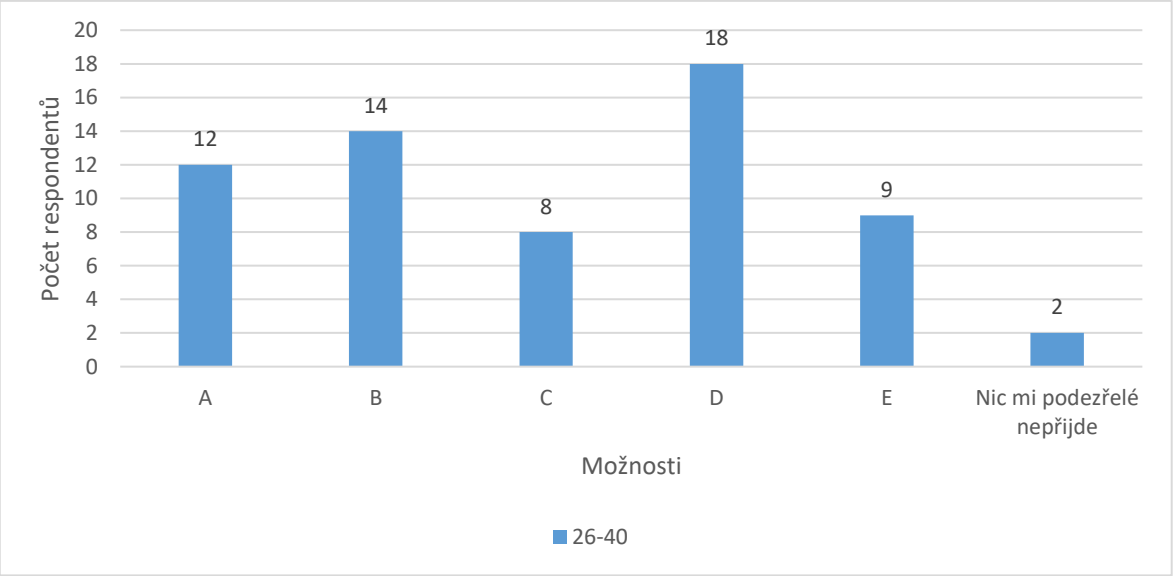
možnosti A bylo důležité si všimnout, že předmět je napsán Caps Lokem a evokuje ve svém znění nátlak na příjemce. U možnosti B si měl respondent všimnout opět falešné adresy odesílatele, která tentokrát představovala falešnou e-mailovou adresu od společnosti Google. Poslední možností, kterou měl respondent označit byla možnost D, která vyzývala uživatele k prokliku na falešnou platební bránu. Znění a vzhled této části byl vytvořen podle skutečné události. E-mail je přiložen v příloze práce.



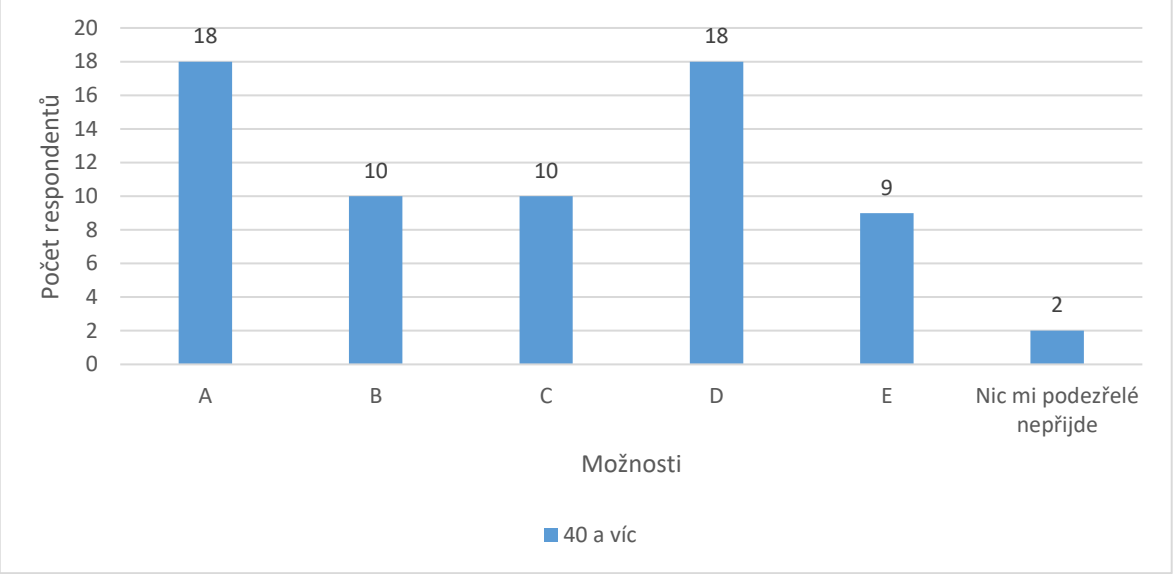
Graf 33. Věková skupina 15 a míň let



Graf 34. Věková skupina 16 až 25 let



Graf 35. Věková skupina 26 až 40 let



Graf 36. Věková kategorie 40 a více let

6.2.4.1 Dílčí shrnutí kapitoly

V této kapitole byli respondenti uvedeni do situace, která simulovala skutečný pokus podvodníka o získání citlivých informací od respondenta. Obsahem byli dva e-maily. První byl od společnosti Facebook a druhý od společnosti Google. Oba tyto e-maily byly vyrobeny tak, aby bylo po vyplnění zřejmé, jak by se respondent po jejich doručení zachoval. Níže jsou uvedeny nejdůležitější poznatky.

Pokud by respondenti dostali obdržely první e-mail od společnosti Facebook, tak by polovina z celkového počtu respondentů heslo změnila a necelé dvě třetiny z celkového počtu respondentů by neudělali nic. (Graf 32).

Pokud by respondentovy přišel druhý přiložený e-mail od společnosti Google, tak jako nejvíce podezřelé místo v e-mailu by respondenti označili část D (Graf 33, Graf 34, Graf 35, Graf 36).

6.3 Vyhodnocení hypotéz

H1: Internetové obchodní portály již využilo 53,4 % respondentů pravidelně a 39,4 % respondentů nepravidelně (Graf 2). Po sečtení obou hodnot vyšlo, že obchodní portály již použilo 92,9 % z tázaných respondentů. Předpoklad byl že drtivá většina respondentů, již obchodní portály využila. Hypotéza č. 1 tedy byla potvrzena.

H2: Platbu kartou online preferuje 50,7 % respondentů (Graf 11). Původní předpoklad pracoval s tím, že alespoň polovina respondentů tento způsob platby preferuje. Hypotéza č. 2 byla potvrzena.

H3: Virtuální kartu pro platby na internetových obchodních portálech využívá 28,26 % respondentů (Graf 14). Předpoklad této hypotézy byl, že jen málo respondentů využívá virtuální kartu. Proto hypotéza č. 3 byla potvrzena.

H4: Cílem internetového podvodu si myslí, že se stalo 38 % respondentů (Graf 19). Původní předpoklad byl, že respondentů bude alespoň polovina, proto hypotéza č. 4 nebyla potvrzena. Pokud by se však k respondentům, kteří se domnívají, že se stali cílem internetového podvodu připočetli i respondenti, kteří si nejsou jistí tak by vyšlo číslo 62 %. Pokud by se tedy bralo v potaz toto číslo tak by hypotéza č. 4 mohla být potvrzena.

H5: U prvního falešného e-mailu by neobstálo necelých 12 % respondentů (Graf 32). Předpoklad pro tuto hypotézu byl, že většina respondentů tomuto e-mailu nepodlehne. Hypotéza č. 5 byla tedy potvrzena.

6.4 Shrnutí dotazníku

Dotazník sdílený v internetové podobě celkem vyplnilo 204 respondentů. Po projití všech odpovědí respondentů bylo nakonec vyřazeno 17 odpovědí. Ke zpracování tedy zbylo 187 vyhovujících odpovědí.

Zhotovený dotazník se skládal ze čtyř pomyslných částí. První část dotazníku byla zaměřena na webové obchodní portály. Z výsledků první části dotazníku vyplynulo, že drtivá většina respondentů obchodní portály využila, nicméně se také ve velkém množství setkala s internetovými podvodníky. Pokud se respondent rozhodne nakupovat na obchodním portálu, se kterým nemá zkušenost, nejvíce dá na recenze ostatních uživatelů obchodního portálu a na místo, kde firma či společnost sídlí.

Druhá část dotazníku byla zaměřena na způsob plateb respondentů na obchodních portálech, Nejdůležitějším zjištěním bylo, že většina respondentů používá online platbu kartou. Následně pokud se respondent stal cílem internetového podvodu tak při tom využíval platby pomocí mobilního telefonu. Naopak pokud si je respondent jistý, že se cílem podvodu nestal, tak nejčastěji využíval pro platbu na internetových portálech platbu pomocí platební karty, bez využití další služby. Další důležité zjištění, které z této části vyplynulo je, že respondenti, kteří nakupují pravidelně na internetových portálech vědí o existenci virtuální platební karty, ale nevyužívají ji. Respondenti, kteří však nenakupují na obchodních portálech pravidelně, využívají virtuální platební kartu častěji. Pokud respondent uvedl, že má zřízené internetové bankovnictví, tak se v drtivé většině respondenti shodli, že mají nastavený limit na jejich platební kartě pro platbu online na webových obchodních portálech-

Ve třetí části byly zkoumány zkušenosti respondentů s internetovými podvody. Podle respondentů se na území České republiky prokázalo mezi 5000 až 15 000 internetovými podvody, kdy přesné číslo, uvedené policí ČR bylo 18 554 prokázaných podvodů (Graf 1). Z toho lze soudit, že respondenti se s podvody setkávají pravidelně. Nejčastější věková skupina, která se setkala s internetovým podvodem je v rozmezí od 16 do 25 let. Dále dle odpovědí respondentů jsou mezi nimi nejznámější internetové podvody, spojené s obchodním portálem Bazoš. S tím je spojený kontakt s podvodníkem. Respondenti, kteří se stali cílem internetového podvodu udávají, že je podvodník kontaktoval skrz e-mailovou adresu. Naopak respondenti, kteří nemají zkušenost s internetovými podvody si myslí, že podvodníci využívají pro komunikaci s obětí sociální sítě. Poté byli respondenti seznámeni s několika

situacemi, které osahovali příklady internetových podvodů, nicméně pokud se respondent s nějakou z uvedených situací setkal, tak v drtivé většině rozpoznal, že se jedná o podvod.

Čtvrtá část se týkala reakce respondenta na internetový podvod. Respondent byl vystaven dvěma falešnými e-maily, a to od společnosti Facebook a Google. První e-mail od společnosti Facebook byl vytvořen tak, aby kopíroval reálnou zprávu o přihlášení na účet respondenta. Reakce respondentů byla velmi optimistická, protože ve většině odpovědí by buď respondent nedělal nic anebo by si přihlašovací údaje změnil přes oficiální stránky Facebooku. Druhý e-mail od společnosti Google byl vytvořen tak, aby bylo možné pozorovat, čeho si respondenti všimnou, pokud jim dojde podezřele vypadající e-mail. Nejčastější odpověď, kterou respondenti označovali byla možnost D, která se týkal prokliku na webové stránky.

7 METODICKÝ NÁVOD

V dnešní době jsou již obchodní portály obeznámeny s nárůstem internetových podvodů, proto na svoje stránky umisťují pokyny pro svoje klienty, aby se nestali cílem internetových podvodníku. Tyto pokyny obsahují podrobný popis toho, s čím se může jejich zákazník setkat, a to včetně příkladů reálných podvodů, které se staly v souvislosti s jejich stránkou. Pokud si prodejce vybere k prodeji aukční portál, tak součástí e-mailu o přijetí jím vytvořeného inzerátu je i informace o tom, že prodejce nemá zadávat údaje o své platební s tím, že dostane na tuto kartu zaplaceno. Níže uvedený metodický návod proto vychází nejen z dat respondentů z předešlé kapitoly a teoretické části práce, ale i ze stránek samotných obchodních portálů. Cílem tohoto návodu, je minimalizovat úspěšnost internetových podvodníků.

7.1 Návod

Zpracování návodu proběhlo ve formě bodů, které by měl člověk dodržovat, aby se nestal cílem internetového podvodu. Samozřejmě, že i po dodržení uvedených bodů se člověk stejně může stát cílem internetového podvodu, protože se podvodníci snaží neustále zdokonalovat. Návod je rozdělen do čtyř hlavních okruhů, které se týkají obchodování na internetových portálech.

Nákup a prodej na internetových portálech

a) Nakupujte pouze na známých a prověřených obchodních portálech.
b) Vyhledejte si recenze na daný e-shop, využijte služby dTestu nebo České obchodní inspekce.
c) Zkontrolujte, zda se na stránkách e-shopu nachází obchodní podmínky.
d) Pokud se na portálu objevuje velké množství překlepů nebo gramatických chyb, rozhodně zpozorněte.
e) Pro nákup volte bezpečné internetové sítě. Veřejné internetové sítě nejsou pro tuto činnost vhodné.
f) Do mobilních telefonů stahujte pouze aplikace z oficiálních obchodů (Google Play, App Store).

Platba na internetových portálech

a) Pokud e-shop vyžaduje platbu převodem kartou na účet, zbystřete a případně vyhledejte jiný obchod.
b) Důvěryhodný e-shop má více možností, jak zaplatit objednané zboží.
c) Číslo Vaší karty zadávejte pouze na ověřených e-shopech
d) Využívejte pro platby přes internet virtuální kartu.
e) Pokud virtuální kartu nevyžíváte a platíte online kreditní kartou, nastavte si na dané kartě limit.
f) Pokud se odkazem prokliknete na stránku, která po Vás vyžaduje ověření identity pomocí internetového bankovnictví, určitě své přihlašovací údaje nevyplňujte.

Kontakt s obchodními portály

a) Pokud na e-shopu není uvedený kontakt (telefon, adresa, e-mail), vyhledejte jiný.
b) Pokud Vám dojde e-mail s podezřelým názvem a odesílatelem, e-mail neotevírejte.
c) Svá citlivá data nezveřejňujte jen kvůli popudu přišlého e-mailu nebo zprávy na sociálních sítích.
d) Neklikejte na odkazy, které Vám přijdou v podezřele vypadajících e-mailech.
e) Pokud Vám dojde SMS zpráva od dopravce, že veze Vaši objednávku a vy jste si nic neobjednali, na SMS zprávu nereagujte.
f) Pokud Vám zavolá někdo z banky, nebo jiné instituce a požaduje od Vás citlivé údaje, určitě je volajícímu nesdělujte a ukončete hovor. Následně zavolejte do příslušné instituce sami.
g) Nikdy nikomu podezřelému neumožňujte vzdálený přístup do Vašeho počítače

Jak postupovat, pokud se stanu cílem internetového podvodu

a) Pokud jste vyzradili své přihlašovací údaje například do internetového bankovnictví, tak kontaktujte banku, změňte si své přihlašovací údaje a kontaktujte policii.
b) Pokud jste zadali údaje o Vaší platební kartě, tuto kartu neprodleně zablokujte ve svém internetovém bankovnictví a kontaktujte policii.
c) Pokud podvodník získal kopii Vašich dokladů, nahlaste to neprodleně na policii.

ZÁVĚR

Tato bakalářská práce měla za cíl poukázat na hrozby, které se vyskytují v oblasti webových obchodních portálů a souvisejících služeb. Jelikož v dnešní době většina lidí využívá služeb webových obchodních portálů pravidelně, je toto téma internetových podvodů na těchto stránkách velmi aktuální. Tato problematika se samozřejmě netýká jen České republiky, ale jedná se o globální problém. Po případném přečtení této práce, by si měl čtenář uvědomit, že zmíněné podvody představují velkou hrozbu a to pro kohokoli, kdo tyto portály využívá. Zároveň upozorňuje na to, jak je jednoduché stát se v dnešní době cílem internetového podvodu a přitom netušit, že je něco v nepořádku. V neposlední řadě by tato práce mohla pro čtenáře posloužit jako pomyslné vodítko, jak čelit případnému pokusu internetového podvodníka a minimalizovat jeho úspěch.

V teoretické části práce byly popsány jednotlivé obchodní portály či aukční síně, které podvodníci rádi využívají ke svým aktivitám. Následně zde byly zmíněny bankovní a nebankovní formy plateb na obchodních portálech. Je také zřejmé, že způsob provedení podvodu se liší v závislosti na cílové skupině. Zvlášť patrný rozdíl lze vidět s útokem na cílovou skupinu mladistvých v porovnání s útokem na cílovou skupinou nad 60 let. Také zde byly vysvětleny metody, které podvodníci využívají. Mezi metody patří především Phishing, Spoofing či Vishing. Na závěr teoretické části práce jsou rozebrány indikátory, které mohou pomoci rozeznat, zda se jedná o podvodný webový obchodní portál či nikoli. Mezi indikátory, které jsou nejvíce směrodatné, patří především absence obchodních podmínek na webu, nespisovná čeština či netradiční nacenění produktů.

Praktická část bakalářské práce byla rozdělena na dvě kapitoly. První kapitola se věnovala dotazníku, který byl zpracován tak, aby z jeho výsledků bylo zřejmé, jaké zkušenosti mají respondenti s internetovými podvody. Dotazník obsahoval 25 otázek, které byly pomyslně rozděleny na čtyři části a vyhodnoceny buď pomocí grafů nebo tabulky. Každá část dotazníku má své vlastní vyhodnocení. Nejpodstatnější jsou tato fakta. Drtivá většina respondentů, která obchodní portály využila, se zároveň již setkala s internetovým podvodem (Graf 3). Respondenti preferují způsob platby online, a to formou platební karty (Graf 11). Respondenti nejčastěji zaznamenali internetové podvody spojené s aukčním portálem Bazoš (Graf 20). Pokud se respondent stal cílem internetového podvodu, byl kontaktován pomocí e- mailové zprávy (Graf 25). Jen velmi málo respondentů se nakonec stalo cílem uvedeného internetového podvodu (Graf 32).

Druhá kapitola je zaměřena na metodický návod, jak se chovat, aby se člověk nestal cílem internetového podvodu. Obsahuje rady, jak se bezpečně pohybovat v prostředí obchodních portálů. Co je dobré dodržovat při platbách na obchodních portálech. Na co si dát pozor při komunikaci prostřednictvím webových obchodních portálů. Nebo také jak se zachovat, pokud se již stanu cílem internetového podvodu. Zároveň je potřeba podotknout, že se prodejce nebo nakupující může stát cílem internetového podvodu i při dodržení všech zmíněných rad a doporučení. Protože internetoví podvodníci budou své metody neustále zdokonalovat, jsou ostražitost a selský rozum při využívání webových obchodních portálů vždy na místě.

SEZNAM POUŽITÉ LITERATURY

[1] Statistika kyberkriminality. *Policie ČR* [online]. Praha: Policie ČR, 2020 [cit. 2023-05-26]. Dostupné z: https://www.policie.cz/clanek/zverejnene-informace-2020-statistika-kyberkriminality.aspx

[2] Vývoj registrované kriminality v roce 2021. *Policie ČR* [online]. Praha: Policie ČR, 2021 [cit. 2023-05-26]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx

[3] Vývoj registrované kriminality v roce 2022. *Policie ČR* [online]. Praha: Policie ČR, 2022 [cit. 2023-05-26]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

[4] Velikost e-commerce trhu. *Česka e-commerce* [online]. Praha: Shoptet, 2022 [cit. 2022-12-16]. Dostupné z: https://www.ceska-ecommerce.cz/

[5] E-commerce. *Idealab* [online]. Praha: Idealab, 2022 [cit. 2022-12-16]. Dostupné z: https://idealab.cz/slovnik/e-commerce/

[6] Nové podvody na českých inzertních portálech: Jak fungují a na co si dát pozor? *Avast* [online]. Praha: Avast Software, 2021 [cit. 2022-12-16]. Dostupné z: https://blog.avast.com/cs/nove-podvody-na-ceskych-inzertnich-portalech-jak-funguji-a-na-co-si-dat-pozor

[7] Informace o Nákupech na Instagramu. *Meta* [online]. Meta [cit. 2022-12-16]. Dostunéz:https://business.itagram.com/?ref=fb4b_site&fbclid=IwAR2jKH9TyVpKNCLBVNbkPSg2nWlbSfRrsNjfi3nLF8XxKs_rBoOGYL-UVjc

[8] Česká pošta. *Česká pošta* [online]. Praha: Česká pošta, 2022 [cit. 2023-05-26]. Dostupné z: https://www.ceskaposta.cz/index

[9] Profesional Parcel Logistic. *Profesional Parcel Logistic* [online]. Praha: PPL, 2023 [cit. 2023-05-26]. Dostupné z: https://www.ppl.cz/o-nas

[10] *Platby na internetu prostřednictvím platebních karet*. Praha, 2012. Diplomová práce. Bankovní institut vysoká škola Praha.

[11] *Elektronické platby na internetu v České republice*. Praha, 2009. Diplomová práce. Bankovní institut vysoká škola Praha.

[12] Co je platba kartou online a jak funguje?. *GoPay* [online]. Planá: GOPAY s.r.o., 2018 [cit. 2022-12-16]. Dostupné z: https://www.gopay.com/blog/co-je-platba-kartou-online-a-jak-funguje/

[13] Jaké existují platební metody?. *Kevin.* [online]. kevin., 2022 [cit. 2022-12-16]. Dostupné z: https://www.kevin.eu/cs-cz/blog/platebni-metody/

[14] Platba na dobírku: Jak funguje a kolik vás bude stát?. *Skip Pay* [online]. Praha: Skip Pay, 2022 [cit. 2022-12-16]. Dostupné z: https://skippay.cz/dobirka

[15] *Zákon o platebník styku*. In: . Praha: Parlament České republiky, 2017, ročník 2017, číslo 370.

[16] Jak funguje PayPal. *MONETA Money bank* [online]. Praha: MONETA Money bank, 2022 [cit. 2022-12-16]. Dostupné z: https://www.moneta.cz/caste-dotazy/odpoved/jak-funguje-paypal

[17] Až třetina lidí se stala cílem podvodu na internetových bazarech. *ESET* [online]. Praha: ESET software spol. s r.o., 2022 [cit. 2023-05-26]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/pruzkum-eset-tretina-lidi-se-stala-cilem-podvodu-na-internetovych-bazarech/

[18] Banky varují před podvodem s odměnou za přihlášení do bankovnictví. *IDnes* [online]. Praha: MAFRA, a.s, 2016 [cit. 2023-05-26]. Dostupné z: https://www.idnes.cz/technet/kratke-zpravy/bankovnictvi-odmena-podvod.A161215_163955_tec-kratke-zpravy_vse

[19] #nePINdej!. *Policie ČR* [online]. Praha: Policie ČR, 2022 [cit. 2023-05-26]. Dostupné z: https://www.policie.cz/clanek/nepindej.aspx

[20] *Bezpečně na internetu průvodce chováním ve světě online*. 6137. U Průhonu 22, Praha 7: Grada, 2016. ISBN 978-80-271-9074-4.

[21] *Využití metod sociálního inženýrství pro etický hacking*. Hradec Králové, 2017. Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu.

[22] Co je phishing?. *ESET* [online]. Amerika: ESET, spol. s r.o., 2019 [cit. 2022-12-09]. Dostupné z: https://www.eset.com/cz/phishing/

[23] Social engineering scams. *Interpol* [online]. Lyon: Interpol, 2022 [cit. 2022-12-09]. Dostupné z: https://www.interpol.int/Crimes/Financial-crime/Social-engineering-scams

[24] 9 kroků, jak poznat podvodné e-maily. In: *Dvojklik* [online]. Bratislava: ESET software spol. s r.o., 2021 [cit. 2022-12-16]. Dostupné z: https://www.dvojklik.cz/9-kroku-jak-poznat-podvodne-e-maily/

[25] Techniky sociálního inženýrství. *KPCS* [online]. Praha: KPCS, 2020 [cit. 2022-12-09]. Dostupné z: https://www.kpcs.cz/cs/novinky/blog/techniky-socialniho-inzenyrstvi.html

[26] Co je vishing?. *ESET* [online]. Amerika: ESET, spol. s r.o., 2019 [cit. 2022-12-09]. Dostupné z: https://www.eset.com/cz/vishing/

[27] Příklad phishingového útoku v podobě SMS zprávy. In: *Forensee* [online]. Praha: forensee, 2021 [cit. 2022-12-16]. Dostupné z: https://www.forensee.cz/2021/05/03/priklad-phishingoveho-utoku-v-podobe-sms-zpravy/

[28] What is a spoofing attack?. *Alwarebytes* [online]. Clearwater, 2022 [cit. 2022-12-16]. Dostupné z: https://www.malwarebytes.com/spoofing

[29] Co je to spoofing?. *InSmart* [online]. Praha: insmart.cz, 2021 [cit. 2022-12-16]. Dostupné z: https://insmart.cz/co-je-spoofing/

[30] *CyberCrime*. Praha: Edice CZ.NIC, 2016. ISBN 978-80-88168-15-7.

[31] PHISHING. In: *Internetem bezpečně* [online]. Karlovy Vary: INTERNETEM BEZPEČNĚ, 2018 [cit. 2022-12-16]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/

[32] MITM (Man in the middle). *Digitální pevnost* [online]. ČR: Digitální pevnost, 2018 [cit. 2022-12-09]. Dostupné z: https://www.digitalnipevnost.cz/viki/mitm-man-middle

[33] Social Engineering Technique: The Watering Hole Attack. *Medium* [online]. Medium, 2021 [cit. 2022-12-16]. Dostupné z: https://medium.com/@thefoursec/social-engineering-technique-the-watering-hole-attack-9ee3d2ca17b4

[34] What is a Quid Pro Quo Attack?. *Techslang* [online]. Techslang, 2021 [cit. 2022-12-16]. Dostupné z: https://www.techslang.com/definition/what-is-a-quid-pro-quo-attack/

[35] 15 Examples of Real Social Engineering Attacks. *Tessian* [online]. London: Tessian Limited, 2023 [cit. 2022-10-18]. Dostupné z: https://www.tessian.com/blog/examples-of-social-engineering-attacks/

[36] Podvodné e-shopy? *Co vybrat* [online]. Co vybrat, 2022 [cit. 2022-12-09]. Dostupné z: https://www.covybrat.cz/recenze-eshopu/podvodne-e-shopy-31156/#jak-ziskat-penize-z-podvodneho-e-shopu

[37] Rizikové internetové obchody. *Česká obchodní inspekce* [online]. ČR: Česká obchodní inspekce, 2022 [cit. 2022-12-09]. Dostupné z: https://www.coi.cz/rizikove-internetove-obchody/

[38] Základní informace. In: *Alza* [online]. Praha: Alza.cz, 2022 [cit. 2022-12-16]. Dostupné z: https://www.alza.cz/zakladni-informace

[39] *Zákon o ochraně spotřebitele*. In: Praha: Parlament České republiky, 1992, číslo 634.

[40] Prohlížení doménového jména. *CZ.NIC* [online]. Praha: CZ.NIC, z. s. p. o., 2022 [cit. 2022-12-16]. Dostupné z: https://www.nic.cz/

[41] Ověření e-shopů. *DTest* [online]. Praha: dTest, 2022 [cit. 2022-12-09]. Dostupné z: https://www.dtest.cz/eshopy

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	Česká republika
B2B	Podnik k podniku
B2C	Podnik ke spotřebitelovi
C2B	Spotřebitelé a podniky
C2C	Spotřebitelé mezi sebou
PPL	Profesionální balíková logistika
DHL	Dalsey, Hillblom, Lynn
DPD	Přímá distribuce balíků
HTTPS	Hypertext transfer protocol secure
iOS	Operační systém iPhone
URL	Jednotný vyhledávač zdrojů
CVC	Ověřovací kód banky
DM	Přímá zpráva
WI-FI	Bezdrátová přesnost
IČ	Identifikační číslo osoby
DIČ	Daňové identifikační číslo

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

Interní přílohy

Příloha P I: Dotazníkové šetření

Externí přílohy

Příloha P II: Stažená a zpracovaná data ze Survia

Příloha P III: Originální odpovědi ze Survia

PŘÍLOHA P I: DOTAZNÍKOVÉ ŠETŘENÍ

Podvody na prodejních portálech a souvisejících službách

Dobrý den, obracím se na Vás s žádostí o vyplnění mého dotazníku, jež je součástí praktické části mé Bakalářské práce. Cílem tohoto dotazníku je analýza zkušeností obyvatel České republiky s internetovými podvody. Účast ve výzkumu je anonymní a dobrovolná. Předem děkuji za spolupráci.

František Tragan, student Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně.

1. Úvod a obchodní portály

1) Jaké je Vaše pohlaví?

- Žena
- Muž
- Jiné

2) Jaký je Váš věk:

- 15 a míň
- 16-25
- 26-40
- 40-60
- 60 a víc

3) Jaké je Vaše nejvyšší dosažené vzdělání?

- Základní
- Střední s maturitou
- Odborné učiliště
- Vysokoškolské
- Jiné

4) Jak často využíváte webové obchodní portály?

- Pravidelně (denně nebo několikrát do měsíce)
- Nepravidelně (párkrát za rok)
- Zatím nikdy

5) Pokud jste tyto portály již použili, v jaké roli jste byli?

- Prodejce
- Kupující

- Prodejce i kupující

6) Využil/la jste ke koupi produktů nějakou z uvedených sociálních sítí?

- Facebook Marketplace
- Instagram (pomocí DM zpráv či Insta Stories)
- Ne nevyužil/la

7) Jak vyhledáváte obchodní portál na internetu?

- Pomocí prokliku z hypertextového odkazu
- Přímým zadáním adresy portálu
- Pomocí vyhledávače

8) Ověřoval/la jste si někdy pravost e-shopu?

- Ano
- Ne

9) Jaké indikátory jsou podle Vás důležité k rozpoznání podvodného e-shopu?

- Jméno provozovatele
- Sídlo firmy či společnosti
- Neuvedení Obchodních podmínek na webu
- Recenze zákazníků
- Fotografie produktů
- Nespisovný jazyk
- Název a vlastník domény
- Ceny produktů

2. Platba přes internet

10) Jakou formu platby preferujete?

- Osobně (hotově)
- Dobírkou
- Online platba kartou
- Bankovním převodem
- Jiné

11) Jaký typ online platby upřednostňujete?

- Online, zadáním údajů o platební kartě bez využití další služby
- Online, zadáním údajů o platební kartě s využitím např. GoPay
- Mobilní platbu (Google Pay, Apple Pay)
- Pay Pal

- Jiné

12) Využíváte pro platbu na internetu virtuální kartu?

- Ano
- Vím, že existují, ale nepoužívám ji
- Ne nikdy jsem o ní neslyšel/la

13) Máte ve svém internetovém bankovnictví nastavený limit pro platby kartou přes internet?

- Ne, limit mám defaultně nastavený bankou
- Ano, limit jsem si nastavil podle svých potřeb
- Nevím
- Nemám internetové bankovnictví

3. Podvody na internetu

14) Kolik si myslíte, že se na území České republiky stalo prokázaných internetových podvodů v roce 2022?

- 100–1000
- 1000–5000
- 5000–15000
- 15000–20000
- 20000 a víc

15) Zaznamenal/la jste některý z níže uvedených příkladů internetových podvodů na internetu?

- Internetový podvod v souvislosti s automobilkou Škoda Auto, kdy podvodníci nabízeli možnost investic či soutěží.
- Skupina podvodníků, kteří využívali falešné investiční bitcoinové platformy.
- Podvody na online bazarech (Bazoš, Sbazar, Vinted), kdy se podvodníci vydávají za kupce. Následně se snaží svou oběť přesvědčit, aby zaplatila dopravu přes odkaz, který obsahuje podvodnou platební bránu, díky které získají citlivé údaje oběti.
- Podvodníci vytvořili falešné inzeráty, které vylepovali na veřejných místech. Součástí těchto inzerátů byl QR kód, kde po jeho načtení byla dotyčná osoba přesměrována na podvodné stránky, díky kterým podvodníci získávali citlivá data oběti.
- Podvodníci vytvořili podvodnou aplikaci pro online sázení, po zaregistrování podvodníci získali citlivá data uživatele.

16) Domníváte se, že jste se někdy v minulosti mohl/la stát cílem internetového podvodu?

- Ano
- Ne

- Nevím

17) Na jakém druhu webové stránky jste se s útočníky setkal/la?

- Amazon
- Česká pošta
- PPL
- DPD
- DHL
- AliExpress
- eBay
- Wish
- Bazoš
- Aukro
- Sbazar
- Sociální sítě (Facebook Marketplace, Instagram DM)
- Letgo
- Vinted
- Allegro
- Jiné

18) Jakým způsobem Vás podvodníci kontaktovali?

- E-mail
- WhatsApp
- Sociální sítě (Facebook, Instagram)
- SMS
- Telefonát
- Jiné

19) Jakou komunikační formu podle Vás útočníci nejčastěji využívají?

- E-mail
- SMS
- Sociální sítě (Facebook, Instagram)
- WhatsApp
- Telefonát

20) Stala se Vám v minulosti některá z těchto situací?

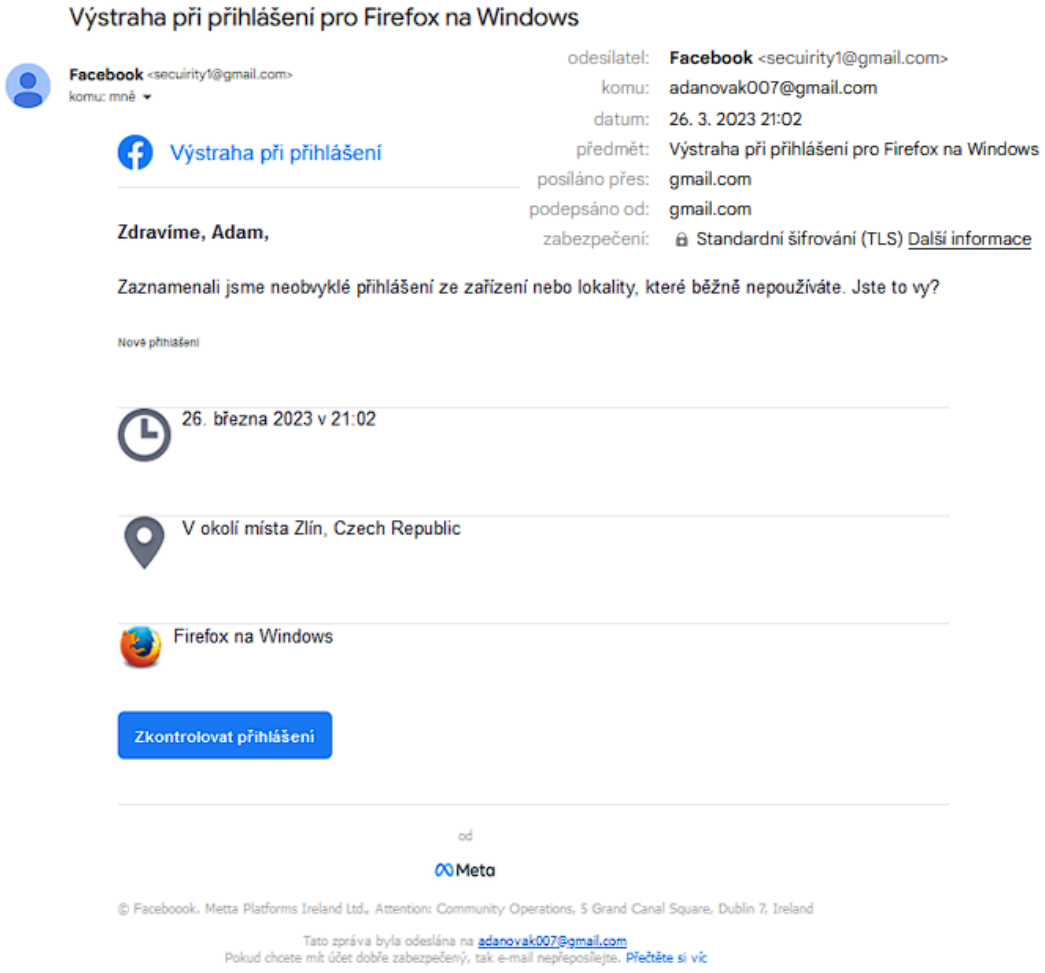
- Zavolal mi někdo neznámý, oznámil mi, že je buď z e-shopu nebo banky a potřeboval ode mě moje osobní údaje.
- Napsal mi e-mail můj vedoucí z práce s prosbou buď o zaslání firemních dokumentů, citlivých informací o firmě či finančního převodu, normálně však tyto informace řeší přes jiné lidi.
- Napsal mi někdo neznámí e-mail, že jsem vyhrál/la větší finanční obnos, ale pro dokončení transakce se musím přihlásit přes jejich odkaz na jejich stránky.
- Využil/la jsem služby internetových obchodních portálů k prodeji (nebo nákupu) produktu, kupující či prodejce po mě chtěl zaplatit dopravu přes jím navrženou cestovní společnost.
- Došla mi SMS s informací, že moje zásilka je připravená k expedici, nicméně není zaplacená její doprava, součástí SMS byl odkaz pro její zaplacení.
- Ne žádná z těchto situací se mi nikdy nestala

21) Pokud se Vám nějaká z těchto situací stala, jak jste se zachoval/la?

- Poznal/la jsem, že se jedná o podvod
- Nepoznal/la jsem, že se jedná o podvod
- podvod se nejednalo

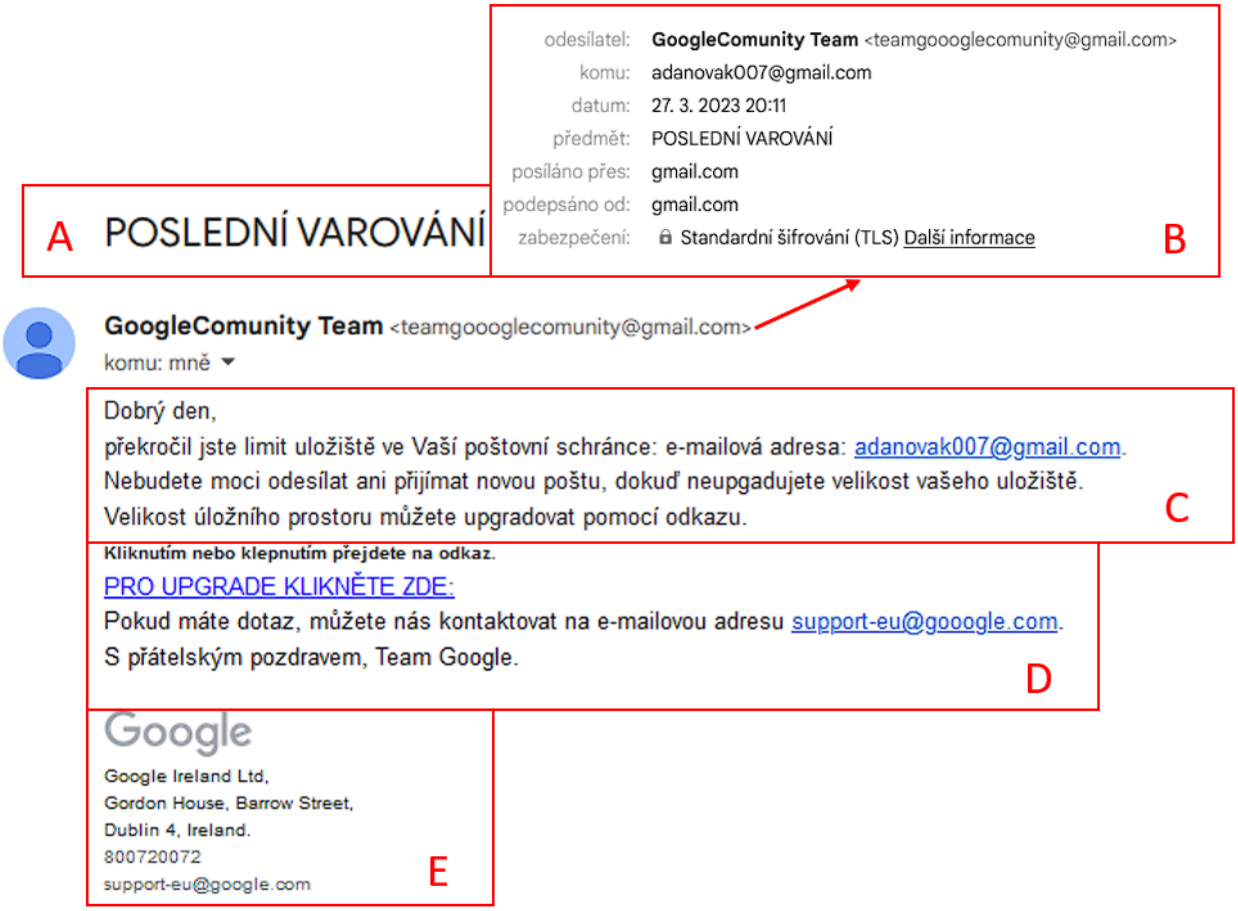
4. Podvodné e-maily

22) Pokud by Vám přišel přiložený e-mail s tím, že o přihlášení nevíte, jak byste postupovali?



- Prokliknu se přes odkaz a heslo změním
- Vyhledám stránky přes vyhledávač a heslo změním
- Nebudu dělat nic

23) Přišel Vám přiložený e-mail, které části byste označil/la za podezřelé?



- A
- B
- C
- D
- E
- Nic mi podezřelé nepřijde

24) Pokud máte nějakou osobní zkušenost a nevadí Vám se o ní se mnou podělit zde je možnost.

- Otevřená nepovinná odpověď

25) Pokud máte zájem, mohu Vám na Vaši e-mailovou adresu zaslat správně vyplněné otázky 9, 14, 22 a 23.

- Otevřená nepovinná odpověď