VYSOKÁ ŠKOLA POLYTECHNICKÁ JIHLAVA

Aplikovaná informatika

SOCIÁLNÍ INŽENÝRSTVÍ A PHISHING: DETEKCE A OBRANA

Bakalářská práce

Autor práce: Lenka Košťálová

Vedoucí práce: Mgr. Antonín Přibyl

Jihlava 2026

Vysoká škola polytechnická Jihlava

Tolstého 16, 586 01 Jihlava

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Autor práce:	**Lenka Košťálová**
Studijní program:	Aplikovaná informatika
Garant studijního programu:	Ing. Lenka Kuklišová Pavelková, Ph.D.
Název práce:	**Sociální inženýrství a phishing: detekce a obrana**
Vedoucí práce:	Mgr. Antonín Přibyl
Cíl práce:	Cílem práce je analyzovat techniky sociálního inženýrství se zaměřením na phishing, zmapovat jejich vývoj a současné trendy, vyhodnotit dostupné nástroje a postupy detekce a prevence a navrhnout doporučení pro zvýšení odolnosti uživatelů i organizací.Součástí práce je návrh a implementace prototypu prohlížečového rozšíření, které varuje před potenciálně nebezpečnými URL (např. detekce podezřelých parametrů a známých vzorů přesměrování).

Abstrakt

Bakalářská práce se v teoretické části věnuje problematice sociálního inženýrství se zaměřením na phishing a jeho metody. Podrobně analyzuje jejich vývoj a současné trendy a rozebírá manipulační techniky představující riziko pro kybernetickou bezpečnost. Na základě zjištění formuluje doporučení ke zvýšení odolnosti jednotlivců s omezenými zkušenostmi v oblasti informačních technologií i malých a velkých organizací vůči phishingovým útokům.

Praktická část představuje návrh a implementaci prototypu prohlížečového rozšíření pro identifikaci potenciálně rizikových odkazů na základě detekčních pravidel (vlastnosti domény, podezřelé parametry URL, vzorce přesměrování) s následným upozorněním uživatele na hrozbu. Účinnost navrženého řešení je ilustrována na vybraném scénáři a testovacím případě.

Hlavním přínosem práce je analýza sociálního inženýrství a technik phishingu, srovnání detekčních a preventivních nástrojů a praktický návrh bezpečnostního protiopatření použitelný v běžném uživatelském prostředí.

Klíčová slova

Sociální inženýrství; phishing; kybernetická bezpečnost; detekce URL; prohlížečové rozšíření; detekční pravidla; manipulativní techniky

Abstract

The bachelor’s thesis, in its theoretical part, deals with the issue of social engineering with a focus on phishing and its methods. It provides a detailed analysis of their development and current trends and discusses manipulation techniques that pose a risk to cybersecurity. Based on the findings, it formulates recommendations to increase the resilience of individuals and organizations to phishing attacks. The practical part presents the design and implementation of a prototype browser extension which, on the basis of detection rules (domain properties, suspicious URL parameters, redirection patterns), identifies potentially risky links and alerts the user to the threat. The effectiveness of the proposed solution is illustrated on a selected scenario and a test case. The main contribution of the thesis is the analysis of social engineering and phishing techniques, the comparison of detection and preventive tools, and the practical design of a security countermeasure usable in a common user environment.

Keywords

Social engineering; phishing; cybersecurity; URL detection; browser extension; detection rules; manipulative techniques

Prohlašuji, že předložená bakalářská práce je původní a zpracoval/a jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil/a autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění, dále též „**AZ**“).

Byl/a jsem seznámen/a s tím, že na mou bakalářskou práci se plně vztahuje **AZ**, zejména § 60 (školní dílo).

Podle § 47b zákona o vysokých školách souhlasím se zveřejněním své práce podle Směrnice pro vedení, vypracování a zveřejňování závěrečných prací na VŠPJ, a to bez ohledu na výsledek obhajoby.

Beru na vědomí, že VŠPJ má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom/a toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem VŠPJ, která má právo ode mě požadovat přiměřený příspěvek na úhradu nákladů, vynaložených vysokou školou na vytvoření díla (až do jejich skutečné výše), z výdělku dosaženého v souvislosti s užitím díla či poskytnutím licence.

V Jihlavě dne 15. dubna 2026

…….

Podpis studenta/ky

Poděkování

Chtěla bych poděkovat svému vedoucímu Mgr. Antonínu Přibylovi za vedení při vypracování závěrečné práce.

Dále děkuji své drahé polovičce za pevné nervy při zpracování práce a své kamarádce za to, že mi pomáhala udržet hlavu nad vodou – věříme si, věříme.

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

2FA	Dvoufaktorové ověření
API	Aplikační programové rozhraní
APT1	Označení čínské pokročilé perzistentní hrozby
BEC	Kompromitace firemní e-mailové komunikace
Bit.ly	Služba pro zkracování webových adres
CVC/CVV	Ověřovací kód platební karty
GPU	Grafický procesor
HTTPS	Zabezpečený protokol – Hypertext Transfer Protocol Secure
IBAN	Mezinárodní číslo bankovního účtu
IDN	Internacionalizovaný název domény
MD5	Hashovací funkce MD5
MFA	Vícefaktorové ověřování
NCSC	Národní centrum kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSINT	Zpravodajství z otevřených zdrojů
PIN	Osobní identifikační číslo
QR	Quick Response – typ čárového kódu
RSA	Kryptosystém Rivest–Shamir–Adleman
Tinyurl	Služba pro zkracování webových adres
URL	Webová adresa zdroje
Zero-day	Dosud neopravená bezpečnostní zranitelnost

Úvod

V rámci každodenní práce s internetem je uživatel vystaven mnoha drobným rozhodnutím. Rutinní charakter činností vede ke snížení pozornosti, což zvyšuje zranitelnost vůči kybernetickým útokům. Phishing se neopírá jen o technologie, ale především jde o lidské návyky, psychologii a vytvoření si důvěry s obětí. Aktuálnost tématu podtrhuje nástup snadno dostupných AI modelů i registrace domén s podobností na první pohled odpovídající značkám, jimž uživatelé běžně důvěřují.

V teoretické části práce mapuji vývoj phishingu a kategorizuji současné taktiky sociálního inženýrství. Zaměřuji se zejména na časový tlak, argument autoritou, reputační parazitování na doménách, přesměrovací řetězce a zkracovače URL.

Současně kriticky hodnotím detekční a preventivní nástroje s cílem formulovat doporučení pro posílení odolnosti uživatelů i malých a velkých organizací.

Praktická část obsahuje návrh a implementaci prototypu rozšíření pro webový prohlížeč s hodnocením rizikovosti odkazů v reálném čase na základě transparentních pravidel. Součástí pravidel je detekce IDN/homoglyfů, analýza parametrů URL a rozpoznání typických vzorců přesměrování. Varování jsou vysvětlitelná a navržená s ohledem na minimální vyrušení uživatele.

Cílem práce je snížit riziko phishingu propojením teorie sociálního inženýrství s jednoduše interpretovatelnými kontrolami v prohlížeči. Přístup využívá behaviorální principy k podpoře obezřetnosti při práci s odkazy a k omezení manipulačních efektů útočníků.

1 Sociální inženýrství

Sociální inženýrství zahrnuje soubor strategických metod určených k tomu, aby uživatele přivedly k prozrazení citlivých osobních údajů nebo k umožnění přístupu do interních struktur organizací. Útočníci často pracují s nabídkami působícími natolik výhodně, že je oběť hůře odmítá, čímž vzniká psychologický tlak vedoucí ke splnění požadavků. Motivace obětí bývá nejčastěji ovlivněna strachem nebo očekáváním zisku.

Útoky mohou být prováděny odkudkoliv, přičemž klíčovým prvkem je lidský faktor.

1.1 Historie a vývoj

Kapitola představuje vývoj sociálního inženýrství od phreakingu a fyzických metod v 80. a 90. letech až po dnešní kombinaci psychologických technik a využívání zranitelností. Cílem je ukázat, jak technologický pokrok a změny v chování uživatelů ovlivnily taktiku útočníků.

1.1.1 60. léta

První historické zmínky o sociálním inženýrství pocházejí ze 60. let 20. století a týkají se útoku zvaného phreaking (Lapsley, 2013).

Phreaking spočívá v manipulaci s telekomunikačními systémy za účelem obcházení poplatků a řízení (směrování) hovorů. Zahrnoval používání tónové volby a trunkových linek i manipulaci s operátory, kteří umožňovali přesměrování hovorů a volání zdarma. K účelu se využíval signál o frekvenci 2600 Hz: krátký tón přiměl systém, aby si myslel, že je linka volná, což umožnilo přesměrování hovorů bez účtování poplatků (Lapsley, 2013).

Hlavní postavou útoku byl Ralph Barclay, vyvinul „blue box“ a prolomil telekomunikační síť Ma Bell a umožnil volání zdarma (Lapsley, 2013).

1.1.2 80.– 90. léta

V 80. a 90. letech došlo k rychlému rozvoji informačních technologií, což brzy přitáhlo pozornost kyberzločinců a vyvolalo obavy o kybernetickou bezpečnost.

Pachatelé začali ve velké míře využívat fyzické i psychologické metody. Mezi fyzické metody patřil pretexting, kdy musí být útočník v přímém kontaktu s obětí a často uplatňuje psychologický nátlak (Social-engineer, nedatováno).

Další technikou byl shoulder surfing, tedy nenápadné pozorování při zadávání uživatelských jmen, hesel a dalších údajů. Neoprávněný vstup a tailgating zahrnovaly získání přístupu do budov, kdy sociální inženýři využili navázané vztahy se zaměstnanci a vešli „v závěsu“ za nimi. Běžná byla technika dumpster diving, kdy pachatelé prohledávali vyřazené materiály a dokumenty, aby našli cenné informace využitelné ve svůj prospěch (Social-engineer, nedatováno).

1.1.3 Současnost

Současné hrozby stojí hlavně na zneužívání zranitelností a na zapojení třetích stran, což výrazně zvyšuje riziko průniků. Ransomware přitom zůstává klíčovým motivem útočníků - často začíná exploitem zranitelnosti nebo kompromitací účtu a má vážné provozní dopady. Phishing a další formy sociálního inženýrství zůstávají častou cestou k získání počátečního přístupu. Následně se objevuje nasazení malwaru, exfiltrace dat a zneužívání rozšířených zranitelností na koncových zařízeních s postupným odstraňováním v rámci aktualizací. Dopady zasahují firmy všech velikostí i odvětví a zahrnují finanční ztráty, poškození reputace a výpadky provozu (Verizon, 2025).

1.2 Phishing

Phishing je jedním z hlavních a nejběžnějších typů kybernetických útoků. Jeho počátky sahají do 90. let, kdy internet zažíval rychlý růst. Z kriminologického hlediska lze phishing definovat jako specifickou formu počítačového podvodu založenou na vytváření věrohodné iluze legitimní komunikace, která vede k neuvědomělému vydání citlivých údajů (Kolouch, 2017). Cílí na citlivé údaje a nejtypičtější techniky zahrnují napodobené weby služeb, bankovnictví a sociálních sítí (Lenaerts-Bergmans, 2024).

1.2.1 Psychologie útoků

Pokud se analyzují příčiny úspěšnosti phishingových útoků, vyplývá, že rozhodující faktor obvykle nespočívá v technické složitosti. Úspěch vychází především ze schopnosti útočníků porozumět lidské psychologii a cíleně ji využít v praxi. Podvodníci cíleně využívají psychologické slabiny a emoce a vedou oběť k jednání, k němuž by za běžných okolností nepřistoupila. Nejde o náhodu, ale o promyšlený postup založený na rutinním chování a zranitelnostech.

Roli zde hraje i zneužití tzv. zachycení rutinou, kdy uživatel v časovém tlaku automaticky vykoná nebezpečnou akci, protože se vizuálně shoduje s jeho běžným pracovním úkonem, přičemž tyto bezpečnostní ohledy často ustupují snaze o zachování pracovní efektivity (Anderson, 2020).

Přehled základních psychologických taktik:

Naléhavost a role

Útočníci vytvářejí zprávy vyvolávající naléhavost nebo působící jako vysoce relevantní pro pracovní roli příjemce či jeho aktuální povinnosti, například ve formě podvržených faktur vyžadujících okamžitou pozornost. Využívají lidskou tendenci upřednostňovat naléhavé záležitosti a jednat impulzivně bez důkladné kontroly (NCSC, 2024).

Přetížení a rutina

V prostředí, kde uživatelé denně zpracovávají velké množství digitální komunikace, je nereálné očekávat, že budou každou zprávu podrobně analyzovat, zvláště při časovém tlaku a souběžném řešení dalších úkolů. Práce s e-maily a klikání na odkazy jsou nedílnou součástí mnoha pracovních postupů, čímž ztěžuje neustálou identifikaci potenciálně škodlivého obsahu (NCSC, 2024).

Tlak a rozptýlení

Jedinci jsou náchylnější k phishingovým útokům, když jsou pod tlakem, rozptýlení nebo přepracovaní. Obviňování uživatelů z kliknutí na škodlivé odkazy je neúčinné, protože jejich chování ovlivňuje široká škála faktorů, včetně osobnostních rysů a situace (NCSC, 2024).

Falešná důvěryhodnost

Útočníci používají dostupné informace o organizaci nebo jejích zaměstnancích, aby jejich phishingové zprávy působily důvěryhodněji a realističtěji, což je typické pro tzv. spear phishing. Dobře napsané e-maily s bezchybnou gramatikou navíc snižují podezření (NCSC, 2024).

Strach z postihu

Phishingové simulace spojené s trestáním chyb mohou narušit důvěru mezi zaměstnanci a bezpečnostními týmy. Zaměstnanci, kteří se obávají negativních následků, jsou méně ochotní hlásit podezřelé incidenty, čímž oslabují systémy včasného varování. Pro účinnou obranu je klíčové podporovat pozitivní kulturu kybernetické bezpečnosti, která motivuje k hlášení bez hledání viníka (NCSC, 2024).

Budoucí útoky pravděpodobně posílí důraz na pokročilé formy sociálního inženýrství s intenzivnějším využitím psychologických mechanismů. Rychlý rozvoj generativní umělé inteligence a technologií deepfake zvyšuje schopnost vytvářet velmi realistické a přesvědčivé podvody. Možnosti umožňují omezit typické nedostatky starších kampaní a připravovat zprávy téměř nerozeznatelné od legitimní komunikace, včetně syntetických videí a hlasových záznamů. Je zřejmé, že trend již není jen vizí, ale stává se realitou, což představuje velkou výzvu pro tradiční metody detekce a zvyšuje potřebu digitální gramotnosti mezi uživateli. V tomto měnícím se prostředí se umělá inteligence stává klíčovým hráčem, a to nejen jako nástroj pro vytváření útoků, ale paradoxně jako nezbytná součást jejich detekce a prevence (Shloman, 2024).

1.3 Významné phishingové útoky

Následující část shrnuje vybrané phishingové incidenty s významným dopadem na vývoj sociálního inženýrství i obranných postupů. Příklady jsou seřazeny chronologicky a ilustrují posun k propracovanějším postupům i rozšíření útoků do dalších komunikačních kanálů.

1.3.1 AOL / AOHell 1995

Popisovaný incident představuje významný milník v dějinách kyberkriminality. Položil základy moderních phishingových technik a přispěl k rozšířenému užívání pojmu „phishing“. Hlavním cílem útočníků bylo přimět uživatele služby AOL, aby prozradili své přihlašovací údaje a informace o kreditních kartách. Za účelem získání důvěry vytvářeli falešné účty a identity, často s využitím automatizovaných nástrojů, jako je AOHell, a vydávali se za pracovníky podpory AOL. Následně rozesílali klamavé zprávy zaměřené především na nové a méně zkušené uživatele v chatovacích místnostech. Jakmile oběť odpověděla a poskytla své přihlašovací údaje, útočníci získali neoprávněný přístup k jejímu účtu. To, co začalo jako snaha teenagerů získat bezplatný přístup ke službě, se rychle vyvinulo v jednu z nejvýznamnějších hrozeb pro počítačovou bezpečnost (Rekouche, 2011, s. 1).

1.3.2 RSA 2011

V roce 2011 se společnost RSA stala terčem vysoce cíleného spear-phishingu. Útok odstartoval škodlivý soubor ve formátu Excel, využívající tehdy neznámou zranitelnost spojenou s Adobe Flash. Operace bývá připisována čínským zpravodajským strukturám, často ve spojení se skupinou APT1 napojenou na Čínskou lidovou osvobozeneckou armádu.

Po otevření souboru se útočníkům podařilo nainstalovat malware Poison Ivy a získat vzdálený přístup do sítě. Následně probíhal systematický pohyb v interní síti, shromažďování přihlašovacích údajů a snaha získat tajné klíče nezbytné pro fungování bezpečnostních tokenů SecurID. Přes zdánlivou izolaci se jim podařilo kritické autentizační údaje odčerpat. Krádež vedla k vážným následkům, včetně kompromitace obranných dodavatelů, a RSA musela přijmout rozsáhlá nápravná opatření.

Incident je dnes uváděn jako jeden z prvních rozsáhlých útoků na dodavatelský řetězec a významně ovlivnil vnímání digitální bezpečnosti (Greenberg, 2021).

1.3.3 Google Docs – „OAuth worm“ 2017

Roku 2017 byl zaznamenán phishingový útok vystupující jako pozvánka ke sdílení dokumentu v Google Docs. Získání přístupů probíhalo přes zneužití OAuth, následně došlo k udělení oprávnění pro Gmail a Disk Google. Po schválení uživatelem falešná aplikace okamžitě stáhla kontakty a automaticky se šířila dál. Incident byl spojován s kampaní Pawn Storm a aktivitami ruských zpravodajských služeb. Uživatelé mohli útok rozpoznat podle podezřelých domén, na což Google rychle reagoval zablokováním škodlivých stránek a odebráním přístupů. Incident zdůrazňuje kritickou nutnost opatrnosti při udělování oprávnění neznámým aplikacím a důkladné kontroly jejich požadavků (Gallagher, 2017).

1.3.4 Mall.cz 2017

V roce 2017 vyšlo najevo, že Mall.cz utrpěl rozsáhlý únik dat, jehož kořeny sahaly do roku 2015, kdy se na platformě Ulož.to objevil soubor s citlivými uživatelskými údaji. Primární příčinou této bezpečnostní slabiny bylo přetrvávající používání zastaralých hashovacích algoritmů, jako je MD5. Uniklá databáze obsahovala více než 735 000 e-mailových adres a 766 000 hesel, z nichž značná část byla buď v prostém textu, nebo snadno prolomitelná. Zranitelnost byla názorně demonstrována, když autor analýzy dokázal s využitím moderních GPU technik dešifrovat desítky tisíc hesel v krátkém čase.

Mall.cz na situaci reagoval resetováním hesel pro postižené účty a zajištěním odstranění souboru z Ulož.to. Incident slouží jako důrazné připomenutí, že uživatelé by měli používat silná a unikátní hesla a poskytovatelé služeb musí implementovat robustní hashovací algoritmy pro ochranu dat (Špaček, 2018).

1.3.5 Dropbox 2022

V říjnu 2022 čelila společnost Dropbox sofistikovanému phishingovému útoku. Útočníci, kteří se vydávali za platformu CircleCI, nástroj pro automatizaci vývoje softwaru, použili falešné webové stránky, aby vylákali od vybraných zaměstnanců jejich přihlašovací údaje ke GitHubu, včetně

jednorázových ověřovacích kódů. To útočníkům umožnilo získat přístup k přibližně 130 interním úložištím obsahujícím prototypy kódu a bezpečnostní nástroje. Incident nezasáhl uživatelské účty, hesla ani platební informace, nicméně byl zaznamenán únik API klíčů u vybraných vývojářů a malého množství osobních údajů. Společnost zabránila dalšímu přístupu a přizvala externí forenzní experty (Dropbox Security Team, 2022).

1.3.6 Quishing 2.0 2024–2025

Útočníci vkládali škodlivé URL do QR kódů v phishingových dokumentech, čímž dosáhli nové úrovně sofistikovanosti a obcházeli vizuální kontrolu cílové adresy na mobilních zařízeních. K maskování skutečného cíle zneužívali mechanismy URL přesměrování, často využívající otevřená přesměrování na legitimních webech, aby oběti nenápadně navedli na phishingové stránky a zamaskovali infrastrukturu útoku.

Pro zvýšení věrohodnosti a obcházení detekce integrovali do přesměrování kroky lidského ověření, například pomocí Cloudflare Turnstile. Konečným cílem promyšlených kampaní bývá získání citlivých přihlašovacích údajů prostřednictvím věrohodných, často personalizovaných podvržených přihlašovacích stránek napodobujících známé služby (Huang a Thothathri, 2025).

1.4 Osobnosti sociálního inženýrství

Rozvoj sociálního inženýrství výrazně ovlivnily osobnosti, jejichž zkušenosti a teoretické koncepty pomohly vysvětlit, jak a proč selhává lidský faktor. Podkapitola představuje klíčové postavy stojící u vzniku manipulačních praktik, popisu zneužívaných kognitivních mechanismů a převodu poznatků do školení, detekčních postupů a organizačních politik. Zvláštní pozornost je věnována principům přenositelným do praxe detekce a prevence phishingu, aby bylo možné v následujících částech formulovat doporučení ke zvýšení odolnosti jednotlivců i organizací v souladu s cíli práce.

1.4.1 Kevin Mitnick

Mitnick je často popisován jako známý hacker a výrazná osobnost sociálního inženýrství; zneužíval lidskou důvěru i slabiny systémů převážně ze zvědavosti. Po odpykání trestu se prosadil jako odborník na kybernetickou bezpečnost a věnoval se osvětě v oblasti obrany proti manipulativním technikám a útokům zaměřeným na lidský faktor (Mitnick a Simon, 2002).

1.4.2 Christopher Hadnagy

Známý pod přezdívkou „Chief Human Hacker“, je uznávanou autoritou v oblasti sociálního inženýrství. Je tvůrcem strukturované metodiky pro tuto disciplínu, formuloval její etické zásady a je autorem mnoha publikací. Pro korporace realizuje simulované phishingové útoky a penetrační testy s cílem posílit jejich kybernetickou obranu, přestože se sám paradoxně stal obětí sofistikovaného podvodného e-mailu. Mimo to založil neziskovou organizaci The Innocent Lives Foundation, která s využitím OSINT technik usiluje o odhalování a prevenci trestné činnosti zaměřené na děti (Darknet Diaries, 2020).

1.4.3 Rachel Tobac

Etická hackerka a přední expertka na sociální inženýrství, která odhaluje zranitelnosti firem mistrnou manipulací lidské psychiky. Využívá pokročilé techniky, včetně spoofingu a AI klonování hlasu, k získávání citlivých informací a demonstraci bezpečnostních slabin. Jako zakladatelka SocialProof Security pomáhá společnostem zlepšovat jejich obranu a prosazuje silné ověřovací protokoly (Rhysider, 2024).

1.4.4 Jenny Radcliffe

Sociální inženýrka a fyzická penetrační testerka, jejíž dovednosti se vyvinuly od dětských průzkumů až po získávání citlivých dat a simulované bankovní průniky. Její metoda spočívá v ovládání lidské psychiky a odhalování slabin v chování, nikoli v technickém hackingu. Dokazuje, že sociální inženýrství je mocným nástrojem v bezpečnosti a vyjednávání, často efektivnějším než technická ochrana (Rhysider, 2021).

1.4.5 Devin Olaf

Specializuje se na testování fyzické bezpečnosti objektů, kdy simuluje vloupání, aby odhalil jejich zranitelnosti. K dosažení cílů využívá širokou škálu metod včetně sociálního inženýrství, což pomáhá překonávat technické i lidské bezpečnostní bariéry. Jeho práce má význam pro organizace usilující o posílení ochrany proti reálným hrozbám (Rhysider, 2023).

2 Typy phishingu

Phishing se neustále přizpůsobuje novým komunikačním prostředkům a zdokonaluje své metody s cílem zvýšit úspěšnost útočných akcí (PROOFPOINT, nedatováno).

Kapitola se systematicky zabývá klasifikací a analýzou hlavních typů phishingových útoků. Účelem kapitoly je poskytnout ucelený přehled o širokém spektru hrozeb. Každý typ bude popsán z hlediska specifických znaků, používaných postupů, cílových skupin a možných dopadů. Současně bude ukázáno uplatnění principů sociálního inženýrství v různých phishingových scénářích. Rozvoj strategií proti dynamicky se proměňujícím kybernetickým hrozbám vyžaduje důkladná znalost odlišností.

Obr. 1: Jak vypadá phishingový útok
Zdroj: BOWCUT (2025)

2.1 E-mail phishing

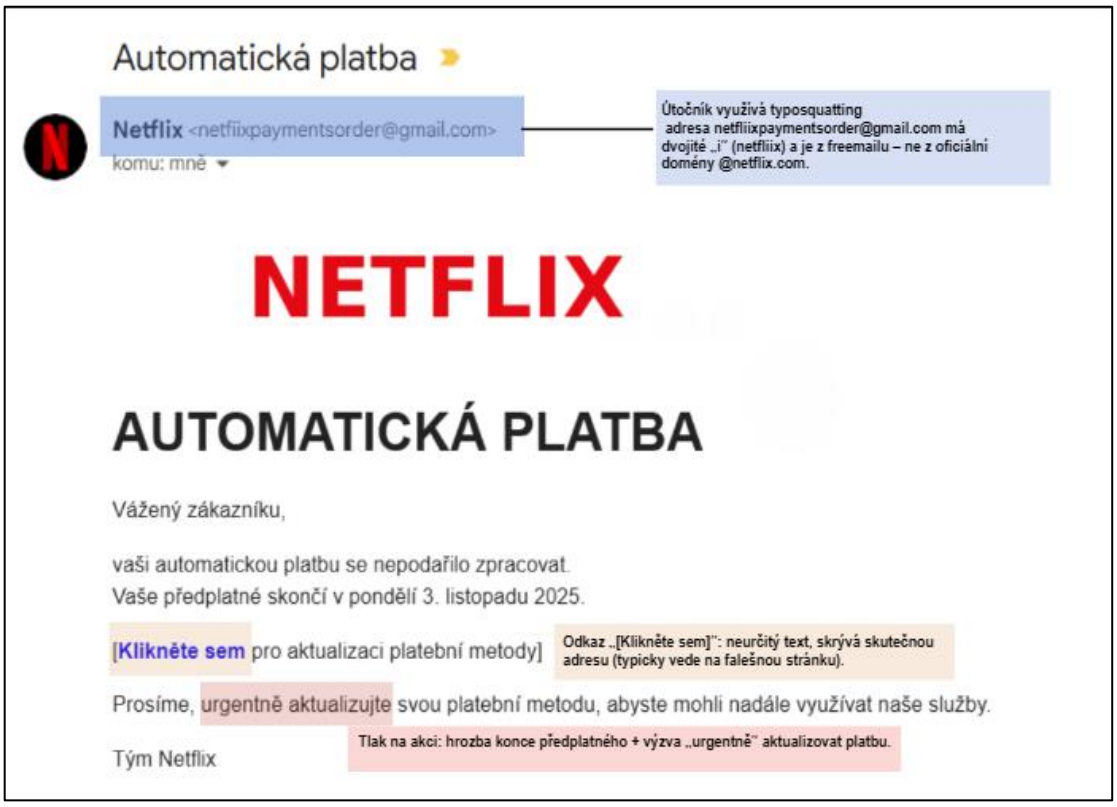
Phishing představuje formu podvodu, při němž útočníci zneužívají sociální inženýrství, aby vylákali od obětí důvěrné údaje, jako jsou přihlašovací hesla nebo detaily platebních karet. Pachatelé se vydávají za legitimní organizace a vytvářejí podvržené zprávy či webové stránky s cílem působit důvěryhodně a přimět uživatele k neuváženým krokům. Získané informace poté zneužívají k neoprávněnému přístupu k účtům nebo je prodávají na nelegálních trzích.

Jednou z nejčastějších forem je e-mailový phishing. Útočníci rozesílají zprávy napodobující oficiální komunikaci, upravují adresy odesílatele pro zvýšení věrohodnosti a připravují podvržené webové stránky s vizuální podobností legitimním službám. Cílem stránek je získat přihlašovací údaje uživatelů. Kromě toho mohou podvodné e-maily obsahovat i škodlivé soubory, jejichž otevření může vést k infikování zařízení malwarem (ESET, 2016).

Základem phishingových kampaní není obvykle zneužití technických chyb, nýbrž psychologická manipulace a sociální inženýrství. Agresoři často hrají na emoce, vytvářejí dojem naléhavosti nebo hrozby, aby přiměli oběti k impulzivnímu jednání (ESET, 2016).

Ačkoliv antivirové a antispamové programy nabízejí určitou úroveň zabezpečení, nejsou schopny zcela eliminovat phishingové hrozby. Z toho důvodu je při komunikaci prostřednictvím e-mailu klíčová maximální obezřetnost:

Před kliknutím na jakýkoli odkaz nebo otevřením přílohy z podezřelé zprávy je nezbytné důkladně prověřit odesílatele a legitimitu webové adresy (ESET, 2016).



Obr. 2: Pokus o e-mailový phishing

Zdroj: Vlastní zpracování (2025)

Pokud máte jakékoli pochybnosti, je nejbezpečnější ověřit si danou informaci nezávisle, například přímým telefonickým kontaktem s příslušnou institucí (ESET, 2016).

2.2 Spear phishing

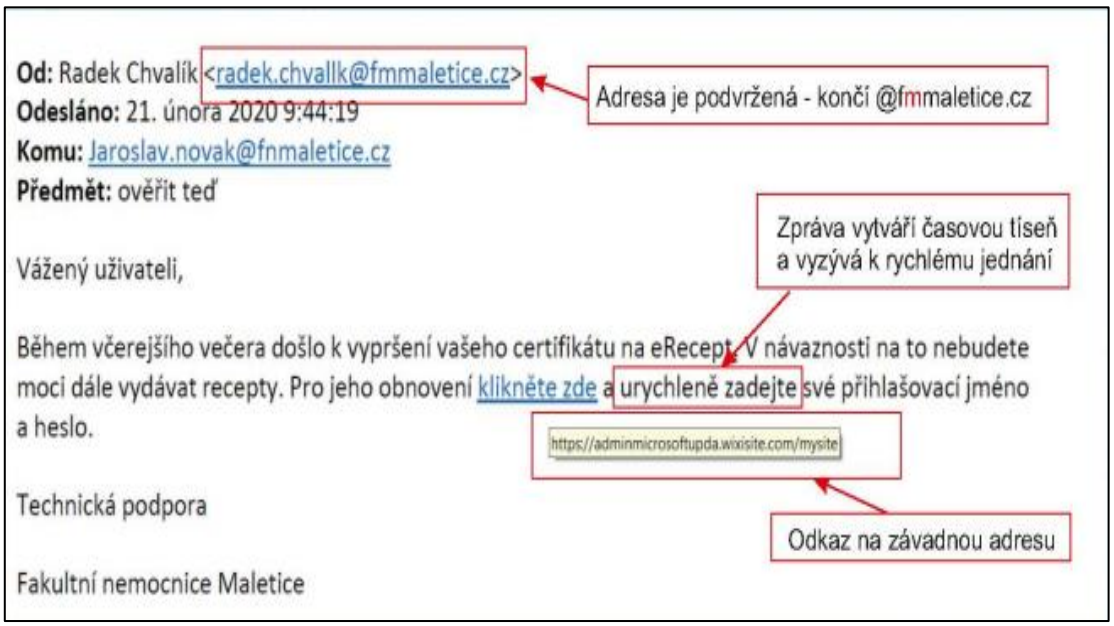
Hlavním cílem útočníků je neoprávněné získání citlivých dat, přístupových údajů či finančního zisku. Rozpoznání útoků je značně obtížné, neboť zprávy jsou pečlivě personalizované a často využívají veřejně dostupné informace o oběti, což výrazně zvyšuje jejich důvěryhodnost.

Útočníci typicky zahajují své operace důkladným sběrem informací, prohledáváním sociálních sítí a dalších veřejných zdrojů, aby si vytvořili detailní profil své oběti (Kosinski, 2024).

Získané informace slouží útočníkům k tvorbě vysoce personalizovaných zpráv napodobujících legitimní komunikaci od důvěryhodného odesílatele, například kolegy nebo nadřízeného (Kosinski, 2024).

V praxi se často uplatňuje kompromitace e-mailových účtů nebo použití adres s minimální odchylkou od originálu (Kosinski, 2024).

Spear phishing primárně zneužívá lidskou psychologii a firemní postupy, čímž se řadí mezi techniky sociálního inženýrství. Útočníci se snaží manipulovat oběťmi prostřednictvím psychologického nátlaku, například vyvoláním pocitu naléhavosti nebo apelováním na silné emoce (Kosinski, 2024).



Obr. 3: Odkaz na závadnou adresu
Zdroj: NÚKIB (2020)

2.3 Whaling

Whaling představuje specifickou formu kybernetického podvodu, často označovanou jako „CEO fraud“, se zaměřením na nejvyšší vedení a strategicky významné zaměstnance organizací.

Pachatelé se při něm zosobňují jako generální ředitel nebo jiná vlivná osoba a s využitím naléhavých požadavků se snaží získat finanční prostředky či důvěrné informace. K provedení útoku často slouží buď kompromitovaný firemní e-mailový účet, nebo nově registrovaná doména, která je vizuálně téměř identická s tou legitimní. Ze zdrojů poté odesílají požadavky na změnu bankovních údajů, schválení finančních transakcí nebo sdílení interních dat (CISCO, nedatováno).

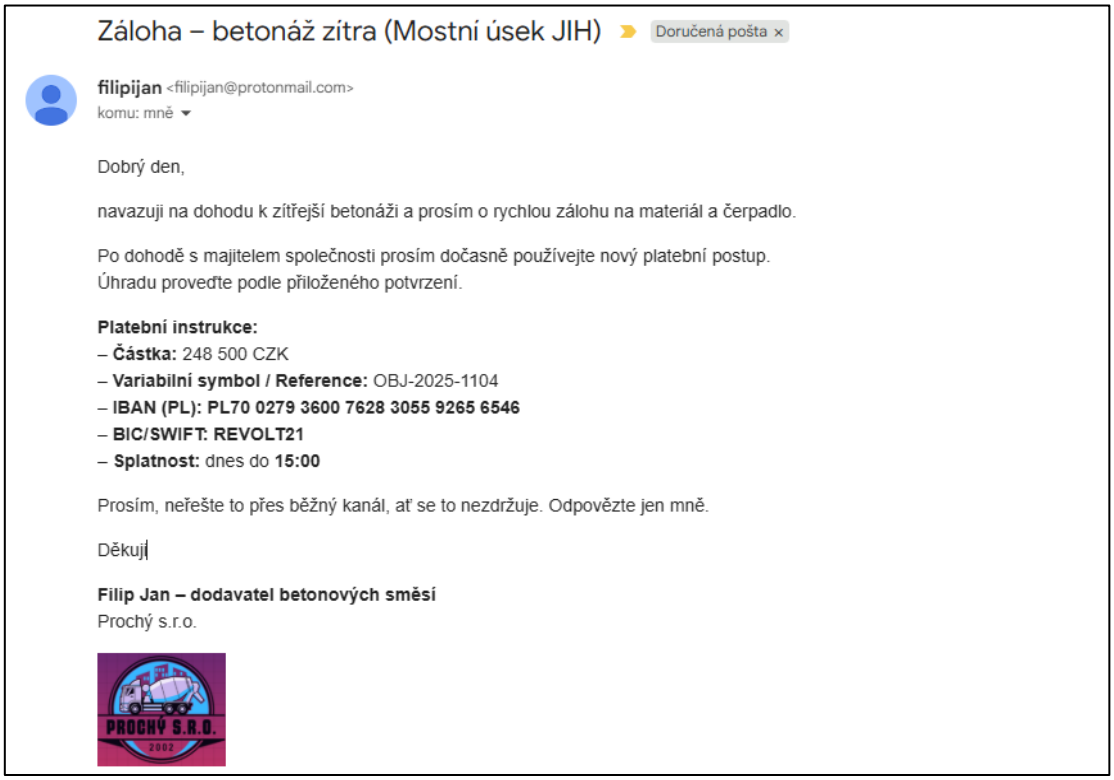
Efektivní ochrana spočívá v zavedení přísných interních procesů a kontrolních mechanismů, jako je povinnost dvojího schválení pro všechny platby a důkladné ověřování veškerých změn prostřednictvím nezávislých a bezpečných komunikačních kanálů, například telefonického hovoru nebo interního firemního systému (CISCO, nedatováno).

2.4 BEC (Business Email Compromise)

BEC primárně cílí na lidské rozhodování, nikoli na technologické zranitelnosti, s cílem přimět jednotlivce k provedení neautorizovaných plateb nebo sdílení citlivých dat.

Útoky se vyznačují vysokou mírou legitimity, často imitují reálné konverzace v rámci stávajících e-mailových vláken, a využívají věrohodné podpisy a tón, čímž se odlišují od běžného spamu (ESET, 2023).

Základní taktikou je zneužití identity nebo domény, ať už prostřednictvím kompromitovaného účtu, podobně vypadající domény, nebo podvržené adresy. Motivace je typicky finanční, doprovázená tlakem na čas, například formou urgentních žádostí o změnu bankovních údajů nebo okamžitých plateb (ESET, 2023).

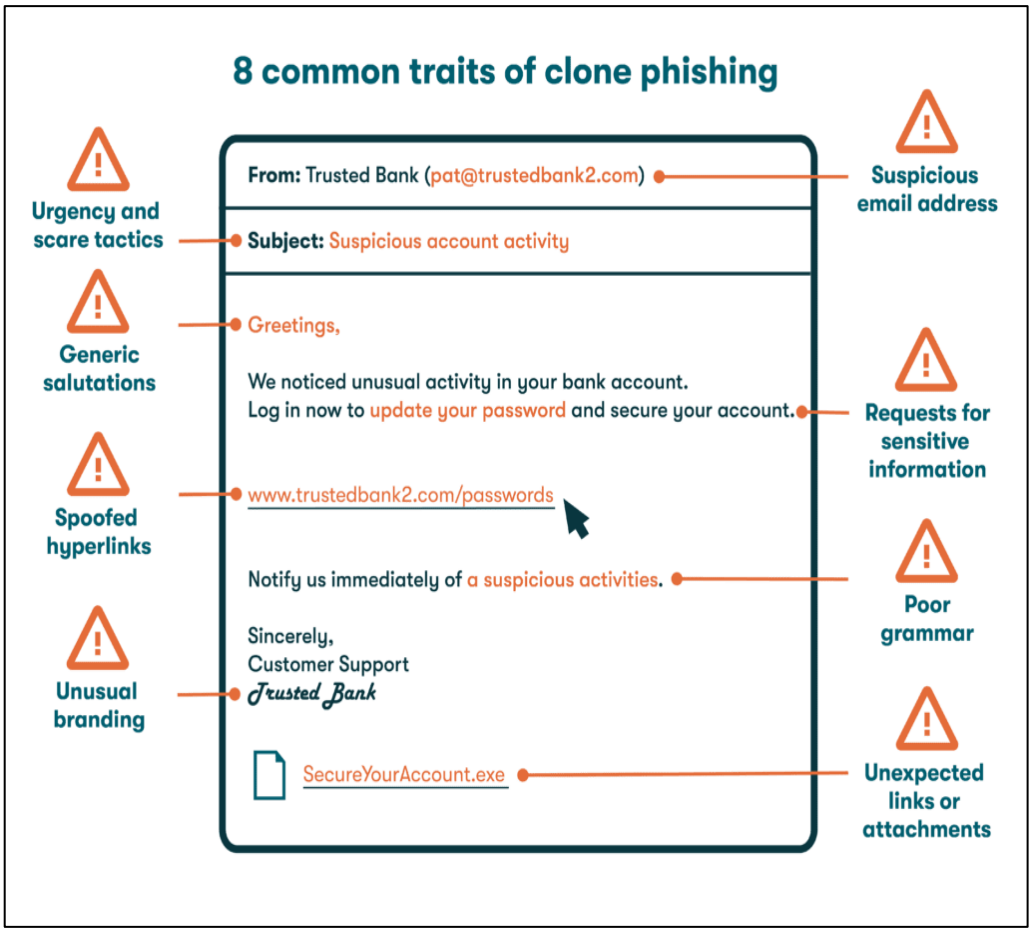


Obr. 4: Pokus o provedení platby
Zdroj: Vlastní zpracování (2025)

Popsaný incident představuje případ podvodného vylákání finančních prostředků prostřednictvím vydávání se za dodavatele v e-mailové komunikaci. Klíčovým prvkem bylo uplatnění časového nátlaku, vyjádřené urgentním požadavkem na zálohovou platbu s přesně stanoveným termínem („dnes do 15:00“). Současně byla požadována změna platebních instrukcí na nově uvedený zahraniční účet (PL IBAN u fintech instituce) a docházelo ke snaze obejít interní schvalovací procesy výzvou ke komunikaci mimo standardní firemní kanály.

2.5 Clone phishing

Clone phishing se od běžných phishingových útoků liší zneužitím důvěryhodnosti již proběhlé a legitimní e-mailové komunikace. Pachatelé zkopírují dříve odeslaný e-mail a upraví ho, aby obsahoval škodlivé odkazy nebo přílohy, čímž vytvářejí iluzi pokračování důvěryhodné konverzace (Kaspersky, 2025).



Obr. 5: 8 cest ke clone phishingu

Zdroj: DASHLANE (2025)

Hlavní cíle:

- Získání citlivých dat (např. osobní údaje, bankovní informace).
- Získání přístupových údajů (např. hesla k účtům).
- Přímý finanční zisk. (Kaspersky, 2025)

2.6 Smishing

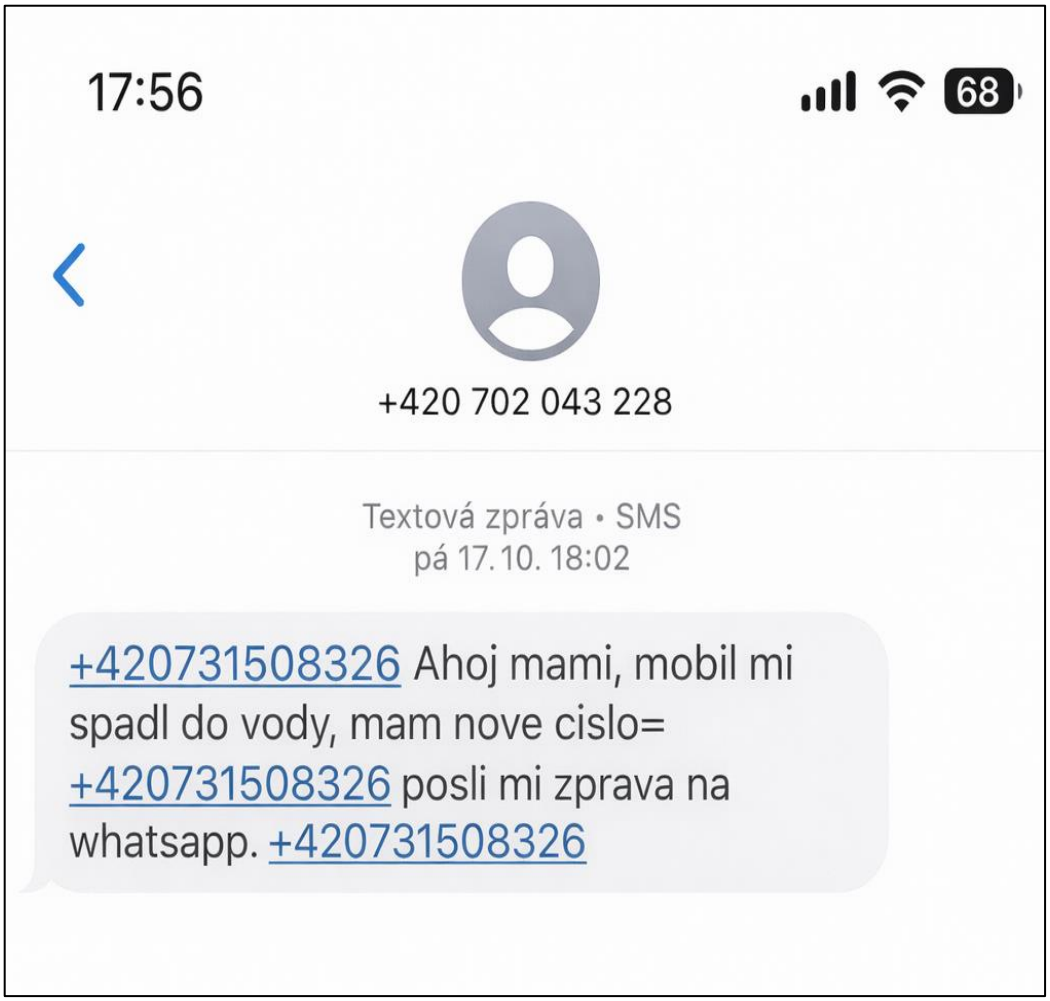
Smishing neboli SMS phishing představuje útok využívající důvěryhodnosti textových zpráv k oklamání uživatelů. Primárním cílem je získat citlivé údaje, například přihlašovací údaje pro bankovní účty, platební informace či autentizační kódy, případně přimět oběti k neoprávněným finančním transakcím. Útok je obzvláště účinný díky stručnému formátu SMS a často uměle vyvolané naléhavosti, čímž ztěžuje rychlé rozpoznání podvodu a nutí uživatele k unáhleným reakcím (Malkusová, 2025).

Kombinuje technické prostředky se sociálním inženýrstvím. Útočníci falšují identitu odesílatele (např. banky nebo doručovací služby) a rozesílají zprávy s maskovanými odkazy směřujícími na podvržené webové stránky s vizuální podobností legitimním portálům. Často se objevují výzvy k zadání jednorázových hesel nebo přesměrování na falešné platební formuláře (Malkusová, 2025).

Útoky mohou zahrnovat i přílohy s malwarem nebo kombinaci SMS s telefonátem či e-mailem pro zvýšení věrohodnosti. Využívají psychologii oběti, hrají na strach, zvědavost nebo touhu po výhodě. Existují i cílené varianty, jako je spear smishing (Malkusová, 2025).

Podle společnosti Kaspersky (2021) lze smishing identifikovat pomocí těchto znaků:

- **Nevyžádané zprávy:** Přicházejí od zdánlivě důvěryhodných institucí (banka, pošta, úřad), ale vy jste je neočekávali.
- **Naléhavost a nátlak:** Zpráva vás nutí k rychlé akci (např. „balíček nelze doručit“, „časově omezená nabídka“).
- **Žádost o citlivé údaje:** Chtějí po vás hesla, čísla karet, rodné číslo nebo jiné osobní informace.
- **Podezřelé odkazy:** Zpráva obsahuje odkaz směřující na falešnou webovou stránku.
- **Sliby zdarma:** Nabízejí výhry, dárky nebo jiné „výhodné“ nabídky.
- **Neobvyklá čísla:** Zpráva přichází z podivného, cizího nebo krátkého telefonního čísla.



Obr. 6: Smishing a jeho podoba
Zdroj: Vlastní zpracování (2025)

Jak se bránit proti smishingu a co dělat v případě útoku:

- **Nereagujte a ověřujte:** Na podezřelé zprávy neklikejte ani neodpovídejte. Pravost vždy ověřte oficiálními kanály.
- **Zabezpečte se:** Používejte vícefaktorové ověřování (MFA) a neukládejte citlivé údaje (např. čísla karet) v telefonu.
- **Jednejte okamžitě:** Nechte zablokovat kartu/platby a kontaktujte banku; podle situace kontaktujte Policii ČR. Změňte související hesla.
- **Sledujte finance:** Pravidelně kontrolujte své účty kvůli neoprávněné aktivitě. (Kaspersky, 2021).

2.7 Vishing

U tohoto typu phishingu podvodníci volají z telefonních čísel, vydávají se za pracovníky bank, policie či úřadů a během hovoru vytvářejí tlak a dojem, že je nutné jednat okamžitě. U sofistikovanějších útoků už dokážou za pomoci umělé inteligence napodobit konkrétní hlasy a tváře, což je obzvlášť nebezpečné pro různé instituce. Pro vlastní ochranu je vhodné číslo ověřit vyhledáním na internetu, případně na webu www.vyhledatcislo.cz, a zkontrolovat, zda odpovídá onomu subjektu (ESET, 2025).

Hlavní znaky:

- **Neobvyklé číslo:** Často zfalšované nebo podezřele krátké.
- **Nejasná identita:** Volající se vyhýbá konkrétnímu představení nebo instituci.
- **Tlak a hrozby:** Vyvíjení psychologického nátlaku.
- **Žádost o důvěrné údaje:** Požadavek na hesla, PIN, kompletní čísla karet, CVC/CVV nebo ověřovací SMS kódy.
- **Typické formulace:** Např. „Volám z vaší banky kvůli ověření účtu“, „Potřebuji ověřit vaši identitu kódem z SMS“ (ESET, 2025).

2.8 Quishing (QR phishing)

Quishing představuje formu phishingu, která zneužívá QR kódy. Jeho účinnost spočívá ve vnímání QR kódů uživateli jako rychlého a spolehlivého nástroje. Útočníci vytvářejí podvržené webové stránky s vizuální i funkční podobností legitimním službám. K oklamání obětí často využívají domény s minimálními odchylkami od originálu, což ztěžuje včasné rozpoznání podvodu. Podvodné QR kódy se šíří digitálně, zejména prostřednictvím e-mailů a sociálních sítí, i fyzicky, například na plakátech, samolepkách nebo formou přelepů přes původní důvěryhodné kódy (Kaspersky, 2025).

Jakmile uživatel naskenuje kód, je obvykle přesměrován na škodlivý web. Cílem je buď vylákat citlivé osobní či platební údaje, nebo v horším případě nainstalovat malware do mobilního zařízení (Kaspersky, 2025).

Mezi typické podvodné scénáře patří imitace platebních bran, lákání na fiktivní slevové akce nebo zneužití QR kódů na veřejných zařízeních, jako jsou parkovací automaty, s cílem získat důvěrné informace (Kaspersky, 2025).

Obr. 7: Obezřetnost u QR skenování

Zdroj: SOSAFE (nedatováno)

Jak se bránit proti Quishingu:

- Ověřte zdroj QR kódu.
- Buďte skeptičtí k nevyžádaným kódům.
- Kontrolujte pravopis a gramatiku.
- Prozkoumejte cílovou URL.
- Zkontrolujte vzhled vstupní stránky.
- Hledejte HTTPS.
- Používejte dvoufaktorové ověřování (2FA).
- Nahlaste podezřelou aktivitu (Kaspersky, 2025).

3 Techniky a obrana

Kapitola se zabývá analýzou technik manipulace URL adres a doménových jmen používaných při phishingových útocích. Úvod představuje základní principy, následně navazuje podrobnější popis vybraných manipulačních metod. Mezi probírané postupy patří typosquatting, target embedding, URL padding, combosquatting a Unicode homografové útoky.

Na základě rozboru uvedených postupů se kapitola dále zaměřuje na možnosti detekce a obrany. Závěr shrnuje požadavky na navrhované řešení vyplývající z identifikovaných hrozeb a vytváří východisko pro praktickou část práce.

3.1 Doménové manipulační techniky

Doménové manipulační techniky představují podskupinu útoků zaměřených na klamání uživatelů prostřednictvím úprav struktury URL adres a doménových jmen. Nevyužívají technické zranitelnosti informačních systémů, ale lidský faktor, především nepozornost a důvěru ve zdánlivě legitimní vzhled webových stránek.

3.1.1 Typosquatting

Doménová manipulační technika, při níž útočníci registrují domény s drobnými překlepy oproti legitimním webovým adresám. Útočníci zneužívají nepozornost při zadávání URL a přesměrovávají uživatele na podvodné stránky napodobující důvěryhodné služby (Amal et al., 2022).

3.1.2 Target Embedding (vložení cílové domény)

Útočník vloží název známé a důvěryhodné domény do adresy vlastní webové stránky, nejčastěji jako subdoménu. Útočník spoléhá na to, že uživatel při pohledu na URL rozpozná známý název a nebude dále zkoumat, komu doména ve skutečnosti patří (Amal et al., 2022).

Při čtení URL adresy je však důležité všímat si části bezprostředně před doménou nejvyšší úrovně (TLD), která určuje skutečného vlastníka domény. V případě této techniky patří celá adresa útočníkovi a známý název se v ní objevuje pouze jako klamavý prvek (Amal et al., 2022).

3.1.3 URL Padding (prodloužení URL adresy)

Nejčastěji se používá v kombinaci s metodami, jako je target embedding nebo combosquatting. Cílem je vytvořit velmi dlouhou URL adresu, u níž je omezením prostoru obrazovky viditelná pouze její zavádějící část, obvykle obsahující název legitimní domény. Útočník může skrýt skutečnou doménu, kterou ovládá, a vyvolat u uživatele mylný dojem, že se nachází na důvěryhodném webu (Amal et al., 2022).

3.1.4 Combosquatting

Při combosquattingu útočníci registrují domény obsahující celý název známé služby doplněný o další slova nebo znaky. Oproti technice target embedding se název legitimní služby nenachází v subdoméně, ale tvoří přímou součást registrované domény (Amal et al., 2022).

Adresa může u uživatele vyvolat dojem legitimního původu, přestože doména není s danou službou nijak spojena (Amal et al., 2022).

3.1.5 Unicode homografy (IDN Homografy)

Mezinárodní doménová jména (IDN) umožňují použití neanglických znaků, jako jsou znaky čínského, cyrilického nebo arabského písma, v názvech domén. Zneužití uvedené vlastnosti je typické pro Unicode homografové útoky, patřící mezi pokročilé techniky doménové manipulace. Útočník nahrazuje vybrané znaky v názvu domény jinými znaky z odlišných znakových sad Unicode, jež jsou pro lidské oko vizuálně téměř nerozeznatelné, avšak technicky se jedná o odlišné znaky (Amal et al., 2022).

V důsledku této záměny může doména na první pohled působit zcela legitimně, přestože ve skutečnosti odkazuje na podvodný web (Amal et al., 2022).

3.1.6 Zkracovače URL

Zkracovače URL umožňují převod libovolné webové adresy na výrazně kratší tvar.Mezi nejrozšířenější patří služby jako bit.ly nebo TinyURL. V rukou útočníka slouží jako poslední krok maskování, při němž se i velmi dlouhá podvodná adresa sestavená kombinací předchozích technik zkrátí na několik znaků. Uživatel tak před kliknutím nemá žádnou možnost zjistit, kam odkaz skutečně směřuje (Kaspersky, 2021).

Uplatnění nacházejí zkrácené odkazy zejména ve smishingových kampaních, kde krátký formát přirozeně odpovídá podobě SMS zpráv (Kaspersky, 2021).

3.2 Detekce a obrana

Detekce doménových manipulací je náročná zejména proto, že tyto techniky nespoléhají na technické chyby systémů, ale na letmé čtení adresy a důvěru uživatele v její vzhled. Obrana proto nestojí jen na technologiích, ale vyžaduje také pozornost samotného uživatele (Amal et al., 2022).

U zkrácených odkazů lze před kliknutím použít náhledové služby jako checkshorturl.com, které zobrazí původní adresu. Obecně platí, že při jakékoli pochybnosti je vhodné adresu ověřit nezávisle, například přímým přechodem na web dané organizace (Amal et al., 2022).

Řadu technik popsaných v předchozích podkapitolách lze identifikovat automatizovaně na základě analýzy struktury URL. Typosquatting odhalí porovnání domény se známými značkami pomocí výpočtu editační vzdálenosti a parametry URL obsahující vnořené adresy naznačují zneužití přesměrování. Přítomnost Punycode v názvu domény signalizuje možný IDN homografový útok (Amal et al., 2022).

Podezření může vzbudit také neobvykle dlouhá adresa nebo nadměrný počet subdomén. Uvedené přístupy tvoří základ detekčních pravidel prohlížečového rozšíření popsaného v kapitole 4.

3.3 NIS2 a povinnosti v oblasti ochrany před phishingem

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze 14. prosince 2022, známá pod zkratkou NIS2, představuje náhradu za starší směrnici NIS z roku 2016. Nová regulace vznikla jako reakce na rozdílné uplatňování původních pravidel v rámci EU, což vedlo k nejednotnému přístupu ke kybernetické obraně. Účelem NIS2 je sjednotit základní bezpečnostní standardy, podpořit odolnost kritické infrastruktury a lépe se bránit stále častějším kybernetickým incidentům s mezinárodním dosahem (Evropský parlament a rada, 2022).

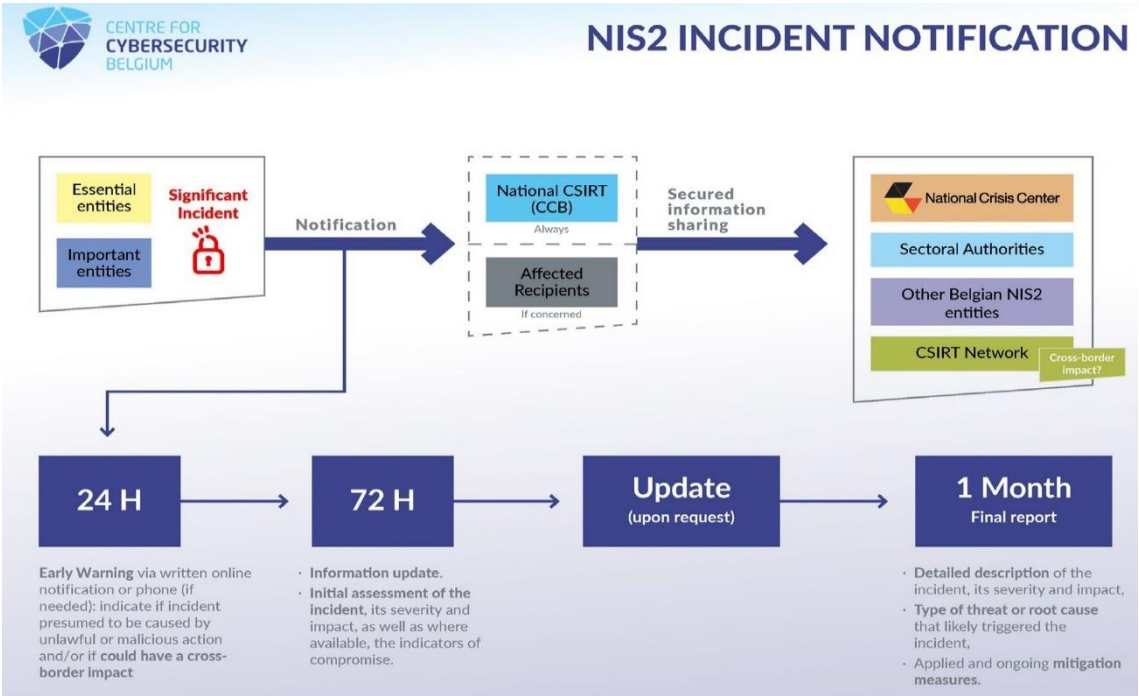
Požadavky na řízení kybernetických rizik stanovuje článek 21, který regulovaným subjektům ukládá řadu technických a organizačních opatření. Z pohledu obrany proti phishingu a sociálnímu inženýrství jsou klíčové zejména vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti, nasazení vícefaktorové autentizace, ochrana firemních komunikačních kanálů včetně hlasu, videa i textu, využití kryptografických nástrojů a jasně definovaná pravidla přístupu k informačním systémům (Evropský parlament a rada, 2022, čl. 21).

Na školení přitom nemají nárok pouze řadoví pracovníci, protože článek 20 rozšiřuje tuto povinnost i na osoby ve vedení regulovaných subjektů, které musí danými kurzy také projít. (Evropský parlament a rada, 2022, čl. 20).

Směrnice uvádí skutečnost, že třetí strany bývají často nejslabším článkem celého systému. Útočníci totiž cíleně vyhledávají zranitelnosti u partnerských organizací, aby je využili jako vstupní bod pro infiltraci do infrastruktury samotného primárního subjektu (Evropský parlament a rada, 2022, čl. 21, odst. 3).

3.3.1 Hlášení bezpečnostních incidentů

V případě incidentu jsou subjekty povinny dodržet vícestupňový proces hlášení směrem k národnímu týmu CSIRT nebo příslušnému orgánu.



Obr. 8: Proces hlášení incidentu

Zdroj: CENTRE FOR CYBERSECURITY BELGIUM (2024)

Proces zahrnuje:

- **Do 24 hodin:** odeslání včasného varování o výskytu incidentu.
- **Do 72 hodin:** předložení podrobnějšího hlášení, které aktualizuje dostupné informace a obsahuje úvodní posouzení závažnosti dopadů.
- **Informování zákazníků:** v případě, že incident může negativně ovlivnit poskytovanou službu, má organizace povinnost bezodkladně informovat své uživatele (Deloitte, 2024).

Za incident se považuje událost, která způsobí narušení provozu, finanční ztrátu nebo značnou materiální či nemateriální újmu jiným osobám a subjektům (Deloitte, 2024).

4 Prototyp prohlížečového rozšíření

Praktická část práce se zaměřuje na návrh a realizaci prototypu prohlížečového rozšíření, jehož úkolem je upozornit uživatele na potenciálně rizikové webové odkazy. Zvolená forma rozšíření umožňuje provádět kontrolu URL adres přímo v prostředí webového prohlížeče, tedy v místě, kde k interakci s odkazy nejčastěji dochází.

Prototyp byl navržen jako lehký doplňkový nástroj využívající omezený soubor detekčních pravidel odvozených z běžně používaných phishingových technik. Řešení se zaměřuje výhradně na analýzu struktury URL adres a neprovádí kontrolu obsahu webových stránek ani komunikaci s externími databázemi. Díky tomu zůstává chování rozšíření transparentní a snadno vysvětlitelné.

Hlavním cílem prototypu je demonstrovat propojení poznatků ze sociálního inženýrství s jednoduchým technickým opatřením podporujícím obezřetnější chování uživatelů při práci s webem. Prototyp slouží především k ověření zvoleného přístupu a k ilustraci jeho přínosů a omezení, nikoli jako plnohodnotná náhrada existujících bezpečnostních řešení.

Následující podkapitoly se věnují stanovení cílů a požadavků, návrhu detekčních pravidel, architektuře řešení, implementaci prototypu a vyhodnocení dosažených výsledků.

4.1 Cíl a požadavky

Cílem prototypu je vyhodnotit rizikovost webových odkazů z pohledu struktury URL a při detekci podezřelých znaků zobrazit uživateli varování, které podpoří obezřetné rozhodnutí před interakcí s odkazem.

Požadavky na prototyp:

Funkční požadavky:

- Analyzuje URL adresu při načtení webové stránky.
- Vyhodnocuje rizikové znaky pomocí jednoduchých detekčních pravidel.
- Při zvýšeném riziku zobrazí uživateli varování.

Nefunkční požadavky:

- Vyhodnocení probíhá lokálně bez odesílání dat mimo prohlížeč.
- Vyhodnocení je dostatečně rychlé, aby nezpomalovalo načítání stránky.
- Varování je zobrazováno jen při překročení prahu rizika a lze jej potlačit pro vybrané domény.

4.2 Pravidla a skórování

Vyhodnocení rizikovosti webových odkazů je v prototypu založeno na jednoduchých pravidlech. Rozšíření neřeší obsah stránky, ale zaměřuje se jen na to, jak URL vypadá a z jakých částí se skládá. U phishingu se totiž často opakují určité znaky, podle kterých se dá poznat, že odkaz může být podezřelý. Typicky se snaží skrýt skutečný cíl, obsahuje přesměrování přes parametr, nebo je zbytečně dlouhý a nepřehledný.

Každé pravidlo má přiřazenou váhu, protože ne všechny znaky jsou stejně závažné. Pokud URL splní pravidlo, přičte se jeho váha do výsledného skóre. Skóre tedy vzniká jako součet bodů za všechny detekované znaky. Čím více jich odkaz obsahuje nebo čím silnější jsou, tím vyšší skóre získá.

Nakonec se skóre porovná s prahovou hodnotou. Když ji odkaz překročí, rozšíření zobrazí varování. Výsledek hodnocení je dočasně uložen pro aktuální kartu, aby jej bylo možné zobrazit v uživatelském rozhraní rozšíření. Data jsou v tomto případě uchována pouze v rámci relace prohlížeče a nejsou odesílána mimo zařízení.

Každému z 29 definovaných pravidel (R1–R29) je přiřazena bodová váha odrážející závažnost daného znaku. Pokud URL adresa splní kritéria pravidla, body se přičtou do celkového skóre. Celková rizikovost odkazu je definována jako součet bodů za všechny detekované anomálie.

V aktuální verzi prototypu byla prahová hodnota pro aktivaci varování nastavena na 10 bodů. Tato hranice je záměrně nastavena přísněji než v počátečních fázích vývoje. Důvodem je snaha o maximální bezpečnostní ostražitost. Vzhledem k tomu, že většina pravidel má váhu 10 a více bodů, dojde k upozornění uživatele již při detekci jediného středně závažného rizikového faktoru (např. použití podezřelé doménové koncovky nebo výskytu phishingových termínů v cestě URL).

Tab. 1: Pravidla a skórování

ID	Název pravidla	Technická specifikace	Body
R1	IPv4 Host	Hostitel odpovídá formátu IP adresy (vynechání DNS).	20
R2	Punycode	Identifikace prefixu xn-- (homografické útoky).	25
R3	Znak @	Přítomnost znaku @ v URL (maskování cílové adresy).	20
R4	Subdomény	Detekce 4+ úrovní v doménové struktuře.	10
R5	Dlouhý Host	Samotný název webové stránky je delší než 40 znaků.	10
R6	Dlouhá URL	Celková délka řetězce URL ≥ 120 znaků.	5
R7	Počet parametrů	Výskyt 8+ unikátních parametrů v query.	10
R8	Redirect klíč	Přítomnost parametrů pro přesměrování (url, target aj.).	20
R9	Vnořená URL	Hodnota parametru obsahuje řetězec protokolu http.	30
R10	Kódování URL	Detekce hexadecimálních sekvencí (např. %3A%2F%2F).	15
R11	Dlouhý Token	Alfanumerická hodnota parametru ≥ 50 znaků.	10
R12	Zkracovač	Shoda hostitele se seznamem služeb (např. bit.ly).	15
R13	Sdílená cloud platforma	Hostování na free platformách (např. vercel.app).	15
R14	Entropie názvu	Nízký podíl samohlásek u domén ≥ 12 znaků.	15
R15	Cizí Brand	Zneužití známé značky na neoficiální doméně.	20
R16	Phishing slova	Současný výskyt ≥ 2 rizikových slov (login, verify).	15
R17	Riziková TLD	Použití koncovek s nízkou reputací (.xyz, .top).	10
R18	Nadměrné pomlčky	Výskyt 3 a více pomlček v názvu domény.	10
R19	Smíšená doména	Kombinace písmen a ≥ 3 číslic (u domén 8+ znaků).	10
R20	Akční slova	Výskyt phishingových termínů v cestě.	15
R21	Maskování koncovky	Imitace doménových koncovek uvnitř cesty.	15
R22	Citlivé termíny	Výskyt bank či gov u neoficiálních hostitelů.	15
R23	Kombinované riziko	Synergie rizikové TLD a podezřelého názvu cesty.	10
R24	Imitace značky	Souběžné zneužití značky a phishingových slov.	10
R25	Dlouhá doména + čísla	Kombinace dlouhého názvu domény a podezřelé koncentrace číslic.	10
R26	Unikátnost	Vysoký poměr unikátních znaků u domén délky 5–8.	10
R27	Náhodný řetězec	Segment cesty obsahuje alfanumerický kód (10+ znaků).	10
R28	Public složky	Využití adresářů jako /archive/ či /public/.	10
R29	Podezřelé ID	Klíče id či token s délkou hodnoty 10+ znaků.	10

Zdroj: Vlastní zpracování (2026)

Nízký práh nastavený na 10 bodů znamená, že konečné rozhodnutí zůstává na uživateli.

Rozšíření funguje jako pomocník, který upozorní na možné skryté hrozby, ale samotný uživatel se musí rozhodnout, jestli stránce bude věřit a jestli na ní bude pokračovat. Tento přístup zároveň pomáhá zvyšovat kybernetickou opatrnost, protože vede uživatele k tomu, aby nad odkazy více přemýšlel i v případě, že se objeví jen jeden varovný znak.

Všechna data se zpracovávají pouze lokálně v prohlížeči. Výsledky analýzy se ukládají jen dočasně kvůli fungování uživatelského rozhraní rozšíření a neposílají se nikam mimo zařízení uživatele. Díky tomu je při používání internetu zachováno soukromí uživatele.

4.2.1 Návrh detekčních pravidel

Návrh pravidel vychází z předchozích poznatků o phishingových útocích a technikách sociálního inženýrství popsaných v teoretické části. Zaměřila jsem se hlavně na znaky, které lze rozpoznat již ze samotné URL a které se v podvodných odkazech opakují. Pravidla a jejich parametry byly následně zpřesněny na základě testování reálných phishingových stránek tak, aby co nejlépe odpovídaly podobě současných phishingových útoků.

Pro přehlednost lze pravidla rozdělit do několika oblastí:

1. Znaky domény a hostitele - Sem patří například použití IP adresy místo domény, výskyt Punycode, vysoký počet subdomén, neobvykle dlouhá doména, nadměrné použití pomlček, kombinace písmen a číslic nebo náhodně působící název domény.

2. Struktura a přehlednost URL - Tato skupina zahrnuje nadměrnou délku celé URL adresy, velké množství parametrů, výskyt podezřelých slov v cestě (path) nebo řetězců připomínajících jinou doménu.

3.Přesměrování a skrytí cílové adresy - Pravidla v této skupině sledují přítomnost přesměrovacích parametrů, vložené URL adresy uvnitř parametrů nebo zakódované URL, které mají skrýt skutečný cíl odkazu.

4. Lexikální a kontextové znaky phishingu - Jde například o výskyt názvů známých značek mimo jejich oficiální domény, použití slov jako login, verify, secure nebo account, případně přítomnost citlivě působících slov v názvu hostitele.

5. Kombinovaná pravidla - Některé znaky samy o sobě nemusí být dostatečně průkazné, ale jejich kombinace zvyšuje pravděpodobnost phishingu. Z tohoto důvodu byla do návrhu zařazena i pravidla, která zvyšují skóre při současném výskytu více podezřelých vlastností.

4.3 Architektura řešení

Prototyp je navržen jako prohlížečové rozšíření pro Chrome (Manifest V3) složené ze tří funkčně oddělených částí.

První část (background script) běží na pozadí prohlížeče jako service worker. Obsahuje funkci analyzujUrl, která přijme URL adresu a vyhodnotí ji podle sady detekčních pravidel R1 až R29. Každé pravidlo přičítá body k celkovému skóre rizikovosti a zaznamenává důvod nálezu. Výsledek, tedy skóre a seznam aktivovaných pravidel, vrací volajícímu přes sendResponse.

Druhá část (content script) je automaticky spuštěna v kontextu každé navštívené stránky. Získá aktuální URL, ověří, zda doména není na uživatelském whitelistu uloženém v chrome.storage.local, a pokud ne, odešle ji k analýze do background scriptu. Při skóre 10 a více zobrazí přímo na stránce varovný banner s možností zavření nebo přidání domény na whitelist.

Třetí část (popup) tvoří uživatelské rozhraní rozšíření, přístupné kliknutím na ikonu v panelu nástrojů. Při otevření zjistí URL aktivní záložky, odešle ji ke stejné analýze do background scriptu a zobrazí výsledné skóre, klasifikaci (bezpečné nebo rizikové) a seznam aktivovaných pravidel.

Všechny tři části mezi sebou komunikují předáváním zpráv přes rozhraní chrome.runtime.sendMessage a chrome.runtime.onMessage.

4.3.1 Průběh vyhodnocení odkazu

Vyhodnocení probíhá v několika krocích. Po načtení stránky je získána její aktuální URL adresa, která slouží jako vstup pro analýzu. Nad adresou jsou postupně aplikována detekční pravidla popsaná v kapitole 4.2 a za každé splněné pravidlo je jeho bodová váha přičtena do celkového skóre. Výsledné skóre je následně porovnáno s nastavenými prahovými hodnotami, na jejichž základě se určí úroveň rizika. Pokud adresa žádný práh nepřekročí, rozšíření neprovede žádnou další akci.

4.4 Implementace

Kapitola popisuje technickou realizaci prototypu, konkrétně strukturu rozšíření, způsob vyhodnocení URL adres a ukládání výsledků pro zobrazení v uživatelském rozhraní.

4.4.1 Použité technologie a cílové prostředí

Prototyp byl vytvořen jako rozšíření pro Google Chrome podle standardu Manifest V3. Kód je napsán v TypeScriptu, který byl zvolen kvůli explicitnímu typování snižujícímu riziko chyb. Před nasazením do prohlížeče je přeložen do JavaScriptu nástrojem webpack s ts-loaderem.

4.4.2 Struktura rozšíření

Zdrojový kód prototypu je logicky rozdělen do dvou hlavních adresářů. Adresář public obsahuje statické soubory, kterými jsou konfigurační soubor manifest.json definující oprávnění rozšíření, konkrétně přístup k aktivní záložce a k lokálnímu úložišti prohlížeče, a soubor popup.html tvořící základní strukturu uživatelského rozhraní.

Zdrojové skripty v TypeScriptu (background, content a popup) jsou umístěny v src. Nástroj Webpack je následně kompiluje do distribučního adresáře dist, připraveného pro instalaci do prohlížeče.

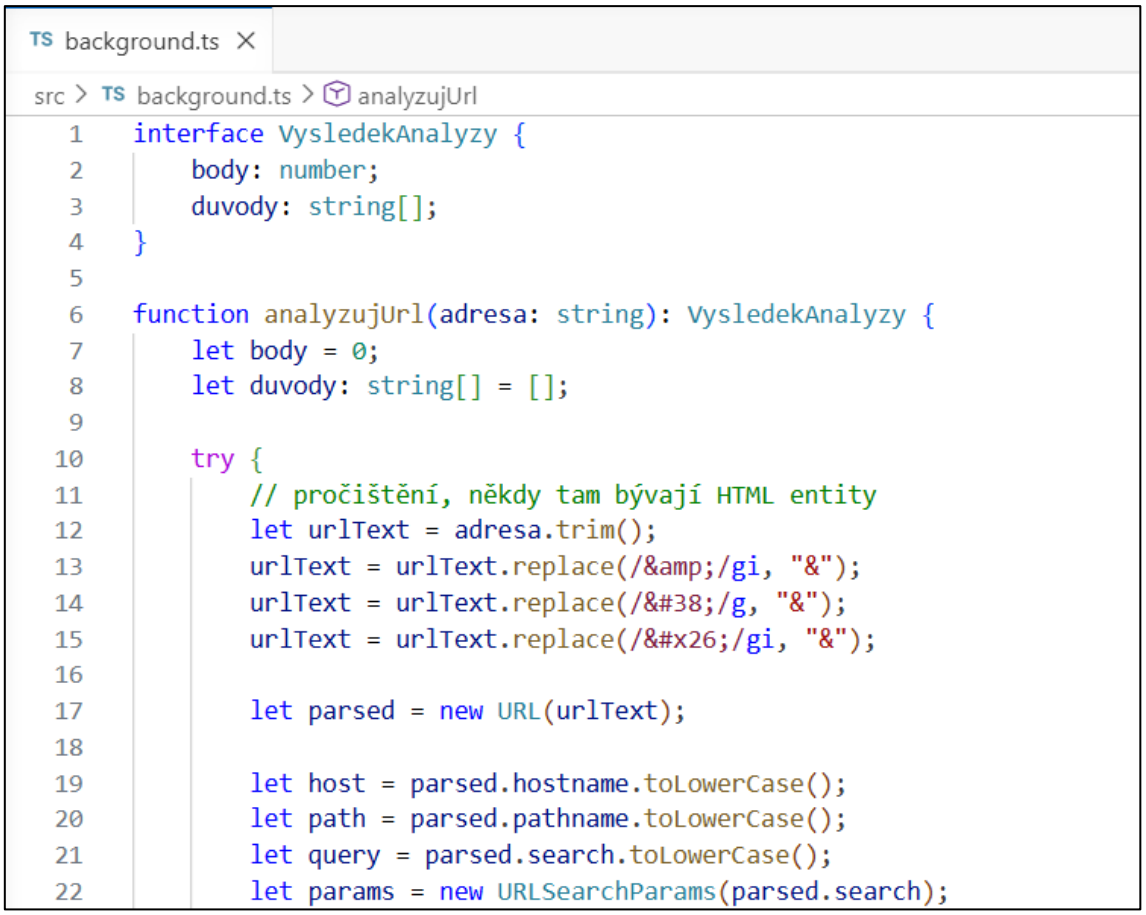
Obr. 8: Struktura souboru manifest.json

Zdroj: Vlastní zpracování (2026)

Soubor obsahuje základní nastavení rozšíření a určuje, jaké jeho části se budou používat a jak budou mezi sebou fungovat. Jsou v něm uvedena také oprávnění, která rozšíření potřebuje pro svou činnost. Hodnota manifest_version: 3 znamená, že je rozšíření vytvořeno podle novějšího standardu Manifest V3. Oprávnění activeTab slouží k tomu, aby rozšíření mohlo pracovat s právě otevřenou kartou v prohlížeči, například zjistit její adresu. Oprávnění storage poté umožňuje ukládat uživatelská nastavení, například seznam důvěryhodných domén. Soubor dále určuje, jakou funkci mají jednotlivé části rozšíření. background.js zajišťuje hlavní logiku na pozadí, content.js se vkládá do navštívených stránek a popup.html představuje jednoduché uživatelské rozhraní, které se zobrazí po kliknutí na ikonu rozšíření. Soubor je důležitý hlavně proto, že spojuje všechny části rozšíření do jednoho celku.

4.4.3 Vyhodnocení URL a výpočet skóre

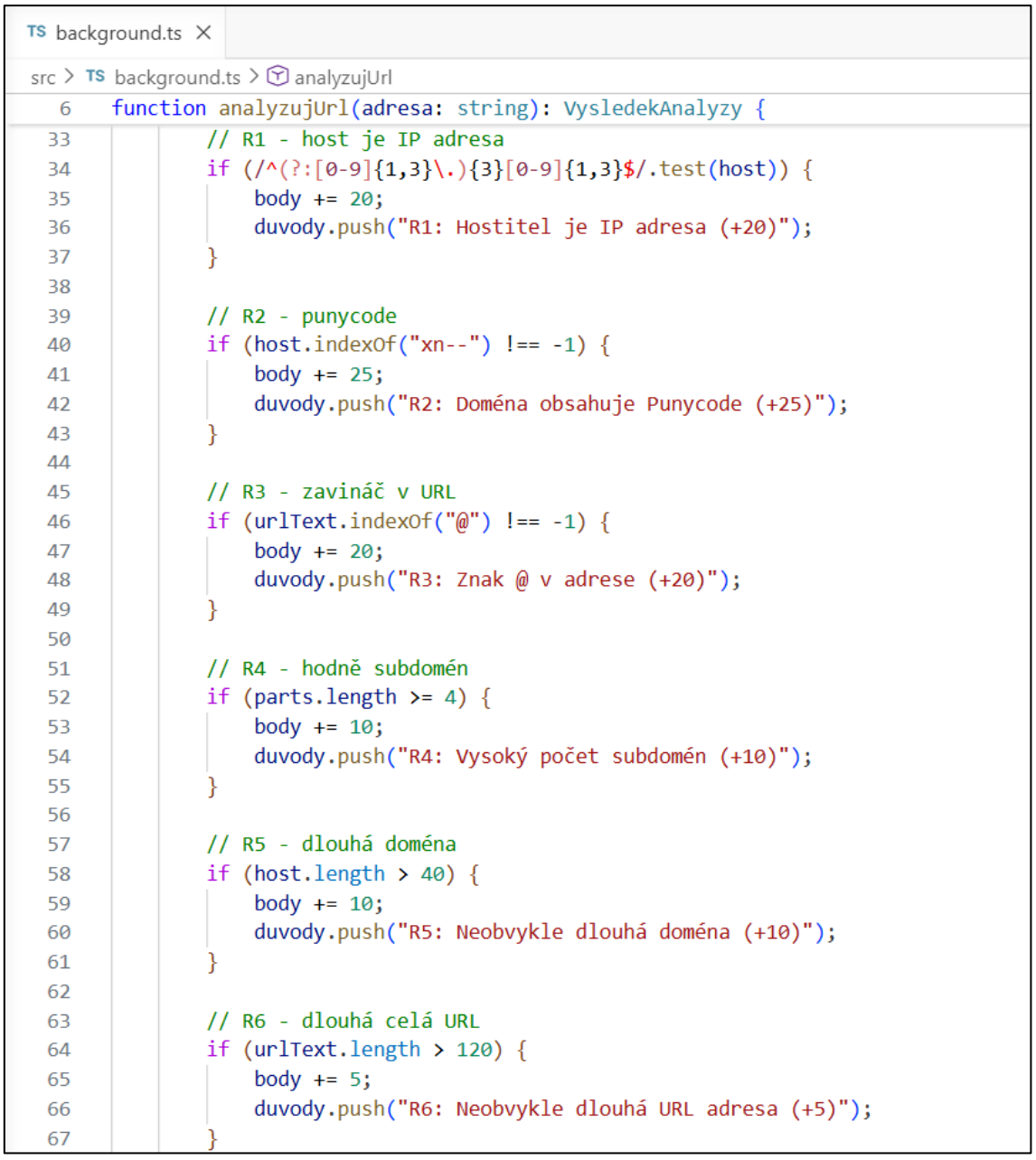
Funkce analyzujUrl běží na pozadí rozšíření a vyhodnocuje, jak moc je daná webová adresa podezřelá. Pro správné rozložení adresy na části, například oddělení názvu domény od cesty nebo parametrů, jsou využita standardní rozhraní prohlížeče URL a URLSearchParams. Adresa je poté procházena krok po kroku a kontrolovány jsou různé příznaky podezřelého chování, jako jsou skryté přesměrování, neobvykle dlouhé části adresy nebo podezřelé parametry. Za každý nalezený příznak se podle předem stanovené tabulky připočítá odpovídající počet bodů. Výsledkem je celkové skóre a seznam popisů vysvětlujících, proč byla jednotlivá pravidla uplatněna.



Obr. 9: Začátek implementace funkce analyzujUrl a zpracování URL adresy

Zdroj: Vlastní zpracování (2026)

Implementace ukazuje vybraná heuristická pravidla použitá při analýze URL adresy. Funkce analyzujUrl sleduje znaky, které se často objevují u phishingových nebo jinak podezřelých odkazů.



Obr. 10: Ukázka pravidel použitých při vyhodnocení URL adresy

Zdroj: Vlastní zpracování (2026)

. V ukázce je zachycena například kontrola, zda hostitel není tvořen IP adresou, detekce prefixu xn-- používaného u punycode domén, kontrola výskytu znaku @ v URL adrese, vyhodnocení nadměrného počtu subdomén a také sledování neobvyklé délky domény nebo celé URL adresy. Pokud je některý z těchto znaků nalezen, zvýší se hodnota proměnné body o předem určený počet bodů a současně se do pole důvody uloží textové vysvětlení, které popisuje důvod navýšení skóre.

```
346         } catch (error) {
347             console.error("Chyba pri analyze URL:", error);
348         }
349
350         return {
351             body: body,
352             duvody: duvody
353         };
354     }
355
356     chrome.runtime.onMessage.addListener((request, sender, sendResponse) => {
357         let vysledek = analyzujUrl(request.url);
358
359         sendResponse({
360             score: vysledek.body,
361             reasons: vysledek.duvody
362         });
363
364         return true;
365     });
```

Obr. 11: Vrácení výsledku analýzy a napojení funkce na komunikaci rozšíření

Zdroj: Vlastní zpracování (2026)

Samotný závěr funkce se stará o vytvoření a vrácení výsledné datové struktury. Ta v sobě nese dvě klíčové informace: celkové skóre rizikovosti a seznam konkrétních důvodů, kvůli kterým byla adresa označena za podezřelou. Díky tomu uživatel vidí nejen jak moc je web nebezpečný, ale i proč tomu tak je.

4.4.4 Správa whitelistu a lokálního úložiště

V rámci nefunkčních požadavků byla do prototypu zahrnuta možnost potlačit varování pro domény, kterým uživatel explicitně důvěřuje. Tento seznam výjimek neboli whitelist, je ukládán prostřednictvím rozhraní chrome.storage.local, které prohlížeč rozšířením poskytuje.

Uživatel může varování zavřít nebo doménu trvale autorizovat. Při schválení se název hostitele extrahuje z URL a uloží se do seznamu výjimek v lokálním úložišti prohlížeče.

TS content.ts ×

src > TS content.ts > zobrazVarovani

```
1   const currentUrl = window.location.href;
2   const hostname = new URL(currentUrl).hostname;
3
4   // Zkontrolujeme, jestli uživatel nedal doménu na whitelist
5   chrome.storage.local.get(['whitelist'], (result) => {
6       const whitelist = result.whitelist || [];
7
8       // Pokud doména NENÍ na whitelistu, pošleme ji k analýze
9       if (!whitelist.includes(hostname)) {
10          chrome.runtime.sendMessage({ action: "analyze", url: currentUrl }, (response) => {
11              // Pokud je skóre 10 a více, zobrazíme varování
12              if (response && response.score >= 10) {
13                  zobrazVarovani(response.score, hostname);
14              }
15          });
16      }
17  });
```

Obr. 12: Kontrola whitelistu a vyvolání analýzy ve skriptu content.ts

Zdroj: Vlastní zpracování (2026)

Při každém dalším načtení stránky skript content.ts nejdříve ověří, jestli je aktuální doména na tomto seznamu. Pokud na seznamu není, pošle se adresa k analýze. Jak je vidět na ukázce kódu, varování se uživateli zobrazí pouze v případě, že výsledné skóre rizikovosti dosáhne hodnoty 10 a více. Pokud je doména na whitelistu, adresa se k analýze vůbec neposílá a uživatel tak není opakovaně obtěžován zbytečnými varováními. Celý mechanismus funguje čistě lokálně na zařízení, takže žádná data nebo preference se nikam neodesílají.

4.4.5 Uživatelské rozhraní

Uživatelské rozhraní je řešeno pomocí vyskakovacího okna (popup), které zobrazuje výsledek vyhodnocení pro aktuální kartu. Součástí zobrazení je úroveň rizika a stručné důvody hodnocení, aby uživatel viděl, proč byla URL označena jako podezřelá.

Skript slouží k tomu, aby se po otevření rozšíření zobrazil výsledek analýzy aktuální stránky. Nejprve se zjistí, která karta je právě otevřená, a její URL adresa se odešle ke zpracování do skriptu na pozadí. Po vrácení výsledku se do popup okna doplní skóre rizikovosti, slovní vyhodnocení a seznam důvodů, které vedly k danému výsledku.

Pokud výsledné skóre dosáhne alespoň hodnoty 10, zobrazí se stav jako rizikový, jinak jako bezpečný. Jestliže nejsou nalezeny žádné rizikové znaky, zobrazí se informace, že nebyly rozpoznány žádné podezřelé vzorce. Význam této části spočívá v tom, že převádí interní výsledek analýzy do jednoduše pochopitelné podoby pro uživatele.

popup.ts

src > popup.ts > ...

```ts
chrome.tabs.query({ active: true, currentWindow: true }, (tabs) => {
    if (tabs.length > 0 && tabs[0].url) {
        const url = tabs[0].url;

        chrome.runtime.sendMessage({ action: "analyze", url: url }, (response) => {
            const scoreSpan = document.getElementById("scoreValue");
            const statusP = document.getElementById("status");
            const reasonsUl = document.getElementById("reasons");

            if (scoreSpan && statusP && reasonsUl && response) {
                scoreSpan.innerText = response.score.toString();

                if (response.score >= 10) {
                    statusP.innerText = "Vyhodnoceno jako: RIZIKOVÉ";
                    statusP.className = "danger";
                } else {
                    statusP.innerText = "Vyhodnoceno jako: BEZPEČNÉ";
                    statusP.className = "safe";
                }

                response.reasons.forEach((reason: string) => {
                    const li = document.createElement("li");
                    li.innerText = reason;
                    reasonsUl.appendChild(li);
                });

                if (response.reasons.length === 0) {
                    reasonsUl.innerHTML = "<li>Nenalezeny žádné rizikové vzorce.</li>";
                }
            }
        });
    }
});
```

Obr. 13: Vyhodnocení a zobrazení výsledků ve skriptu popup.ts

Zdroj: Vlastní zpracování (2026)

4.5 Dataset a metodika

Pro ověření funkčnosti prototypu bylo nezbytné sestavit sadu testovacích URL adres, která odpovídá reálným hrozbám.

Hlavním zdrojem dat pro hromadné testování se stala celosvětově uznávaná databáze PhishTank, konkrétně dataset aktuálních a ověřených phishingových odkazů dostupný na adrese hxxp://data.phishtank.com/data/online-valid.json.gz.

Z celkového množství dat byly pro hloubkovou analýzu a demonstraci přínosu této práce vybrány čtyři URL adresy, které tvoří jádro testovací sady:

- **Jeden legitimní vzorek:** Slouží pro srovnání a ukázku toho, jak analýza probíhá u běžné bezpečné adresy bez aktivace rizikových pravidel.
- **Tři phishingové vzorky:** Tyto adresy byly zvoleny pro upřesnění výpočtu skóre, jelikož každá z nich využívá odlišné techniky maskování.

Konkrétní stránky byly podrobeny testování, aby bylo možné názorně ukázat reakci algoritmu na specifické prvky phishingu. Jejich podrobný rozbor, dosažené bodové skóre a vyhodnocení přínosu pro detekci jsou uvedeny v kapitole 4.6 Výsledky a hodnocení.

4.5.1 Struktura datasetu

Validace proběhla formou hromadného testování na datasetu z databáze PhishTank. Analýze bylo podrobeno 55 803 unikátních URL, které byly v době testu klasifikovány jako aktivní a ověřené phishingové hrozby. Tento rozsáhlý vzorek reálných dat umožnil objektivně ověřit funkčnost detekčních pravidel R1–R29 a nastavit jejich váhy pro výsledné skóre.

Vzhledem k bezpečnostnímu charakteru a velkému rozsahu dat nejsou v textu práce uváděny všechny testované adresy v úplné podobě.

4.5.2 Implementace automatizovaného testovacího skriptu

Mechanismem celého rozhodování je konstanta threshold, který je v algoritmu nastaven na hodnotu 10 bodů. Celý princip funguje tak, že každé z devětadvaceti pravidel má svou specifickou váhu odpovídající jeho závažnosti, a pokud je u kontrolované URL adresy daný příznak nalezen, body se přičtou do celkového součtu.

test.ts

src > test.ts > createCounter

```
1   import * as fs from "fs";
2
3   interface AnalysisResult {
4       score: number;
5       reasons: string[];
6   }
7
8   const LIMIT = 60000;
9   const THRESHOLD = 10;
10
11  const RULES = [
12      "R1", "R2", "R3", "R4", "R5", "R6", "R7", "R8", "R9", "R10",
13      "R11", "R12", "R13", "R14", "R15", "R16", "R17", "R18", "R19", "R20",
14      "R21", "R22", "R23", "R24", "R25", "R26", "R27", "R28", "R29"
15  ];
```

Obr. 14: test.ts

Zdroj: Vlastní zpracování (2026)

Hranice 10 bodů slouží jako dělící čára: jakmile ji skóre dosáhne nebo překročí, systém vyhodnotí adresu jako rizikovou a varuje uživatele, zatímco v opačném případě ji propustí jako bezpečnou.

Konkrétní hodnotu jsem zvolila po kalibraci jako ideální kompromis. Kdybych hranici nastavila příliš nízko, hrozilo by velké množství falešných poplachů u legitimních stránek, zatímco příliš vysoký limit by mohl způsobit, že systém přehlédne promyšlenější formy phishingových útoků.

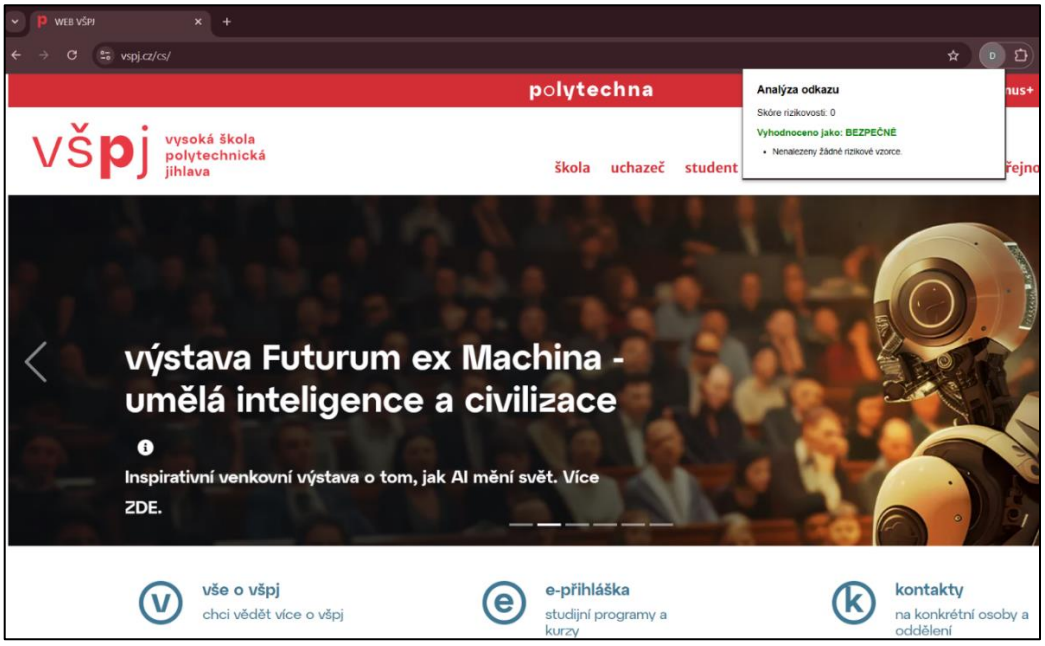
Konstanta LIMIT je nastavena na 60 000. limit optimalizuje výkon systému a stabilitu prostředí, což umožnilo kompletní analýzu 55 803 záznamů bez nutnosti redukovat objem dat.

4.6 Výsledky a vyhodnocení

Testování prokázalo, že heuristická analýza struktury URL je schopna identifikovat podezřelé vzorce chování. Níže jsou představeny vybrané testovací scénáře, které ilustrují reakci rozšíření na různé typy webových adres. Z důvodu zachování bezpečnosti a omezení šíření potenciálně rizikových odkazů byly části URL adres záměrně anonymizována a nahrazena symboly XXXX.

Scénář 1: Legitimní webová stránka

Při návštěvě oficiálního webu Vysoké školy polytechnické Jihlava rozšíření neodhalilo žádné rizikové znaky. URL adresa neobsahovala podezřelé prvky ani vzorce typické pro phishing. Výsledné skóre rizikovosti proto bylo 0.



Obr. 15: Legitimní webová stránka

Zdroj: Vlastní zpracování (2026)

Rozšíření odkaz vyhodnotilo jako bezpečný a nezobrazilo varovný banner. Tím se potvrdilo, že navržené řešení při práci s legitimními stránkami uživatele zbytečně nevyrušuje

Obr. 16: Analýza odkazu – výsledek heuristického hodnocení 0

Zdroj: Vlastní zpracování (2026)

Scénář 2: Odkaz s detekovanými rizikovými znaky

Při návštěvě adresy s neobvyklou strukturou URL rozšíření detekovalo přítomnost několika rizikových vzorců. Celkové skóre rizikovosti dosáhlo hodnoty 30, přičemž byly identifikovány následující indikátory:

Rozšíření bylo testováno na propagačním odkazu vedoucím na herní platformu.

Obr. 17: Analýza odkazu – výsledek heuristického hodnocení 30

Zdroj: Vlastní zpracování (2026)

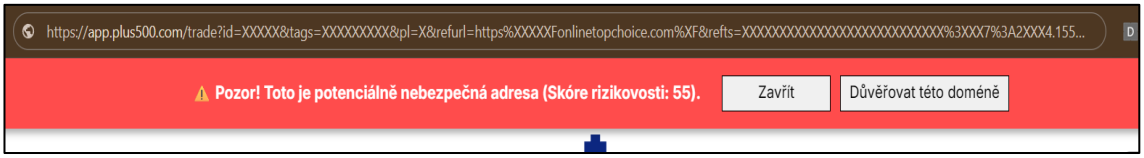
Systém zde zachytil rizikové vzorce a v reakci na vysoké skóre vygeneroval varovný banner. Uživateli poskytl informace o možném nebezpečí a nechal na jeho uvážení, zda stránku opustí, či jí bude důvěřovat.

Chování aplikace tak naplňuje její primární cíl: poskytnout srozumitelné varování, aniž by došlo k nucenému zablokování prohlížené stránky.

Obr. 18: Výsledek detekce s heuristickým skóre 30

Zdroj: Vlastní zpracování (2026)

Scénář 3: URL adresa s nepřehlednou strukturou



Obr. 19: Výsledek detekce s heuristickým skóre 55

Zdroj: Vlastní zpracování (2026)

V testovacím scénáři byla analyzována URL adresa, která vykazovala několik rizikových znaků. Rozšíření ji vyhodnotilo jako rizikovou se skóre 55 a zobrazilo uživateli varovný banner.

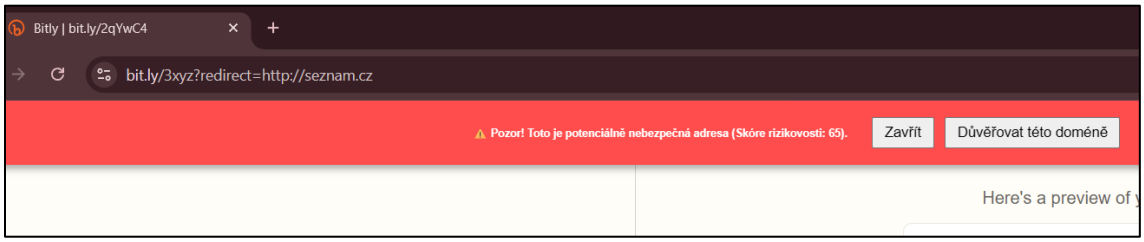
Obr. 20: Analýza odkazu – výsledek heuristického hodnocení 55

Zdroj: Vlastní zpracování (2026)

Hodnocení ovlivnila hlavně extrémní délka URL, skrytá adresa v parametrech a kódované znaky. Tyto prvky snižují přehlednost odkazu a ztěžují identifikaci cíle, což může naznačovat snahu o maskování adresy nebo podvodné přesměrování.

Scénář 4: Odkaz se zkracovačem a přesměrováním

V testovacím scénáři byla analyzována URL adresa, která obsahovala zkracovač odkazu a současně vykazovala znaky přesměrování. Rozšíření ji vyhodnotilo jako rizikovou se skóre 65 a zobrazilo varovný banner.



Obr. 21: Výsledek detekce s heuristickým skóre 65

Zdroj: Vlastní zpracování (2026)

K výslednému hodnocení přispěla především přítomnost přesměrovacího parametru, skrytí cílové adresy v parametru URL a také použití zkracovače URL. Tato kombinace je z bezpečnostního hlediska problematická, protože uživatel nemá na první pohled jasnou informaci o skutečném cíli odkazu. Současně je zřejmé, že odkaz pravděpodobně využívá mechanismus přesměrování na jinou stránku, což je postup často spojovaný se zakrýváním konečné cílové adresy. Z výsledků testování je patrné, že běžné webové stránky s jednoduchou a přehlednou strukturou URL získaly nulové nebo jen velmi nízké bodové hodnocení, a proto u nich nedošlo k vyvolání varování.

Naopak nejvyšší skóre bylo zaznamenáno u scénářů, ve kterých se současně vyskytovalo více rizikových technik. Přesměrování v kombinaci se zkracovačem URL a skrytým cílovým odkazem uloženým v parametru. Výrazně se projevily také případy využívající Punycode domény a otevřené přesměrování, protože právě tyto techniky aktivovaly pravidla s nejvyšší bodovou hodnotou. To naznačuje, že z pohledu heuristické detekce jde o snadno identifikovatelné hrozby.

Obr. 22: Analýza odkazu – výsledek heuristického hodnocení 65

Zdroj: Vlastní zpracování (2026)

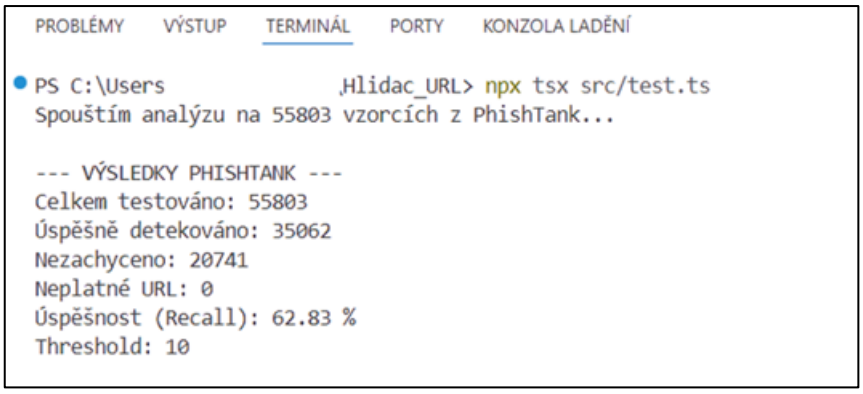
Na základě testování lze říci, že rozšíření dokáže rozlišovat mezi běžnými a podezřelými URL adresami a přiřazovat jim odpovídající míru rizika.

4.6.1 Hromadné testování prototypu

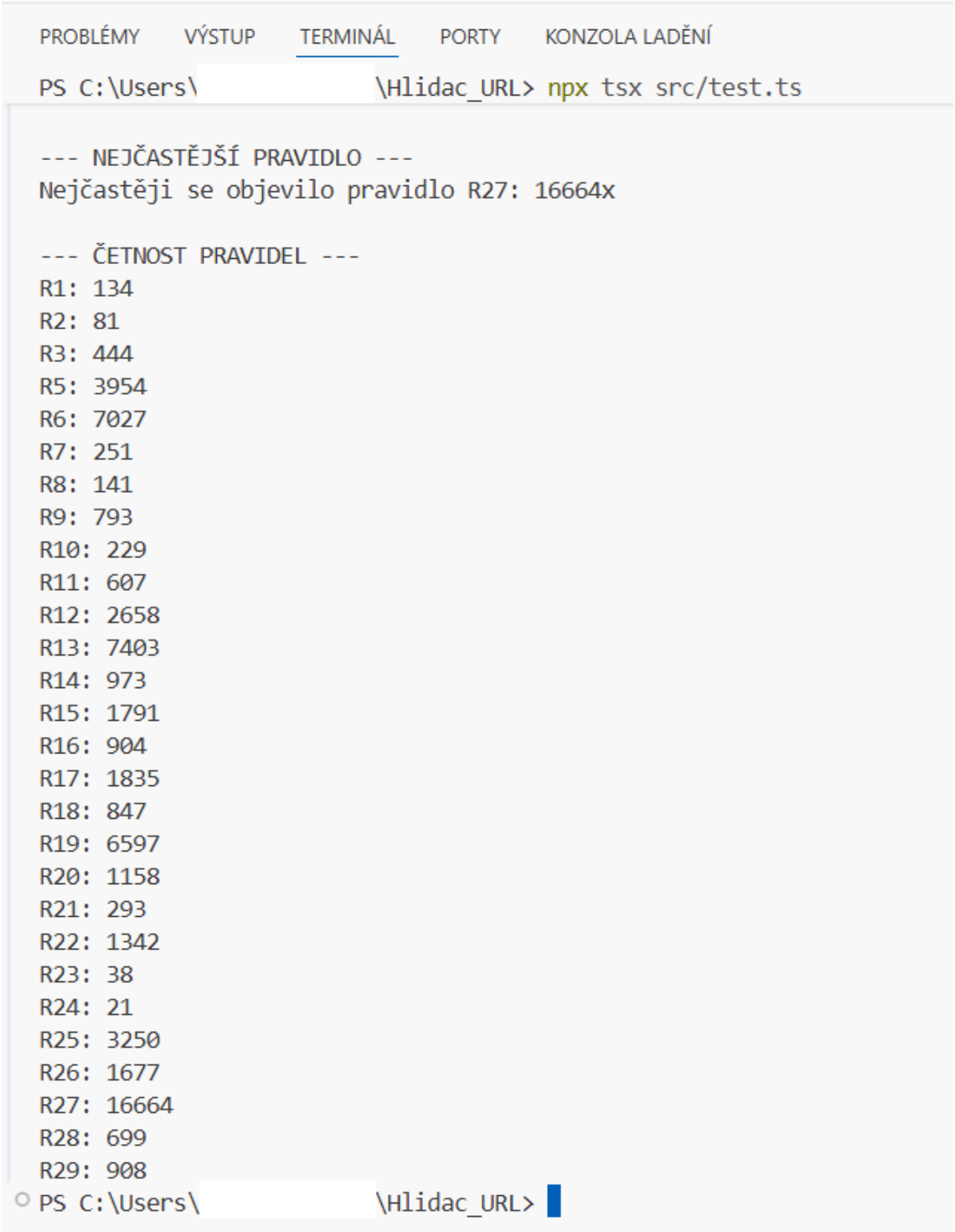
Klíčovou součástí ověření navrženého prototypu bylo hromadné testování v prostředí terminálu pomocí automatizovaného skriptu, který analyzoval rozsáhlý vzorek URL adres z databáze PhishTank.

Z 55 803 ověřených phishingových URL bylo rozšířením správně označeno jako rizikových 35 062 (62,83 %). Zbývajících 20 741 adres (37,17 %) zůstalo pod prahem detekce.

Analýza nedetekovaných URL ukázala, že se převážně jedná o adresy s jednoduchou a přehlednou strukturou hostované na kompromitovaných legitimních doménách, u nichž samotná podoba URL neobsahuje znaky typické pro phishingové techniky popsané v kapitole 3. Navržené řešení je účinné především proti phishingu využívajícímu manipulaci se strukturou URL, nikoli proti útokům prováděným z kompromitovaných legitimních domén.



Obr. 23: Terminálový výstup hromadného testování
Zdroj: Vlastní zpracování



Obr. 24: Výstup analýzy použitých detekčních pravidel

Zdroj: Vlastní zpracování (2026)

Tato analýza umožňuje lépe posoudit význam jednotlivých pravidel v rámci navrženého detekčního mechanismu a ukazuje, že některé heuristiky měly na výsledné rozhodování systému výrazně větší vliv než jiné.

V testovaném vzorku dominovaly zejména indikátory spojené s náhodnými alfanumerickými řetězci v cestě URL, hostováním na bezplatných platformách, nadměrnou délkou adresy a kombinací písmen a číslic v názvu domény.

Naopak komplexnější pravidla založená na souběhu více podezřelých znaků se uplatnila pouze okrajově. Pravidlo sledující výskyt čtyř a více úrovní subdomén nebylo během testování aktivováno vůbec, což naznačuje, že tento znak nepatřil v analyzovaném vzorku mezi významné indikátory phishingu.

4.7 Srovnání nástrojů

Tradiční nástroje fungují převážně na principu černé listiny. Navštívenou adresu porovnávají s databázemi známých hrozeb, což je přístup, který je sice přesný, ale má jedno zásadní omezení. Než se nový phishingový web do takové databáze dostane, musí ho někdo nejdříve nahlásit a analyzovat. Během tohoto časového okna, které bývá označováno jako Zero-day, jsou uživatelé bez ochrany.

Jak velký problém toto časové okno představuje, jasně dokládají statistiky. Podle dostupných dat totiž trvá průměrně 9 hodin, než je podvodný odkaz vůbec odhalen poté, co na něj klikne první oběť. Dalších 7 hodin zabere, než prohlížeče začnou uživatele varovat. Útočníci tak mají celkem přibližně 16 hodin, během kterých mohou volně jednat, aniž by jim cokoli bránilo (Oest et al., 2020, cit. podle Fernando et al., 2021). Navíc než dojde k samotnému zapsání hrozby do bezpečnostních seznamů, jako je například Google Safe Browsing, může to trvat 24 až 48 hodin, v některých případech i tři dny (Fernando et al., 2021).

Navržený prototyp proto pracuje jinak. Nezajímá ho, jestli je doména někde vedena jako škodlivá, ale sleduje, jestli její struktura nevykazuje znaky typické pro phishingové útoky. Prototyp tedy není náhradou za plnohodnotná antivirová řešení, ale může fungovat jako užitečná doplňková vrstva ochrany. Jeho hlavní výhoda spočívá v tom, že dokáže uživatele upozornit i na zcela nové útoky, které ještě nebyly nikde nahlášeny a tradičními filtry by tak snadno prošly.

4.8 Doporučení pro praxi

Výsledky testování prototypu i teoretická část ukazují, že při ochraně proti phishingu nestačí spoléhat jen na jeden typ nástroje. Jako vhodnější se v praxi jeví kombinace běžných bezpečnostních mechanismů s doplňkovými metodami, které dokážou analyzovat strukturu URL adresy a včas upozornit na podezřelé znaky.

Důležitou roli hraje také samotný uživatel. Ten by měl věnovat větší pozornost tomu, na jaké odkazy kliká. Opatrnost je na místě hlavně u neobvykle dlouhých adres, skrytých přesměrování v parametrech nebo při použití zkrácených URL. Právě těmito způsoby může být skutečný cíl odkazu skrytý.

Ve firmách a organizacích je vhodné uplatňovat vícevrstvý přístup k ochraně. Nestačí používat pouze technická opatření, ale je potřeba je doplnit i pravidelným školením zaměstnanců, jasně nastavenými postupy při práci s podezřelými zprávami a ověřováním neobvyklých požadavků. Důležitou součástí prevence je také vícefaktorové ověřování a pravidelná aktualizace systémů.

Navržený prototyp zároveň ukazuje, že i jednoduchá kontrola URL adres může být užitečným doplňkem ochrany. Jeho hlavní přínos spočívá v tom, že dokáže uživatele včas upozornit na

podezřelý odkaz. Takové upozornění může přerušit bezmyšlenkovité klikání, vést k větší opatrnosti a snížit riziko úspěšného útoku.

4.9 Omezení řešení

Navržený přístup stojí čistě na heuristickém posouzení lexikální podoby URL, což s sebou nese dvě zásadní slabiny: vznik falešně negativních a falešně pozitivních detekcí.

Falešně negativní výsledky se objevují především u phishingových kampaní, které nemanipulují strukturou adresy. Hromadné testování ukázalo, že 37,17 % phishingových URL nebylo zachyceno, protože šlo zejména o kompromitované legitimní domény s jednoduchou a přehlednou adresou bez sledovaných podezřelých znaků.

Naopak falešně pozitivní výsledky vznikají u legitimních URL s neobvyklou strukturou. Testy prokázaly, že některé důvěryhodné služby používající zkrácené odkazy, sledovací parametry nebo interní přesměrování mohou překročit stanovený limit 10 bodů. Ukázkou je scénář S04, v němž legitimní URL s vysokým počtem parametrů dosáhla skóre 20. Z tohoto důvodu rozšíření nabízí možnost přidat doménu na whitelist a tím varování pro danou adresu trvale vypnout.

Další slabinou je, že systém neprovádí kontrolu obsahu cílové stránky a není propojen s externími reputačními databázemi. Vyhodnocení tedy probíhá výhradně podle textové podoby URL, bez zohlednění širších souvislostí.

Do budoucna by bylo možné systém rozšířit o napojení na reputační databáze, analýzu obsahu cílové stránky, detailnější posuzování přesměrovacích řetězců a také o adaptivní práh, který by lépe reflektoval specifické vlastnosti jednotlivých domén.

Závěr

Práce se zabývala phishingem a důvody jeho vysoké úspěšnosti. Analýza potvrdila, že jádro těchto útoků nespočívá v technických chybách, ale v cílené manipulaci s lidským chováním.

Teoretická část práce shrnula hlavní typy phishingových útoků, popsala jejich vývoj a analyzovala vybrané manipulační techniky, které útočníci využívají ke zvýšení důvěryhodnosti svých zpráv a odkazů. Ukázalo se, že právě struktura odkazu může představovat důležitý signál rizika, přestože bývá pro běžného uživatele obtížně čitelná a snadno přehlédnutelná.

Praktická část navázala návrhem a implementací prototypu prohlížečového rozšíření určeného k heuristickému posuzování rizikovosti URL adres. Navržené řešení analyzuje vybrané znaky odkazu, přiřazuje jim bodové ohodnocení a při překročení stanovené prahové hodnoty zobrazí uživateli varování. Hromadné testování na datasetu 55 803 ověřených phishingových URL z databáze PhishTank prokázalo, že prototyp správně označil jako rizikových 35 062 adres (62,83 %). Zbývajících 37,17 % nedetekovaných adres tvořily převážně stránky hostované na kompromitovaných legitimních doménách, jejichž URL neobsahovala sledované podezřelé znaky. Prototyp je tak schopen zachytit vybrané rizikové vzorce, například nepřehledně strukturované adresy, skryté cílové odkazy v parametrech URL nebo znaky naznačující přesměrování. Současně se potvrdilo, že navržený přístup může fungovat jako srozumitelná doplňková vrstva ochrany, která upozorní i na odkazy, jež dosud nejsou evidovány v reputačních databázích.

Zároveň se v průběhu práce ukázala omezení navrženého řešení. Prototyp vyhodnocuje pouze lexikální strukturu URL a nepracuje s obsahem cílové stránky ani s externími seznamy známých hrozeb. Z tohoto důvodu nelze jeho rozhodování považovat za absolutně přesné a v některých případech může docházet k falešně pozitivním i falešně negativním výsledkům. Navržené řešení proto nepředstavuje náhradu za komplexní bezpečnostní nástroje, ale spíše jejich vhodné doplnění.

Došlo k propojení teoretického rozboru phishingu a sociálního inženýrství s návrhem konkrétního technického protiopatření v podobě prototypu prohlížečového rozšíření. Přínos práce spočívá jak v uceleném zpracování problematiky phishingu a jeho manipulačních mechanismů, tak v praktickém ověření možnosti využít transparentní heuristická pravidla pro včasné upozornění uživatele na potenciálně rizikový odkaz.

Seznam použité literatury

AMAL, Derin, AULBACH, Juliane a ZIRNGIBL, Johannes. *A Survey on Domain Impersonation.* In: Technical University of Munich [online]. 2022 [cit. 2025-12-21]. Dostupné z: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2022-01-1/NET-2022-01-1_07.pdf

ANDERSON, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3. vyd. Indianapolis: Wiley, 2020. ISBN 978-1-119-64278-7. Kapitola 3, Psychology and Usability. Dostupné také z: https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3-ch03.pdf

BOWCUT, Steven. *What a Phishing Attack Looks Like for Individuals and Small Businesses.* In: Brilliance Security Magazine [online]. 7. 7. 2025 [cit. 2025-11-05]. Dostupné z: https://brilliancesecuritymagazine.com/cybersecurity/what-a-phishing-attack-looks-like-for-individuals-and-small-businesses/

CENTRE FOR CYBERSECURITY BELGIUM. *NIS2 Notification Guide: Version 10.2024 – 1.2* [online]. Brussels: Centre for Cybersecurity Belgium, 2024 [cit. 2026-04-07]. Dostupné z: https://nis2-umsetzung.com/wp-content/uploads/2025/02/NIS2-Notification-guide-10-2024-v1.2-EN.pdf

CISCO. *What is a whaling attack?* In: CISCO [online]. nedatováno [cit. 2025-11-05]. Dostupné z: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-whaling-attack.html

Citace.com [online]. [cit. 2025-10-16]. Dostupné z: citace.com

DARKNET DIARIES. *EP 144: Rachel.* In: Darknet Diaries [online; přepis podcastu]. 2024-04-02 [cit. 2025-10-16]. Dostupné z: https://darknetdiaries.com/transcript/144/

DARKNET DIARIES. *EP 90: Jenny.* In: Darknet Diaries [online; přepis podcastu]. 2021 [cit. 2025-10-16]. Dostupné z: https://darknetdiaries.com/transcript/90/

DASHLANE. *What Is Clone Phishing? Common Cases & Security Tips* [online]. aktualizováno 6. 6. 2025 [cit. 2025-11-05]. Dostupné z: https://www.dashlane.com/blog/what-is-clone-phishing

DELOITTE. *The NIS2 Directive: High common level of cybersecurity across the European Union* [online]. 2024 [cit. 2026-04-07]. Dostupné z: https://www.deloitte.com/nl/en/services/consulting-risk/perspectives/the-nis2-directive.html

DROPBOX SECURITY TEAM. *How we handled a recent phishing incident that targeted Dropbox.* In: Dropbox.tech [online]. 2022 [cit. 2025-10-12]. Dostupné z: https://dropbox.tech/security/a-recent-phishing-campaign-targeting-dropbox

ESET. *Co je phishing?* [online]. 2016 [cit. 2025-10-16]. Dostupné z: https://www.eset.com/cz/phishing/

ESET. *Phishing 2.0: Znáte pretexting a Business Email Compromise?* In: ESET Digital Security Guide [online]. 2023 [cit. 2025-11-05]. Dostupné z: https://digitalsecurityguide.eset.com/cz/phishing-20-znate-pretexting-a-business-email-compromise

ESET. *Vishing: Co je to a jak se bránit?* In: ESET [online]. 2025 [cit. 2025-11-05]. Dostupné z: https://www.eset.com/cz/vishing/

EVROPSKÝ PARLAMENT A RADA. Směrnice (EU) 2022/2555 (NIS2). In: *EUR-Lex* [online]. 14. 12. 2022 [cit. 2026-04-07]. Dostupné z: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

FERNANDO, Matheesha, Abdun Naser MAHMOOD a Mohammad Jabed Morshed CHOWDHURY. *PhishLex: A Proactive Zero-Day Phishing Defence Mechanism using URL Lexical Features.* In: La Trobe University [online]. 2021 [cit. 2026-03-31]. Dostupné z: https://www.researchgate.net/publication/363698036_PhishLex_A_Proactive_Zero-Day_Phishing_Defence_Mechanism_using_URL_Lexical_Features

GALLAGHER, Sean. *All your Googles are belong to us: Look out for the Google Docs phishing worm.* In: Ars Technica [online]. 2017 [cit. 2025-10-12]. Dostupné z: https://arstechnica.com/information-technology/2017/05/google-docs-phish-worm-grabs-your-google-app-permissions-contacts/

GREENBERG, Andy. *The Full Story of the Stunning RSA Hack Can Finally Be Told.* In: WIRED [online]. 2021 [cit. 2025-10-12]. Dostupné z: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told

HADNAGY, Christopher. *Social Engineering: The Art of Human Hacking.* Indianapolis, In: Wiley Publishing, Inc., 2011. ISBN 978-0-470-63953-5. [online]. [cit. 2025-10-15]. Dostupné také z: http://repo.darmajaya.ac.id/4637/1/Social%20Engineering_%20The%20Science%20of%20Human%20Hacking%20%28%20PDFDrive%20%29.pdf

https://www.bookport.cz/kniha/cybercrime-5994/

HUANG, Aiden a THOTHATHRI, Vishwa. *Evolution of Sophisticated Phishing Tactics: The QR Code Phenomenon.* In: Unit 42 [online]. 2025 [cit. 2025-10-12]. Dostupné z: https://unit42.paloaltonetworks.com/qr-code-phishing

KASPERSKY. *What is Quishing or QR Phishing – Signs & Preventive Tips* [online]. 2025 [cit. 2025-10-16]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-quishing

KASPERSKY. *What is smishing and how to defend against it?* [online]. 2021 [cit. 2025-10-16]. Dostupné z: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

KOLOUCH, Jan. *CyberCrime*. Praha: Edice CZ.NIC, 2017. ISBN 978-80-88168-15-7 [cit. 2026-04-06]. Dostupné také z: https://www.bookport.cz/kniha/cybercrime-5994/

KOSINSKI, Matthew. *Spear phishing.* In: IBM.com – Think [online]. 2024 [cit. 2025-11-05]. Dostupné z: https://www.ibm.com/think/topics/spear-phishing

LAPSLEY, Phil. *Phreaking Out Ma Bell.* In: IEEE Spectrum [online]. 2013 [cit. 2025-10-11]. Dostupné z: https://spectrum.ieee.org/phreaking-out-ma-bell

LENAERTS-BERGMANS, Bart. *What is phishing? Techniques and prevention.* In: CrowdStrike [online]. 2024 [cit. 2025-10-16]. Dostupné z: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/phishing-attack/

MALKUSOVÁ, Tereza. *Smishing: Co to je a proč na něj snadno naletíme?* In: Dvojklik [online]. 6. 5. 2025 [cit. 2025-11-05]. Dostupné z: https://www.dvojklik.cz/smishing-co-to-je-a-proc-na-nej-snadno-naletime/

MITNICK, Kevin D. a SIMON, William L. *The Art of Deception: Controlling the Human Element of Security* [online]. Indianapolis, In: Wiley Publishing, Inc., 2002. ISBN 0-471-23712-4. [cit. 2025-10-11]. Dostupné z: https://ia600102.us.archive.org/4/items/pdfsandebooks/UP/Life%20Skills/Teach%20Yourself%20-%20Body%20Language%20%20Ebooks%20-%20Mantesh/The%20Art%20of%20Deception%20-%20Kevin%20Mitnick.pdf

NCSC. *Phishing attacks: defending your organisation* [online]. 2024 [cit. 2025-10-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/phishing

NÚKIB. *Spear-phishing a jak se před ním chránit* [online]. 3. 4. 2020 [cit. 2025-11-05]. Dostupné z:https://nukib.gov.cz/download/publikace/analyzy/Spear-phishing_a_jak_se_pred_nim_chranit.pdf

OEST, Adam a kol. *Sunrise to Sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale.* In: Proceedings of the 29th USENIX Security Symposium [online]. USENIX Association, 2020, s. 361–377. ISBN 978-1-939133-17-5. [cit. 2025-11-05]. Dostupné z: https://www.usenix.org/system/files/sec20-oest-sunrise.pdf

PROOFPOINT. *Phishing.* In: Proofpoint [online]. nedatováno [cit. 2025-10-16]. Dostupné z: https://www.proofpoint.com/us/threat-reference/phishing

REKOUCHE, Koceilah. *Early Phishing.* In: arXiv [online]. 2011 [cit. 2025-10-15]. arXiv:1106.4692. Dostupné z: https://arxiv.org/pdf/1106.4692

RHYSIDER, Jack. *EP 134: DEVIANT.* In: Darknet Diaries [online; přepis podcastu]. 2023-07-06 [cit. 2025-10-16]. Dostupné z: https://darknetdiaries.com/transcript/134/

RHYSIDER, Jack. *Human Hacker.* In: Darknet Diaries [online; přepis podcastu]. 2020-07-07, č. 69 [cit. 2023-10-27]. Dostupné z: https://darknetdiaries.com/episode/69

SHLOMAN, Tomer. *The Psychology of Phishing: Unraveling the Success Behind Phishing Attacks and Effective Countermeasures.* In: Trellix [online]. 2024 [cit. 2025-10-16]. Dostupné z: https://www.trellix.com/blogs/research/understanding-phishing-psychology-effective-strategies-and-tips/

SOCIAL-ENGINEER, LLC. *Physical Methods of Information Gathering.* In: Social-Engineer.org – Security Through Education [online]. nedatováno [cit. 2025-10-11]. Dostupné z: https://www.social-engineer.org/framework/information-gathering/physical-methods-of-information-gathering/

SOSAFE. *Quishing (QR code phishing)* [online]. nedatováno [cit. 2025-11-05]. Dostupné z: https://sosafe-awareness.com/glossary/quishing/

ŠPAČEK, Michal. *Cracking passwords from the Mall.cz dump.* In: Michalspacek.com [online]. 2018 [cit. 2025-10-12]. Dostupné z: https://www.michalspacek.com/cracking-passwords-from-the-mall.cz-dump

VERIZON. *2025 Data Breach Investigations Report* [online]. 2025 [cit. 2025-10-11]. Dostupné z: https://www.verizon.com/business/resources/T18b/reports/2025-dbir-data-breach-investigations-report.pdf