Katedra informatiky
Přírodovědecká fakulta
Univerzita Palackého v Olomouci

BAKALÁŘSKÁ PRÁCE

Jednoduchý phishingový útok

Podvodný web

2020

Veronika Klugerová

Vedoucí práce: doc. Mgr. Jan Outrata, Ph.D.

Studijní obor: Informatika pro vzdělávání, prezenční forma

Bibliografické údaje

Autor:	Veronika Klugerová
Název práce:	Jednoduchý phishingový útok (Podvodný web)
Typ práce:	bakalářská práce
Pracoviště:	Katedra informatiky, Přírodovědecká fakulta, Univerzita Palackého v Olomouci
Rok obhajoby:	2020
Studijní obor:	Informatika pro vzdělávání, prezenční forma
Vedoucí práce:	doc. Mgr. Jan Outrata, Ph.D.
Počet stran:	41
Přílohy:	1 CD/DVD
Jazyk práce:	český

Bibliograhic info

Author:	Veronika Klugerová
Title:	A simple phishing attack (The fraudulent website)
Thesis type:	bachelor thesis
Department:	Department of Computer Science, Faculty of Science, Palacký University Olomouc
Year of defense:	2020
Study field:	Computer Science for Education, full-time form
Supervisor:	doc. Mgr. Jan Outrata, Ph.D.
Page count:	41
Supplements:	1 CD/DVD
Thesis language:	Czech

Anotace

Obsahem práce je vytvoření falešného, avšak důvěryhodně vyhlížejícího, univerzitního webu pro studenty s nabídkou běžně nedostupných výukových materiálů a zkouškových testů. Práce, motivovaná tzv. Nigerijskými dopisy, by měla upozornit na problematiku stále aktuálních internetových podvodů, zejména phishingu, které mají za cíl získání finančních částek nebo citlivých informací, které mohou být následně zneužity například jako neopatrné vydání osobních a přístupových údajů k univerzitním systémům studenty.

Synopsis

The content of the thesis is the creation of a fake, but trustworthy-looking, university website for students with a range of commonly unavailable teaching materials and exam tests. The thesis, motivated by the so-called Advance-fee scam, should draw attention on the issue of still current Internet fraud, especially phishing, which aim to obtain financial amounts or sensitive information, which can then be misused, e. g. as a careless release of personal and access data to university systems by students.

Klíčová slova: podvod; Nigerijské dopisy; zneužití citlivých informací; web; Phishing

Keywords: hoax; Advance-fee scam; abuse of sensitive information; website; Phishing

Mé poděkování patří doc. Mgr. Janu Outratovi, Ph.D. za odborné vedení, vstřícnost a trpělivost, kterou mi v průběhu zpracování bakalářské práce věnoval. Děkuji i Mgr. Jiřímu Novotnému a správci sítě za ochotu a pomoc. V neposlední řadě děkuji svým přátelům a rodině, kteří mě podporovali nejen během psaní práce, ale i v průběhu studia.

Místopřísežně prohlašuji, že jsem celou práci včetně příloh vypracoval/a samostatně a za použití pouze zdrojů citovaných v textu práce a uvedených v seznamu literatury.

datum odevzdání práce podpis autora

Obsah

Seznam obrázků

Seznam tabulek

Seznam zdrojových kódů

1 Úvod

Internetové podvody jsou stále populárnější formou klasického podvodu. Jejich myšlenka spočívá v tom, že se útočník snaží od svých obětí získat osobní údaje nebo přímo finanční částky a to nenásilnou formou a pouze pomocí elektronické komunikace.

Nigerijské dopisy se řadí se mezi nejzajímavější druhy. I přes všeobecné povědomí lidí jsou stále jedny z nejvíce rozšířených internetových podvodů. Pod záminkou určité odměny, se pachatel snaží dostat k osobním údajům oběti a zachází i tak daleko, že ji žádá o finanční prostředky.

Pro částečnou simulaci tohoto podvodu využijeme techniky phishingu, kterou představíme v průběhu práce. Formou falešného univerzitního webu s nabídkou běžně nedostupných výukových materiálů se pokusíme získat přístupové údaje studentů Univerzity Palackého do informačního sytému STAG.
Bakalářská práce se bude skládat dohromady ze čtyř částí.

První část nás uvede do problematiky internetových podvodů. Zaměříme se na popis Nigerijských dopisů a phishingu, jejich vývoj a uvedeme pár nejzajímavějších příkladů.

Druhá část práce bude o vytvoření zmíněného webu a o využití phishingové techniky v praxi. Web budeme prezentovat jako „Nový výukový portál UP“, na němž budeme nabízet studijní materiály a především testy z minulých let, díky kterým bychom měli obdržet očekávané údaje.

Budeme se snažit vzhled našich webových stránek co nejvíce přizpůsobit vzhledu aktuálních stránek a aplikací Univerzity Palackého. Pokusíme se vytvořit co nejpřehlednější seskupení literatury a vyučovaných předmětů. Zaměříme se na přihlašovací formulář do sekce „Testy“, který zpřístupní různé pomocné materiály k ústním zkouškám a zápočtům. Jako jediná bude vyžadovat přístupové údaje stejně jako do portálu STAG. Všechny ostatní materiály bude možné libovolně stahovat v podobě PDF nebo jako obrázek PNG.

Vzhled našeho přihlašovacího formuláře přizpůsobíme systému STAG, tak aby přihlášení vypadalo věrohodněji. Zároveň ale budeme mít stránky po celou dobu experimentu nezabezpečené a budeme používat pouze protokol HTTP, který neumožňuje potřebné šifrování. Většina internetových prohlížečů na tento problém upozorní v podobě grafického znázornění v adresním řádku. V tomto ohledu spoléháme na to, že student nebude ověřovat pravost webových stránek a přihlášení bude brát jako samozřejmost.

Ve chvíli, kdy student vyplní požadované informace a přihlásí se, uložíme si jeho údaje do databáze a dostaneme tak možnost podívat se na jejich univerzitní účet a tedy i možnost zneužití jejich osobní dat.

Protože se bude jednat o „Nový výukový portál“ vybereme si pouze vzorek studentů a to studenty z oborů Matematika a Informatika. Dostupné materiály přizpůsobíme jejich zaměření. Pokud se student přihlásí do sekce „Testy“, pomocí svého univerzitního loginu, obdrží, po určité době, email v podobě upozornění na případný stav zneužití a následné oznámení o tom, že jeho uživatelské jméno a heslo budou z naší databáze odstraněny.

Třetí část se zaměří na správné nakonfigurování poštovního serveru Postfix, který, pro naše účely, poslouží k prvotnímu kontaktu se skupinou vybraných studentů. Vzorku rozešleme email o existenci webu spolu s odkazem na stránky. Web bude dál obsahovat emailový formulář pro případné dotazy. Na závěr nám poslouží jako upozornění na možné riziko zneužití přihlašovacích údajů.

Čtvrtá část bude obsahovat analýzu sekce „Testy“.

2 Internetový podvod

Internetové podvody lze definovat jako trestné činy, které jsou páchány proti jednotlivcům nebo skupinám lidí s úmyslem poškodit jejich pověst nebo jim přivodit přímou či nepřímou újmu nebo ztrátu. Cílem je získat citlivé informace, údaje o platebních kartách, heslech apod.

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

2.1 Druhy internetových podvodů

Mezi nejčastěji páchané internetové podvody řadíme podvody, které jsou kombinací sociálního inženýrství spolu s instalací škodlivého softwaru.

> „*Sociální inženýrství* je snaha podvodem vylákat od důvěřivých uživatelů jejich osobní informace, jako jsou hesla nebo bankovní údaje, případně získat přístup k jejich počítači, za účelem instalace škodlivých programů. Zloději a podvodníci používají techniky sociální inženýrství. Je totiž snadnější podvodem vylákat uživatelské heslo, než složitě obcházet zabezpečení počítače.“[2]

> „*Malware* (zkratka anglického výrazu pro škodlivý software – ‘malicious software’) je typ obtěžujícího nebo škodlivého softwaru, který má za úkol zajistit útočníkovi tajný přístup do vašeho zařízení.“[3]

1. Mezi techniky a nástroje sociálního inženýrství patří:

   Pretexting
   Útočník si dopředu vytvoří scénář (pretext), podle kterého se během komunikace s obětí bude řídit. Forma tohoto podvodu většinou probíhá po telefonu nebo přes oficiálně domluvenou schůzku, tedy pomocí rozhovoru. Zde se útočník vydává za osobu, která je ve svém, podle scénáře připraveném, oboru důvěryhodná a má tak právo na bližší dotazování oběti na informace, na které by oběť za normálních okolností neodpověděla. Cílem je nenápadně vylákat důležité údaje o oběti.

Scareware
Zobrazuje falešná upozornění na „pravděpodobné“ infikování počítače škodlivým softwarem. Zároveň nabízí i jednoduché řešení, jak se problému zbavit a to pomocí instalace falešného antivirového programu nabízeného v rámci upozornění. Ten bývá většinou zpoplatněn, ale je to jediný způsob, jak se rychle zbavit problému. Oběti tak stahují falešný antivirus, což je ve skutečnosti Malware určený k odcizení osobních údajů oběti.

2. Mezi druhy malwaru patří:

Spyware
Tajně shromažďuje informace o našem chování na internetu. Jeho cílem je zaznamenávat navštívené stránky, údaje o platebních kartách, heslech apod.

Adware
Většina adware programů pouze obtěžuje uživatele vyskakovacími okny, tedy nepředstavuje riziko načež najdou se i takové, které sbírají informace o historii prohlížeče, zadané osobní údaje nebo jsou dokonce schopny nahrávat stisknuté klávesy. Mezi nejčastější řadíme nevyžádané reklamy, pop-up okna nebo automatickou změnu domovské stránky.

Trojský kůň
Jeden z nejznámějších škodlivých softwarů vůbec. Bývá přestrojen za užitečný program, aplikaci, hru apod., ale slouží k infikování systému určitého počítače. Často jej můžeme naleznout i jako součást emailu, přesněji jako připnutý soubor v příloze. Slouží ke krádeži osobních informací nebo šíření jiných virů.

Podvodné emaily, jakožto kombinace obou zmíněných tříd, jsou nejrozšířenějším typem internetového podvodu. Často v emailové schránce můžeme objevit zprávy o snadném přivýdělku, výhře v loterii, možnosti výhodné půjčky nebo seznámení se s ideálním partnerem a mnoho dalších. Ve většině případů emaily obsahují i přílohy různých dokumentů nebo souborů, které v sobě mohou škodlivý software skrývat.

3. Zástupce této třídy jsou:

Phishing

Nigerijské dopisy

3 Nigerijské dopisy

Nigerijské dopisy, taktéž známé jako **Scam419** nebo **419 Advance Fee Fraud**, jsou zvláštním a také jedním z nejrozšířenějších druhů internetového podvodu.

Označení „zvláštní“ nabyly Nigerijské dopisy právě proto, že jsou většinou kombinací více internetových podvodů dohromady. Využívají jak techniky sociálního inženýrství tak škodlivého softwaru.

Princip spočívá v elektronické komunikaci mezi podvodníkem a jeho obětí, ze které se snaží, pod různými záminkami, vylákat nemalou částku peněz.

Komunikace mezi podvodníkem a osloveným funguje na bázi dopisování si emailových zpráv, anebo také často pomocí internetových diskuzí. Většinou se pachatel vydává za někoho jiného a přizpůsobí tomu i ostatní postupy, takže je obtížné ho vysledovat a nepravděpodobné, že by se někdy mohl se svoji obětí setkat, pokud by sám nechtěl.

Bohužel, pokud se oběť rozhodne odpovědět a pošle peníze nebo umožní nějakou transakci, začíná páchat trestný čin. Přistupuje tím tak na kriminální jednání, přesněji na zřetelný pokus o krácení či zkrácení na dani.

Pokus o krácení daně se řadí mezi trestné činy, které jsou obsaženy v trestním zákoníku každé země. Jedná se o odvod peněz ze státního rozpočtu, a to považujeme za závažný zločin.

Číslo 419 je odvozeno od číselného označení kriminálního činu „pokusu o vyvedení peněz ze státního rozpočtu“ v Nigérii. Tuto příponu zavedla nigerijská vláda právě kvůli častým zločinům tohoto typu.

Brzy po odpovědi bude následovat další žádost o finanční výpomoc. Většinou se jedná o neočekávané náklady, jako jsou zvýšené daně, různé poplatky za převody a odvody nebo úplatky úředníkům.

V dnešní době se najdou i případy, kdy se snažíme získat mimo financí i osobní informace, které jsou někdy mnohem cennější než obnos peněz, i když jsou s penězi velmi spjaty. Řadí se mezi ně například číslo občanského průkazu, bankovního účtu, rodné číslo nebo číslo kreditní karty. Případně jiné citlivé informace.

Oběť se tak sama o sobě stává vydíratelnou a právě vydírání je další prvek, který specifikuje Scam 419.

3.1 Realizace

Kontakt vytvoří sám pachatel, který se pomocí internetových služeb, spojí se svojí obětí. Podvodníci rozesílají hromadné zprávy po celém světě, aby pravděpodobnost následné odpovědi byla vyšší - jedním ze specifických prvků Nigerijských dopisů je špatná gramatika přeloženého textu do angličtiny.

V emailu útočník nabízí své oběti velkou částku peněz výměnou za malou zálohu finančních prostředků. S tím souvisí i předání informací o bankovním účtu a dalších identifikačních údajích, aby bylo možné transakce provést.

Podvodníci se většinou prezentují jako zoufalý, ale renomovaný člověk, který se ocitá v nesnázích. Kvůli různým překážkám nemůže prozradit svoji identitu nebo vystupuje jako zprostředkovatel komunikace pod vymyšleným jménem.

Do emailu přidávají i falešné dokumenty, které nesou oficiální vládní značky, aby zpráva vypadala věrohodněji.

Pokud oběť sama neukončí komunikaci s podvodníkem, budou žádosti o další finanční výpomoc i nadále pokračovat. Podvodník bude žádat o peníze, do té doby, kdy oběť přestane komunikovat nebo už víc peněz jednoduše nemá.

Netřeba dodávat, že oběti nikdy nebude vyplacena žádná finanční částka a to bez ohledu na to, jak velkou sumu byla ochotna věnovat.

3.2 Historie

Historie Nigerijských dopisů má prameny až v 16. století, datující se kolem roku 1598, kdy probíhala válka mezi Španělskem a Anglií. Pro Španělsko konec 16. století nebyl příznivý, protože prodělalo dva státní bankroty, přišlo o svou neporazitelnou flotilu Armada a ztratilo svého panovníka Filipa II., kterého vystřídal ne moc schopný Filip III.[4]

Španělský vězeňský podvod, tedy prvotní „Nigerijský dopis“, spočíval v komunikaci mezi obětí a podvodníkem, který spoléhal na to, že mu někdo (oběť) poskytne potřebné finance k zajištění jeho propuštění ze španělského vězení. Samozřejmě ne zadarmo.

Nejčastěji se jedná o Angličana, který se nedopatřením dostal na španělskou půdu, kde mu v období rozporu mezi Španělskem a Anglií, hrozila i smrt. V dopise uváděl, že je z bohaté rodiny nebo alespoň blízký příbuzný někoho bohatého, případně se prezentoval jako voják s vyšší hodností. Ve Španělsku plnil jistou tajnou misi, kterou ale nedokončil a byl Španěly uvězněn do jednoho z jejich vězení.

V dopise žádal oběť o peněžní prostředky potřebné k útěku s příslibem, že za pomoc bude později velkoryse odměněna a to jak finančně, tak i například prostřednictvím sňatku s jeho „krásnou“ dcerou.

Jakmile se však oběť obrátí s odpovědí a finanční výpomocí zjistí, že se objevily potíže (nečekané výdaje) a je zapotřebí poslat další peníze. Místo toho, aby oběť komunikaci ukončila, je ochotná do ní investovat víc. Tento postup pokračuje do doby než oběť sama nepřestane komunikovat s podvodníkem nebo podvodník nevyláká dostatečné množství prostředků, které zamýšlel.

V 16. století bylo velice obtížné pachatele dopadnout a požadovat nějakou náhradu, protože k tomu nebyly dostatečné možnosti ani technologie. Nicméně, i přes dnešní možnosti a technologie, to platí stále...

Ve Francii se kolem roku 1876 objevily první zmínky žádostí o dopadení podvodníků. Byla vymyšlena nová forma španělského vězeňského podvodu, tzv. „Dopisy z Jeruzaléma“, protože příběh útěku z vězení přestal být efektivní. Na scéně se začaly objevovat dopisy o dcerách v nebezpečí, truhlicích plných peněz a mnoho dalších podobných témat. Tyto dopisy byly psány bohatými obchodníky, často pocházejícími z Jeruzaléma, kteří potřebovali přemístit své peníze. Dopisy byly adresovány převážně vysoce postaveným lidem a to především kvůli větší pravděpodobnosti dosažení vyššího zisku a kvůli tomu, že neradi působili skandály

na veřejnosti.

První, kdo zdokumentoval případy dopisů, byl bývalý zločinec a galejník E. F. Vidocq, kterého považujeme za zakladatele moderní policejní organizace ve Francii a který se postupem času stal uznávaným kriminalistou.[5] Konkrétní příklad dopisu zmiňuje ve svých pamětech Memoare of Vidocq, kde uvádí i statistiky.

(a) Eugène-François Vidocqe

"In this cruel situation, having heard mention of you by a relation of my master's, who had property in your district, I beg to know if I cannot, through your aid, obtain the casket in question and get a portion of the money which it contains. I could then supply my immediate necessities and pay my counsel, who dictates this, and assures me that by some presents, I could extricate myself from this affair.

"Receive, sir, &c.

(Signed) "N———."

Out of one hundred such letters, twenty were always answered

(b) příklad dopisu uveden v Memoare of Vidocq

Obrázek 1: E. F. Vidocq

Další vlna dopisů proběhla během války USA se Španělskem roku 1898. Boje začaly kvůli výbuchu na americké lodi v havanském přístavu, kterou údajně způsobily španělské tajné služby. Spojené státy podporující nezávislost Kuby vyprovokovali Španělsko, očekávajíc rozsáhlé územní zisky na úkor zámořských kolonií. Dopisy byly adresovány americkým společnostem od uvězněného vojáka na španělském území.

Naopak dálnopisem se do USA dostaly listy o tankeru převážející ropu z Nigérie, která by mohla být prodávaná za velice výhodnou cenu - samozřejmě výměnou za určitou hotovost předem.

3.3 Současnost

Známky moderních podvodných dopisů byly objeveny v 70. letech minulého století. Tehdy ještě pomocí klasické pošty většinou od bohatých nigerijských obchodníků, kteří v dopisech žádali o pomoc s vývozem nemalého finančního obnosu ze země a nabízeli odškodnění v podobě určitého podílu nazpět. S příchodem elektronické pošty se podvody začaly přesouvat na internet.

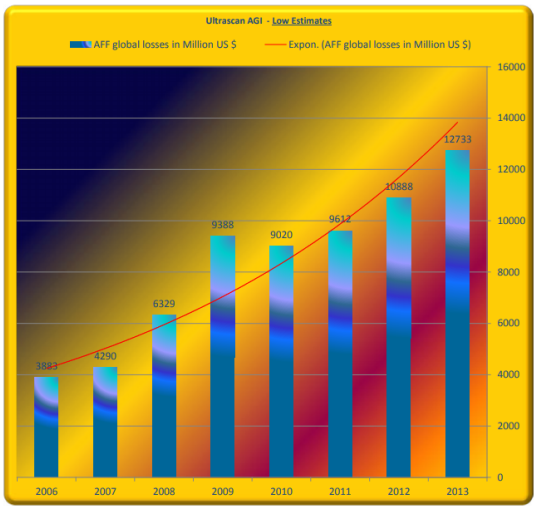
Masivní rozesílání emailů lidem do celého světa od nigerijských obchodníků, princů, ředitelů a jiných vlivných lidí právě z Nigérie mělo za následek označení této země za největší podvodný stát na světě. Toto tvrzení není až tak zcela pravdivé.

„V roce 2002 americké Ministerstvo Spravedlnosti získalo soudní příkaz k otevření všech zásilek z Nigérie, které procházely letištěm JFK v New Yorku. Přibližně 70% se týkalo podvodných nabídek."[6]

Statistiky v roce 2006 ukázaly, že největším zdrojem podvodných emailů na světe je z 61% USA. Z Velké Británie se odesílá 16% a z Nigérie pouze necelých 6%. To ale neznamená, že počáteční myšlenka za vznikem takovýchto dopisů nepochází právě ze zmiňované Nigérie. Podvodníci operují ze zdejších internetových kaváren a označují své cíle jako *Magas*, což v jejich slangu znamená hlupáci. Mají komplice po celém světě, kteří pak dokončují větší transakce.[7]

> „Každá osoba, která z jakéhokoli nepravdivého předstírání a se záměrem podvádět získá od jakékoli jiné osoby něco, co by mohlo být ukradeno, nebo přiměje jinou osobu, aby doručila jakékoli osobě něco, co by mohlo být ukradeno, je vinna zločinem, a je uvězněn na tři roky.
>
> V případě, že věc je v hodnotě jednoho tisíce Nairů nebo výš, to je náchylné k odnětí svobody na sedm let.
>
> Je nepodstatné, že věc je získána nebo její dodání je vyvoláno prostředkem smlouvy vyvolané falešným předstíráním.
>
> Pachatele nelze bez zatýkacího rozkazu zatknout, pokud nebude zjištěno, že spáchal trestný čin.“[8]

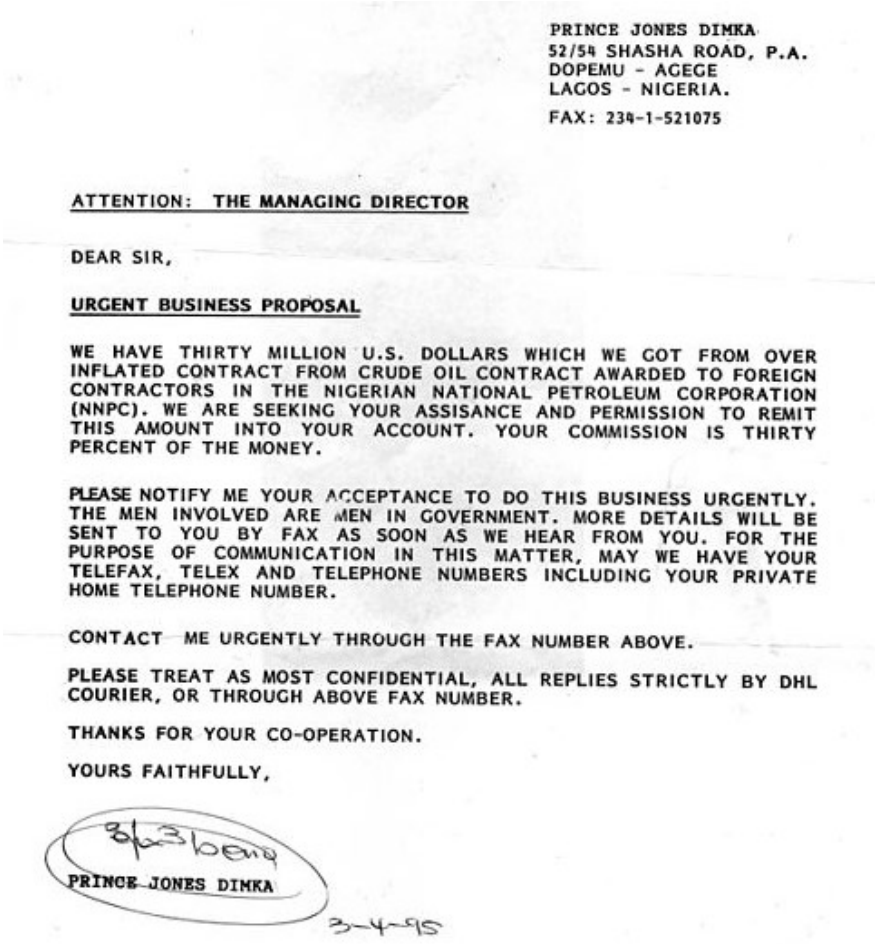
Podvody dramaticky vzrostly v roce 2009. Společnost Ultrascan, mezinárodní výzkumná organizace zaměřující se převážně na finanční podvody, padělání a kybernetickou kriminalitu uvedla, že po přezkoumání 8 503 stížností Nigerijských dopisů pocházejících ze 152 zemí, byla škoda vyměřena na 9,3 miliardy dolarů, což bylo dle průměru o 3 miliardy víc než v předchozím roce.



Obrázek 2: Vývoj a ztráta od 2006 do 2013 [9]

3.4 Příklady dopisů

„Úspěšný podvodník je ten, který dokáže nakombinovat dobrou nabídku s přesvědčivým příběhem a může si tak oběť svými slovy koupit.“



PRINCE JONES DIMKA
52/54 SHASHA ROAD, P.A.
DOPEMU - AGEGE
LAGOS - NIGERIA.
FAX: 234-1-521075

ATTENTION: THE MANAGING DIRECTOR

DEAR SIR,

URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE.

PLEASE TREAT AS MOST CONFIDENTIAL, ALL REPLIES STRICTLY BY DHL COURIER, OR THROUGH ABOVE FAX NUMBER.

THANKS FOR YOUR CO-OPERATION.

YOURS FAITHFULLY,

PRINCE JONES DIMKA

3-4-95

Obrázek 3: Klasický Scam 419 [10]

Každý z nás obdržel alespoň jeden email od nigerijského velvyslance, ředitele národní nigerijské banky nebo třeba od bratrance tajemníka nigerijského prince. Pro příklad uvedeme ty Nigerijské dopisy, které překvapivě dosáhli nečekaných úspěchů.

3.4.1 Daenerys Targaryen žádá o pomoc

V roce 2012 začala Daenerys Targaryen představovaná jako Daenerys za bouře zrozená z rodu Targaryenů, Královna Andalů a prvních lidí, Khaleesi velkého Dothrackého moře, Ničitelka okovů a Matka draků, pomocí emailových zpráv žádat lid po celém světě o pomoc v podobě $520, jedné lodi a jednoho draka,

aby se mohla vrátit zpět domů. Na oplátku za požadované služby, nabízí odměnu ve formě titulu Nejvyššího lorda Sedmi Království. [11]

3.4.2 Nigerijský astronaut

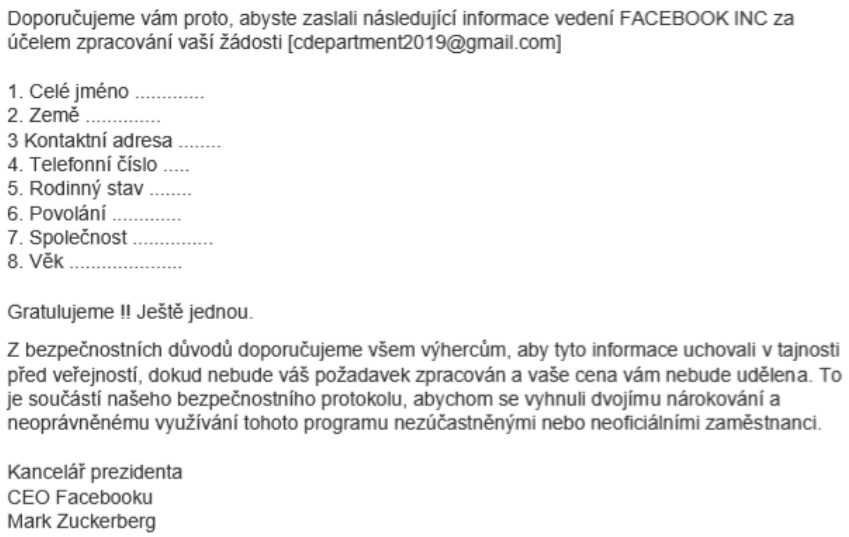
Rok 2016. Hitem se stal Nigerijský astronaut, který se ztratil ve vesmíru. K tomu, aby se vrátil, potřebuje pomoc v podobě finanční částky, která byla vyčíslena na hodnotu 3 miliónů dolarů. Zní to nemožně, ale našli se i tací, kteří byli ochotni tuto částku astronautovi nabídnout bez větších problémů.

Vysvětlené jednotlivé odstavce nalezneme na [12].

3.4.3 Facebooková výhra v loterii od Marka Zuckerberga

Dalším velice zajímavým příkladem Nigerijských dopisů jsou emaily o výhrách v loteriích rozšířené především na sociálních sítích.

Oběť obdrží falešné oznámení o výhře v loterii a nezáleží na tom, jestli se vůbec nějaké loterie zúčastnila. Výhra může být různá od telefonů po rekreační pobyty v zahraničí. V tomto případě se jedná o email od samotného zakladatele Facebooku, Marka Zuckerberga, který informuje vybrané uživatele sociální sítě o výhře 1 miliónu amerických dolarů za propagaci „2019 Edition Facebook“.
Je požádána o zaslání osobních informací, jako je jméno, bydliště nebo pracoviště nejspíš pro ověření její osoby, aby výhra nepadla do rukou někomu jinému. Po odeslání těchto údajů obdrží odpověď, kde útočník/Mark Zuckerberg žádá o zaslání menšího poplatku za uhrazení tak velké výhry. Jakmile oběť poplatek pošle, pachatel si následně vymyslí další.



Doporučujeme vám proto, abyste zaslali následující informace vedení FACEBOOK INC za účelem zpracování vaší žádosti [cdepartment2019@gmail.com]

1. Celé jméno .....
2. Země .....
3 Kontaktní adresa .....
4. Telefonní číslo .....
5. Rodinný stav .....
6. Povolání .....
7. Společnost .....
8. Věk .....

Gratulujeme !! Ještě jednou.

Z bezpečnostních důvodů doporučujeme všem výhercům, aby tyto informace uchovali v tajnosti před veřejností, dokud nebude váš požadavek zpracován a vaše cena vám nebude udělena. To je součástí našeho bezpečnostního protokolu, abychom se vyhnuli dvojímu nárokování a neoprávněnému využívání tohoto programu nezúčastněnými nebo neoficiálními zaměstnanci.

Kancelář prezidenta
CEO Facebooku
Mark Zuckerberg

Obrázek 4: Úryvek z dopisu - Facebook Lottery scam email [13]

3.5 Škody a hrozby

I přes všeobecně panující názor, že lidé z chudších vrstev jsou v tomto ohledu mnohem zranitelnější, průzkum emailových scamů ukázal, že lidé s větší inteligencí jsou častěji okradeni.

Pro větší podvody útočníci potřebují, aby jejich oběti věřili převážně ve vlastní schopnosti a zkušenosti. Například doktoři často odpovídají na podvody, které začíná žádostí o pomoc méně šťastným. Naproti tomu málo vzdělaní nebo finančně nezkušení lidé nejsou pro podvodníky tak žádoucí, neboť obecně nedůvěřují tolik svému vlastnímu úsudku a brzy si uvědomí, že existuje možnost být podveden.

Při dlouhodobějším jednáním si oběť s podvodníkem vytvoří vztah, který můžeme přirovnat ke Stockholmskému syndromu. Když k tomu dojde, je velmi obtížné přesvědčit oběť o tom, že je stále oběť a útočník ji i nadále využívá.

I když před tímto druhem podvodu bezpečnostní společnosti i média pravidelně varují, stále existuje mnoho uživatelů, kteří na emaily odpovídají nebo dokonce rovnou zasílají peníze. Uvedeme několik příkladů následků.

3.5.1 Případ lékaře Jiřího Pasovského

Mělnický lékař Jiří Pasovský v únoru roku 2003, přímo na nigerijské ambasádě v Praze 6, zastřelil nigerijského konzula a postřelil recepčního. „Brzo vyšlo najevo, že Jiří Pasovský zabíjel, protože se nechal nachytat autory takzvaných nigerijských dopisů. Postupně jim poslal dva milióny dolarů, což tenkrát odpovídalo zhruba šedesáti miliónům korun. Půl miliónu pocházelo z rodinných úspor, zbytek si popůjčoval z různých zdrojů, včetně lichvářů. (...)

Pasovský byl po delších tahanicích odsouzen na pět let, ale do vězení nikdy nešel. Sehnal si potvrzení, že nemůže, je prý nemocný.“ [14]

3.5.2 Případ studentky Jaiyue Wang

V květnu 2007 spáchala dvacetitříletá studentka práv na Nothhinghamské univerzitě Jaiyue Wang, původem z Číny, sebevraždu kvůli nigerijským dopisům. Obdržela email o výhře v loterii v hodnotě 500.000 liber. Byla přemluvena k tomu, aby vynaložila svých 6.000 liber za zprostředkování zmíněné výhry. Následující měsíc ji našli oběšenou v kampusu univerzity.

3.6 Jak se bránit

- Neotvírejte emaily s podezřelým předmětem.
- Pokud náhodou otevřete podezřelý email, tak na něj neodpovídejte. Jen tím potvrdíte existenci své emailové adresy a objem spamu se zaručeně znásobí.

- Podvodníci se snaží přimět své oběti k rychlému bezmyšlenkovitému jednání. Nespěchejte.
- Neklikejte na žádné odkazy ve zprávě. Mohlo by dojít k instalaci škodlivého softwaru.
- Neposkytujte informace o své kreditní kartě, bankovním účtu či jiné údaje cizinci, který Vám pošle email.
- Neprovádějte finanční transakce na veřejném internetovém připojení. Vaše zprávy mohou být zachyceny a váš emailový účet napaden.

4 Implementace Nigerijských dopisů vzhledem k práci

Jak již bylo mnohokrát konstatováno, Nigerijské dopisy se řadí mezi nejrozšířenější internetové podvody. Na druhou stranu je zajímavé, že je společnost stále nebere dost vážně a neuvědomuje si následná rizika. To samé, ve velké míře, platí i u ostatních internetových podvodů.

4.1 Využití phishingu v práci

Protože nabízíme materiály na *Výukovém portálu Univerzity Palackého*, bylo by neprofesionální žádat od studentů finanční částky. Proto využijeme druhé „kombinované třídy“ internetových podvodů a pomocí phishingu realizujeme naši vizi.

> „Phishingové zprávy vypadají jako zprávy od důvěryhodných organizací, jako je PayPal, Česká pošta nebo vaše banka.
> ...
> Po kliknutí na odkaz v podvodném emailu jste přesměrováni na falešné stránky, kde vás útočníci nabádají k zadání citlivých informací o vašem účtu, což může vést ke krádeži identity.“[15]

5 Phishing

> „Dopátrat se v odborné literatuře k jednoznačné definici pojmu phishing je úkolem o poznání obtížnějším, než by se mohlo na první pohled zdát. Prakticky každá odborná publikace, výzkumná zpráva a článek jej totiž popisuje způsobem více či méně odlišným.“[16]

Phishing neboli **Rhybaření** je jedním z nejrozšířenějších a zároveň nejnebezpečnějších druhů internetového podvodu.

Slovo phishing vychází z anglického slova *fishing* a doslova znamená „ulovit citlivé informace popř. přihlašovací údaje od oběti, která se chytne“. Některá literatura uvádí, že „ph“ ve slově phishing pochází ze slova *phreaking* [1] , které se datuje ke konci 50. let a poprvé se objevilo ve Spojených státech.

Jedná se o podvodnou techniku, díky které šlo manipulovat s telefonním vedením. To přinášelo různé výhody jako volat zadarmo, surfovat po internetu taktéž zadarmo nebo dokonce odposlouchávat hovory ostatních.[17]

Princip phishingu spočívá v napodobení oficiálních webových stránek určité instituce tak, aby oběť, na odkazované stránce, zadala své přihlašovací údaje stejně jako na stránce oficiální. V našem případě se bude jednat o *Výukový portál* nabízející materiály ke studiu a především testy z minulých let, které nejsou lehce dostupné.

Odkazy na stránky se převážně rozesílají emailem a obsahují link, na kterém pak oběť přihlašovací údaje zadá. Vstupní email s odkazem a krátkým popisem, co stránky nabízí, studenty navede správným směrem.

Problém phishingu je ten, že podvržené stránky velmi často vypadají jako oficiální a je tak těžké je rozeznat od originálu.

Samozřejmě není podmínkou získat pouze přihlašovací údaje například do banky nebo na portál STAG. Na rozdíl od Nigerijských dopisů může útočníka motivovat více než jen finanční zisk. Stává se, že v některých případech jde i o slávu či případné uznání v jejich komunitě.

5.1 Historie

První zmínky o phishingovém útoku se jsou známy již v 90. léta 20. století. V roce 1987 byla technika phishingu detailně popsána v práci International HP Users Group, Interex.[18]

Termín „Phishing“ připisujeme v té době známému hackerovi a spammerovi Khanu C. Smithovi, který byl, v polovině 90. let, součástí warezové skupiny.[2]

První phishingové útoky zaznamenala společnosti AOL, která poskytuje internetové služby. Útoky byly mířeny na zaměstnance společnosti, kterým skupina warez ukradla osobní informace, hesla a další pomocí algoritmu pro náhodné generování kreditních karet. - Jediným kontrolovaným údajem bylo číslo kreditní karty, které navíc procházelo pouze jednoduchým a dobře známým testem validity, který však nebere v potaz ani vlastníka, ani skutečnou existenci karty s tímto číslem.[19]

Když se skupině podařilo vygenerovat skutečnou kartu, začali se podvodníci vydávat za zaměstnance AOL a dostali tak do kontaktu s ostatními pracovníky. Prostřednictvím internetové komunikace je žádali například o ověření hesla v rámci společnosti nebo o potvrzení fakturačních údajů.[20]

[1] Phreaking je kombinace slov *freak* = šílenec; *ph* - *phone* = telefon

[2] Wazerová skupina nelegálně šíří autorská díla po internetu. Členy označujeme jako počítačové piráty.

Problém se stal natolik velký, že společnost AOL začala přidávat upozornění do všech softwarů pro rozesílání zpráv o tom, že žádný zaměstnanec nemá právo žádat od jiného jeho údaje.

Aktualizací AOL bezpečnostních systému byl phishingový útok na společnost ukončen, ale útočníci si uvědomili, že další útoky je možné páchat ještě ve větším měřítku například na platební systémy.

První veřejně známý phishingivý útok proběhl v roce 2001. Mířil na webové stránky eCommerce, kdy se podvodnící snažili napadnout platební systém e-Gold. Tento pokus však skončil neúspěchem. Do roku 2003 si zaregistrovali několik domén, které připomínaly názvy známých společností jako PayPal nebo eBay.

K roku 2004 byl již phishing považován za plně rozvinutou ekonomiku zločinu, která poskytovala za hotovost součásti, které byly shromažďovány na konečný útok. Odhaduje se, že mezi květnem 2004 a květnem 2005 se vinou phishingu ztratilo 929 milionů USD.[21]

5.2 Současnost

V minulosti bylo poměrně jednoduché odhalit phishing. Mezi základní znaky se řadily například špatný překlad do rodného jazyka nebo doména neodpovídala doméně instituce, kde útok probíhal.

Dnes však můžeme narazit na téměř dokonalé phishingové zprávy, bez překladových chyb apod. Podvodníci jsou schopni vytvořit skoro přesné zprávy přímo na míru.

5.2.1 Phishingový útok na uživatele počítačové sítě UP

V roce 2018 sdružení CESNET[3] ve spolupráci s UP vytvořili simulaci phishingového útoku na zaměstnance a studenty univerzity.

> Simulovanému útoku na UP podlehla skoro desetina všech uživatelů. Přes dva tisíce studentů, akademických pracovníků a dalších pracovníků UP tak dobrovolně odevzdalo přístupové údaje ke svým datům fiktivnímu útočníkovi.[22]

5.3 Druhy Phishingu

Phishing považujeme za obecnou formu. Můžeme říct, že „obecný“ phishing není přizpůsoben jednotlivci, ale určité mase lidí. Od toho se též odvíjí i text zprávy - je neosobní, obsahuje (neúmyslné) chyby a odkaz na internet. Zpravidla neobsahuje žádnou přílohu.

[3]CESNET je sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní e-infrastrukturu pro vědu, výzkum a vzdělávání zahrnující počítačovou síť, výpočetní gridy, datová úložiště, prostředí pro spolupráci a nabízející širokou škálu služeb.

Druhy phishingu dělíme podle skupin lidí, na které míříme a podle způsobu komunikace, kterou používáme. Pro ukázku zde uvádíme nejznámější druhy phishinhu.

Pharming
: Je phishing, založený na manipulaci s DNS záznamy, kdy útočník odcizí DNS záznamy určitého webu a přesměruje je na podvodné stránky. Oběť netuší, že zadává své údaje na jiné IP adrese než je IP adresa webu, kam se chtěla dostat.

Spear phishing
: Jedná se o podvod zaměřený na konkrétní osobu. Zpravidla jde o osobu s určitým postem v určité společnosti. Neobsahuje žádný odkaz na internet a není zde požadováno zadání žádných údajů. Obsahuje pouze přílohu, která obsahuje škodlivý software.

Whaling
: Lov velryb je forma Spear phishingu, která se zaměřuje na vysoce postavené osoby (velryby) v rámci organizace. Podvodníci se snaží před kontaktováním „velryby“ zjistit co nejvíce informací, aby nebyl pochyb o jejich věrohodnosti. Často čerpají z internetových zdrojů jako je LinkedIn, Twitter nebo Facebook.

Clone phishing
: Jak vyplývá z názvu Clone phishing využívá skutečné zprávy, která je odeslána z důvěryhodné společnosti. Pachatel zprávu upraví tak, že nahradí nebo přidá odkaz, který oběť přesměruje na falešné stránky (klonují web). Zprávy se většinou odesílají jako hromadně více lidem.

Vishing
: Vishing *(Voice phishing)* je telefonický phishing. Pomocí technologie VoIP jde od obětí získat čísla účtů nebo jejich přístupové údaje. V poslední době se velice rozšířil. Jedná se o automat, který přečte oběti hlasovou zprávu, ve které ji vyzývá k činnosti se svým účtem a následně je mu zašle SMS s odkazem na podvodnou stránku.

5.4 Jak se bránit

- Neotvírejte emaily s podezřelým předmětem.
- Pokud náhodou otevřete podezřelý email, tak na něj neodpovídejte. Jen tím potvrdíte existenci své emailové adresy a objem spamu se zaručeně znásobí.
- Nikdy pomocí emailu nesdělujte své přihlašovací údaje – takové údaje emailem nejsou požadovány!

- Na svém emailovém účtu (popř. v poštovním klientu) mějte zapnutou ochranu proti spamu.
- Neklikejte na žádné přílohy ve zprávě. Mohlo by dojít k instalaci škodlivého softwaru.
- Neposkytujte informace o své kreditní kartě, bankovním účtu či jiné údaje cizinci, který Vám pošle email.
- Neprovádějte finanční transakce na veřejném internetovém připojení. Vaše zprávy mohou být zachyceny a váš emailový účet napaden.

Jak vidíme, jsou si zmíněné internetové podvody v mnoha bodech podobné či přímo stejné.

6 Webová část

Práce se dále zabývá vytvořením webové stránky. Bude určena pro sdílení literatury a studijních materiálů. Tyto materiály byly sesbírány z volně přístupných webů vyučujících, pracovišť apod.

Významnou částí těchto stránek bude kromě pokusu o přehlednost vyhledávání literatury a materiálů i sekce „Testy“ obsahující testy z různých předmětů. Podmínkou pro stažení těchto souborů je přihlášení následné zadání přihlašovacích údajů do přihlašovacího formuláře.

6.1 Použité technologie

Pro vytvoření webového formuláře jsme využili následující technologií. Jsou volené s ohledem na opakované použití, přehlednost kódu a přizpůsobené zařízením různé velikosti a rozlišení. V této podkapitole budou stručně popsány jednotlivé technické rysy.

HTML
: HTML je zkratka pro Hypertext Markup Language. Patří mezi základní stavební kámen každé webové stránky v systému World Wide Web. Vytváří obsah webové stránky. Obsah mohou tvořit například texty, obrázky nebo tabulky.

CSS
: Kaskádové styly využíváme pro styl vizuální prezentace webových stránek. Pomocí CSS je možné definovat rozložení prvků na stránce, okraje, barvy, písma a další vlastnosti. Tím nabývá samotný HTML kód nových možností.

PHP

Hypertext Preprocessor je skriptovací jazyk určený pro programování dynamických stránek. Jsou řešeny na straně serveru a k uživateli se dostane pouze výsledek nadefinování. Kombinuje HTML kód se zpracovanými skripty skriptovacího jazyka. Nejčastěji se PHP kód vkládá přímo do HTML kódu.

JavaScript

JavaScript je skriptovací, objektově orientovaný jazyk, který vytváří animace nebo efekty na stránkách. Na rozdíl od PHP se celá akce provádí na straně klienta, což má své výhody především pro server, který nemusí být zbytečně zatěžován.

JavaScriptový kód je možné umístit, stejně jako v případě CSS či PHP, do externího souboru a odvolávat se na něj.

MySQL

MySQL je v současnosti jedna z nejrozšířenější relační databáze na internetu. Struktura je tvořena soustavou propojených tabulek, kde jsou jednotlivé záznamy vkládány do řádků a sloupce určují jméno a datový typ.

6.2 Programátorská příručka

Webové stránky dělíme na dvě hlavní části. Jsou to:

1. Viditelná část, kam se dostane každý, kdo stánky navštíví
2. Zabezpečená část, jenž je zpřístupněna pouze přihlášeným uživatelům

Šablonu obou částí tvoří:

1. Menu: používáme jako rozcestník dalších pozic. Udává cestu k předmětům, testům, kontaktu a přihlášení.
2. Body: nejdůležitější část celých stránek, která je dynamicky měněna podle toho, na které stránce se zrovna nacházíme a tedy určuje obsah aktuální stránky.

Obrázek 5: Index - stránka

6.2.1 Viditelná část

Tato část je volně přístupná a pomocí ní se pokusíme nalákat studenty k otevření části, kde vyžadujeme citlivé informace. Nazýváme ji sekce Předměty, na kterou se student dostane po rozkliknutí kolonky „Předměty“ na hlavní stránce. Obsahuje pouze veřejně dostupné materiály, jaké vyučující sdílí na stránkách katedry. Převážně se jedná o literaturu, kterou používají k výuce látky. Jsou rozděleny podle aktuálně vyučujících předmětů od povinných po doplňující „dobrovolně povinné“ vyučující předměty nacházejících se v kolonce „Ostatní“.

Tato část dále obsahuje položku „Kontakt“, „Testy“ a „Přihlášení“. „Kontakt“ je formulář pro případné dotazy, tedy i osoba, která nebude přihlášena, může zanechat vzkaz v podobě emailu.

Obrázek 6: Předměty

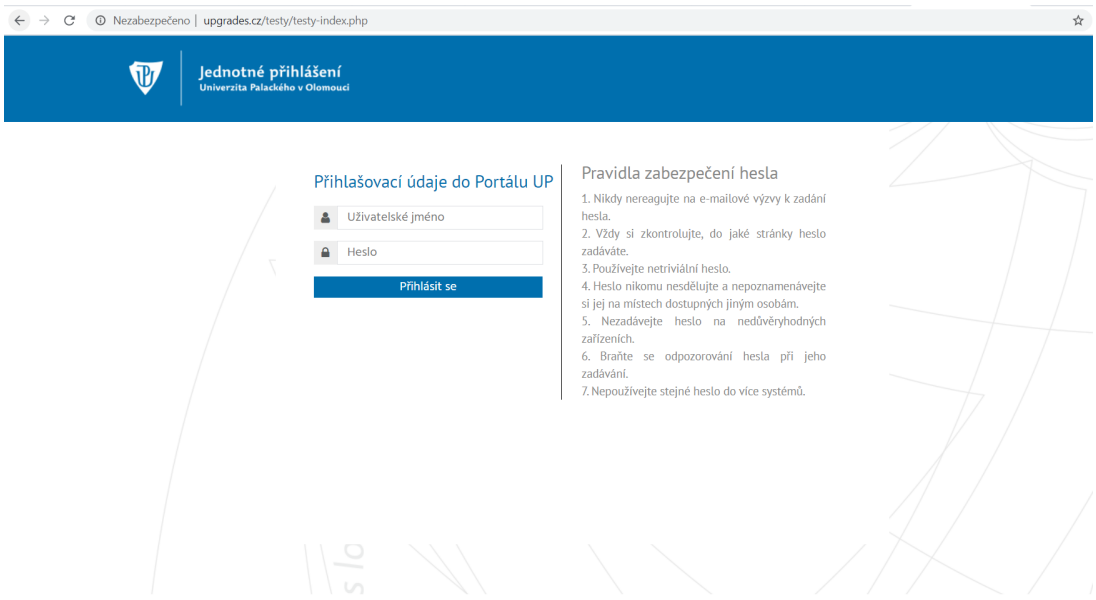
„Testy“ a „Přihlášení“ se ve viditelné části odkazují na stejný skript, ve kterém vyžadujeme přihlášení. Je to proto, aby nebylo možné se mu nijak vyhnout.

6.2.2 Zabezpečená část

Zabezpečená část pod názvem „Testy“ je určena pouze studentům, kteří jsou ochotni zadat své přihlašovací údaje. K přihlášení vyžadujeme údaje stejné, jako pro přihlášení do Stag.Upol.cz. V této části najdou kromě literatury i testy a materiály k zápočtům a zkouškám.

6.2.3 Přihlášení

Design přihlašovací stránky připomíná oficiální stránky STAGu. Měl by dotyčného utvrdit v tom, že je provozovaný univerzitou. Pokud se ale zaměříme i na zbytek okna, mělo by být jasné, že se jedná o podvod. V adresním řádku je web označen textem „Nezabezpečeno“.



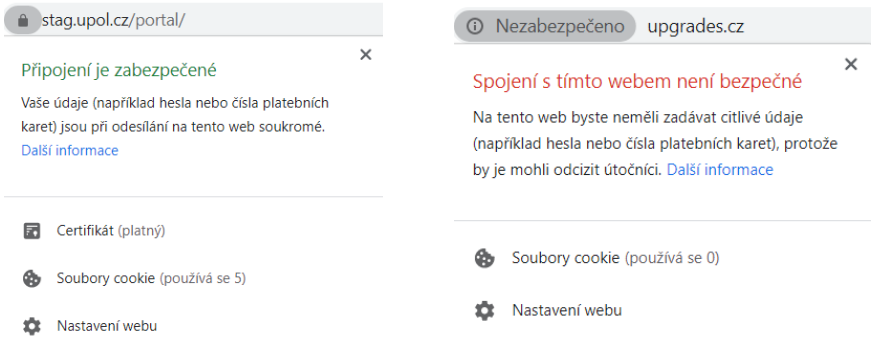
Obrázek 7: Přihlášení

Po následném přihlášení se údaje zapíší do databáze, ze které následně budeme čerpat informace. Jedná se o podvod a každý podvod je postaven na malé informovanosti a znalosti dotyčného problému. Přihlášení uživatele je spíše jeho registrace do systému.

6.2.3.1 Nezabezpečenost webu

Nezabezpečenost webu znamená, že stránky fungují na protokolu, který není zašifrován.

Pokud web nepoužívá šifrovaný protokol HTTPS (Hypertext Transfer Protocol Secure), potom veškerá komunikace, která na něm probíhá, není chráněna před případným zneužitím. Tedy ke sledování toku dat se dokáže dostat kdokoli cizí. To platí i pro přihlašovací údaje. Pokud dotyčný zadá své údaje na nezabezpečenou stránku, může je někdo jiný přečíst, sledovat nebo zaměnit.



(a) HTTPS (b) HTTP

Obrázek 8: Protokoly HTTPS a HTTP

Protokoly HTTP (Hypertext Transfer Protocol(s)), tedy nešifrované připojení, se řadí mezi identifikátory potenciálních hrozeb a problémů, protože veškerá data, která mezi uživatelem a serverem posílá, posílá v čitelné podobě. Navíc všeobecně panuje názor, že mít založené stránky pouze s protokolem HTTP není dobré.

Využití protokolu HTTP je, v našem případě, záměr. Grafické znázornění a spolu s textem „Nezabezpečeno“ v adresním řádku by mělo dostatečně vypovědět o věrohodnosti webu a uživatele tak dostatečně varovat.

6.2.4 Databáze

Databáze je stěžejní struktura, která zapisuje uživatele stránek v rámci přihlášení a přidělí jim další přístup. Pro potřeby aplikace postačí databáze obsahující jednu tabulku jménem Loginsystem, do které jsou zapisovány pouze tři údaje a to: login, heslo a datum přihlášení. Tyto údaje postačují ke zneužití účtů uživatelů.

Atribut	Typ
username	integer
password	varchar
datetime	datetime

Tabulka 1: Databáze

7 Mailová část

Mailová část se bude zabývat sestavením poštovního serveru, ze kterého budeme rozesílat emaily na vybrané studentské účty.

Pro reprezentaci jsme vybrali mailový sever Postfix. Ten nepotřebuje žádné speciální knihovny ani nastavení a lehce se ovládá. Má však i svoje slabiny. Jeho největší nevýhodou je fakt, že kdokoliv může, při odesílání emailu, použít jakoukoli adresu tedy i takovou, která mu například vůbec nepatří. Pro naše účely se jedná o výhodu, ale jako internetová služba v tomto případě selhává.

Email bude prvním navázáním kontaktu se studentem. Díky krátkému vysvětlení, proč email odesíláme a k čemu jsou webové stránky vytvořeny, bude na závěr uveden i jejich odkaz.

7.1 Poštovní server

Pro přenos elektronické pošty slouží počítačový program Mail Transport Agent neboli **MTA**. Mezi nejznámější přepravce elektronické pošty patří Postfix, SendMail nebo Microsoft Exchange Server. Postifx je bezplatný poštovní server používaný jakožto alternativa Sendmailu. Je rychlý, snadno spravovatelný a bezpečný. Pro využití v této práci pracujeme právě s mailovým serverem Postfix.

Přeprava mailů je realizována **SMTP**, internetovým protokolem, který přenáší zprávy elektronické pošty mezi přepravci elektronické pošty.

Samotná přeprava zpráv probíhá tak, že uživatel vytvoří mail v programu **MUA**. Mail User Agent slouží k přístupu a správě mailu uživatelem. Podrobnosti o přenosu zprávy jsou zapisovány a upřesněny protokolem SMTP. Email je předán nejbližšímu přepravci MTA, který podle doménové části mailové adresy cílového uživatele zjistí, kam zprávu předat. Jakmile email doručí do cílového počítače, je zpráva předána programu **MDA**, který jej zapíše do příchozí složky elektronické pošty oprávněného uživatele.

> Simple Mail Transfer Protocol je internetový protokol určený pro přenos zpráv elektronické pošty mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli přistupovat (vybírat zprávy) buď přímo na serveru, nebo z jiného počítače pomocí protokolů jako POP3 nebo IMAP.“[23]

7.1.1 Implementace

Jakožto program pro přepravu elektronické pošty, Postfix přijímá a odesílá zprávy přes internet pomocí protokolu SMTP.

Instalace na operačním systému Linux je poměrně jednoduchá a stačí pouze zadat příkaz:

```
sudo apt install postfix
```

Konfigurace Postfixu jsou uloženy v souboru **/etc/postfix/main.cf**. Důležitou částí tohoto konfiguračního souboru je sekce s příkazy:

Zdrojový kód 1: Konfigurace Postfixu 1

```
myhostname =
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination =
relayhost =
mynetworks =
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
```

Určité příkazy jsme v našem případě dodefinovali podle potřeb na:

Zdrojový kód 2: Konfigurace Postfixu 2

```
myhostname = klugve00.inf.upol.cz
mydestination = $myhostname, klugerova.student.inf-
.upol.cz
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104
[::1]/128
inet_protocols = all
home_mailbox = Maildir/
virtual_alias_maps = hash:/etc/postfix/virtual
```

To jsou postačující informace k jednoduchému přijímání a odesílání zpráv přes Postfix. Konfigurace poštovního serveru je ale složitější.

Odesílání zpráv následně zadáváme příkazem:

Zdrojový kód 3: Příkaz pro rozesílání emailu 1

```
cat ~/test_message | s-nail -s 'Predmet' -r (od koho) komu
```

7.1.2 Program s-nail

Přijímání zprávy zobrazujeme pomocí:

```
s-nail
```

Jedná se o doplnění poštovního serveru Postfix, které dělí emaily do složek a umožňuje uživatele s nimi dále nakládat. Umí zpracovávat jak odeslanou, tak i doručenou poštu. Balíček nabízí množství funkcí pro manipulaci s emaily. Stlačením „?“ uvedeném vedle verze programu se otevřou možnosti, kterými s-nail disponuje např. - klávesa „q“ pro ukončení. Po stlačení klávesy „ENTER“ se zobrazí, kolik příchozích emailů schránka obsahuje.

Instalace programu s-nail je opět velice jednoduchá. Stačí zadat příkaz:

```
sudo apt install s-nail
```

Protože ale hlavním záměrem této práce je získání osobních údajů, které obdržíme hned po té, co se jakýkoliv student přihlásí do sekce „Testy“ pomocí přihlašovacích údajů do STAGu, je důležité, abychom upozornili na opravdové nebezpečí, které při takových situací může nastat.

8 Statistiky

Dříve bylo možné vyselektovat studenty podle určitých oborů přímo na portálu STAG, ale dnes již tomu tak není. Po zavedení GDPR[4] je složitější vyhledávat údaje na ověřených stránkách, jako může být například STAG, ale internet je mocný nástroj, tedy pokud chceme o určité osobě najít informace, možnost vždy se najde.

> „Osobní údaje jsou ve stávající směrnici z roku 1995 i v GDPR definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.
>
> Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam.
>
> Obecné nařízení věnuje speciální pozornost zpracování zvláštních kategorií osobních údajů, jimiž jsou údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení. Do kategorie citlivých údajů nařízení nově zahrnuje genetické, biometrické údaje a osobní údaje dětí. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.“[24]

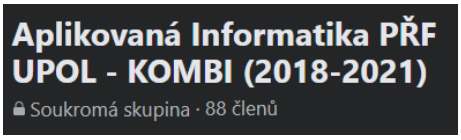
Mnohem jednodušší a efektivnější cesta, navíc bez povinnosti se přihlásit do univerzitního systému, je využití sociálních sítí. Stačí se „Přidat“ do určité skupiny například na Facebooku, počkat na následné schválení správcem skupiny a vyhledávání je u konce.

Vytvoření a nastavení účtu na sociálních sítích zabere pár minut. Do vyhledávače stejně tak není složité zadat klíčová slova, které se snažíte objevit. V našem případě šlo převážně o „informatika upol“, „informatika přf upol“ „matematika upol“, „matematika přf upol“.

Přidání do určité skupiny, funguje na bázi důvěry, to v praxi znamená, že nikoho moc nezajímá, kdo jste a jaký je Váš záměr - jednoduše odsouhlasí žádost. Po přijetí žádosti se kromě jiných informací především zpřístupní seznam členů.

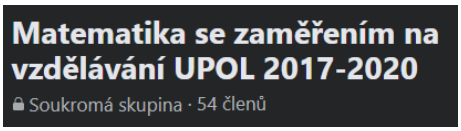
Pro ilustraci uvádíme příklady skupin vyskytující se na Facebooku.

[4] Obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) je revoluční legislativa EU, která výrazně zvyšuje ochranu osobních dat občanů.



(a) Apl = 88 členů

(b) Inf + Apl = 121 členů



(c) M = 54 členů

(d) M = 40 členů

Obrázek 9: Příklady soukromých skupin na Facebooku

8.1 E-mailové adresy studentů UP

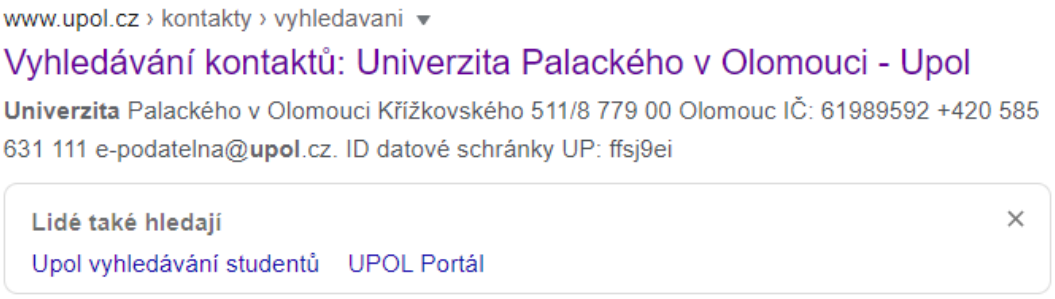
Není složité zjistit univerzitní email dotyčného, pokud patří do některé ze skupin, vytvořených pro zájmy univerzity, vyskytujících se na sociálních sítích.

Struktura univerzitního emailu vypadá následovně:

```
portalID@upol.cz                (1)
jmeno.prijmeni0*@upol.cz        (2)
```

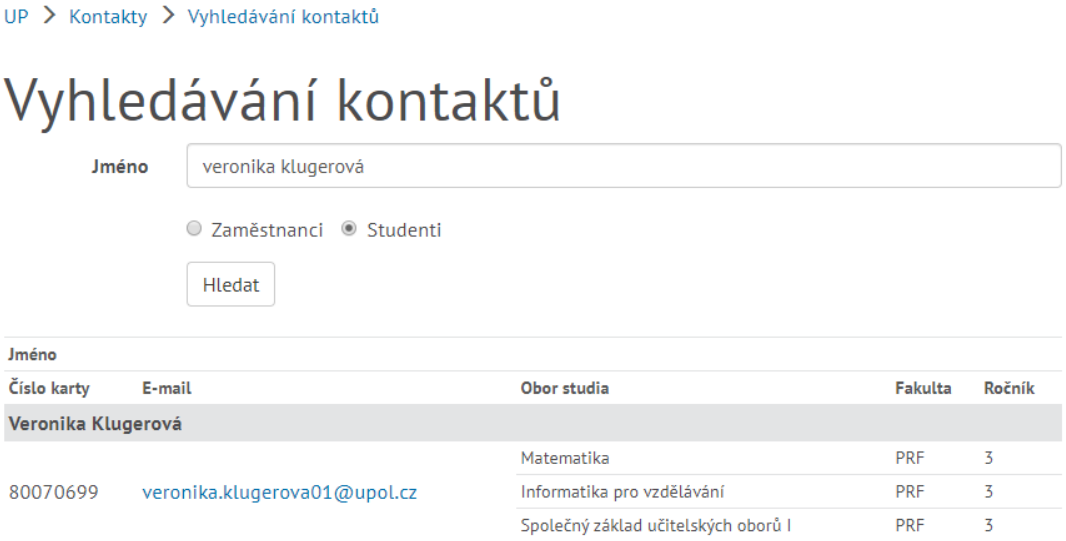
Vzor pro strukturu (1) uvádí Wiki - Upol nebo CVT, ale k tomu je zapotřebí znát ID studenta. To se skládá z prvních 4 písmen příjmení, prvních 2 písmen z křestního jména a dvojmístného čísla, které se teoreticky může nacházet v rozmezí od 00 do 99.

Po zadání slov „univerzitní email upol“ do vyhledávače, je přibližný počet výsledků odhadován na: 89 900 (0,39 s). Mezi nimi se nachází i odkaz na vyhledávání kontaktů přímo v rámci univerzity.



Obrázek 10: Vyhledávání

Po přesměrování na stránku stačí zadat jméno dotyčného, které známe ze sociálních sítí a tak zjistit jeho email. Případně se můžeme odkazovat pouze na křestní jméno nebo příjmení, ale postup je zdlouhavější.



Obrázek 11: Filtrování podle jména

Pak už stačí pouze rozeslat email, který navede studenty na naše stránky. Postup zprovoznění mailového serveru jsme zmínili v kapitole 7.1.1 a odesílání zprávy ve zdrojovém kódu 3.

8.2 Web a vstupní email

Webové stránky jsou k dispozici na: http://upgrades.cz.

Email rozeslaný studentům:

Díky mailovému serveru Postfix je zpráva rozesílána z fiktivního účtu jménem *„administrace@upgrades.cz“*, které někomu může (i přes výtky) připomínat oficiální adresu *„administrace@upol.cz“*. Pokud by se tak nestalo, jako předmět zprávy uvádíme *„Nový výukový portál UP“*.

Ve zprávě používáme odkaz na zmíněné stránky, ale bez zabezpečujícího certifikátu, který považujeme za ukazatel toho, že něco není úplně v pořádku.

8.3 Počet přihlášení

Email byl poslán 50-ti studentům. Studenty jsme náhodně vybrali na sociální síti bez toho, abychom ověřovali, zda-li daný obor stále studují nebo studium již ukončili.

Zaměřili jsme se především na konec bakalářského studia studentů matematiky a informatiky. Mezi to řadíme i kombinace matematiky s ostatními obory a i zaměření informatiky.

Nový výukový portál UP

administrace@upgrades.cz <administrace@upgrades.cz>
Po 18.05.2020 9:34
Komu: Klugerova Veronika <veronika.klugerova01@upol.cz>

Vážené studentky, vážení studenti,

tým studentů, oborů matematika a informatika, pro vás vytvořili nový výukový portál UPgrades.

Je určen pro sdílení studijních materiálů jako jsou SKRIPTA, PREZENTACE, UČEBNICE, jiná použitá LITERATURA nebo TESTY nasbírané z předchozích let.
Najdete zde materiály na zkoušky, zápočty i státnice.

odkaz: http://upgrades.cz/

Prozatím se portál otevírá pouze pro studenty MATEMATIKY a INFORMATIKY, kterým byl rozeslán tento email.

Budeme rádi za zpětnou vazbu.

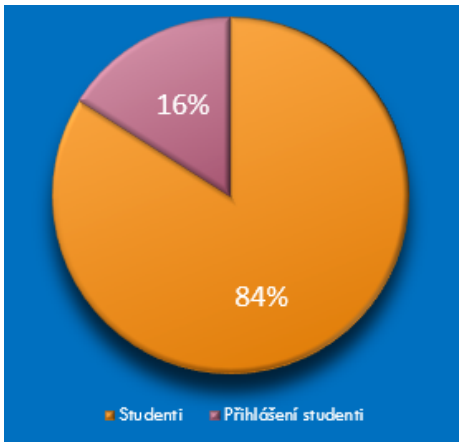
Univerzita Palackého
Team UPgrades

Obrázek 12: E-mail rozeslaný studentům

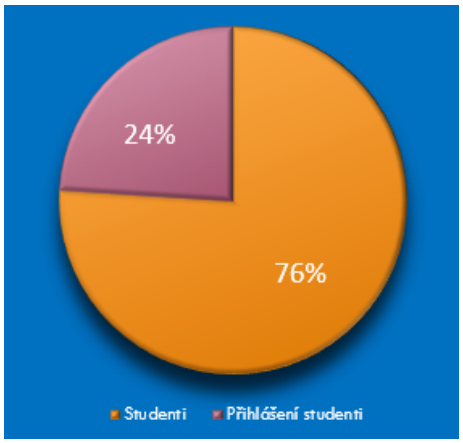
Počet	Obor
5	matematika a informatika
25	matematika a její kombinace (Fyzika, Biologie, Chemie,...)
20	aplikovaná informatika

Tabulka 2: Počet studentů vybraných z určitých oborů

Největší vlna přihlášení proběhla v 24 hodinách po odeslání emailu, kdy jsme získali přihlašovací údaje od 8 studentů - tj. 16%. Pokud bychom měli brát přihlášení bez duplikátů, tak se v průběhu prvních 9-ti dnů přihlásilo celkem 12 studentů - tj. 24% přihlášení z celkového počtu 50-ti osob.



(a) 16% během 24 hodin



(b) 24% během 9-ti dnů

Obrázek 13: Celkový počet vs. přihlášení

Následně se počet zastavil, ale náhodný výběr prokázal, že studenti zadávají

oficiální údaje do portálu. Tedy přesně ty údaje, které potřebujeme.

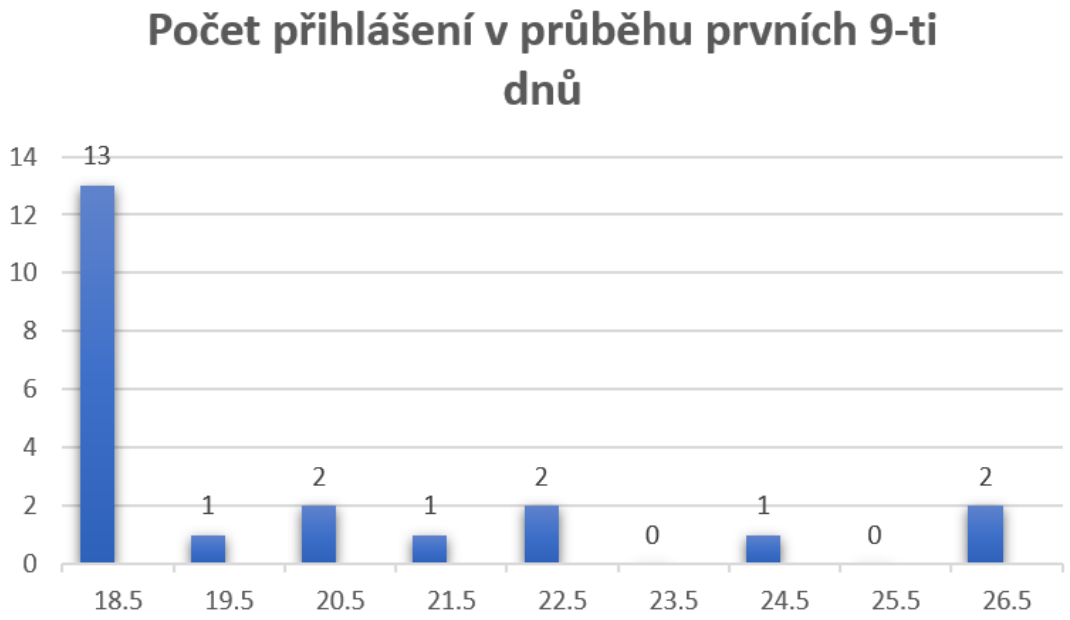
Většina studentů, kteří se na web přihlásili jsou studenti kombinace matematiky, ale najdou se i ti, kteří končí studium oboru Aplikovaná informatika.

Obor	Počet přihlášených studentů
matematika a informatika	2
matematika a její kombinace	8
aplikovaná informatika	2

Tabulka 3: Počet přihlášených studentů z určitých oborů

8.4 Četnost přihlášení

Někteří studenti navštívili web vícekrát. Nejvíce přihlášení je evidováno k prvnímu dni, kdy počet záznamů dosáhl čísla 13. Dále bohužel počet návštěv upadá a pohybuje se kolem 1-2 přihlášení za den.



Obrázek 14: Četnost přihlášení během prvních 9-ti dnů

8.5 Oslovení dotyčného studenta

Pro ilustraci jsme oslovili jednoho náhodného studenta, kterého jsme požádali, aby nám zodpověděl následující otázky.

Je jím studentka 3. ročníku s akreditací učitelství matematiky a učitelství deskriptivní geometrie, která souhlasila se zodpovězením následujících otázek.

Proč jsi otevřela odkaz?
Otevřela jsem odkaz, protože se mi nápad velmi líbil a zajímalo mě, co daná stránka obsahuje a zda je možnost něco sdílet. Také mě k tomu vedlo i to, že v poslední době byl umožněn přístup do více knihoven, tak jsem se nad tím ani nepozastavila. Dále jsou na internetu stránky sestavené z materiálů vyučujících a bakalářských prací - jako například www.karlin.mff.cuni.cz.

Přišly ti stránky vzhledově podobné s dalšími stránkami UP?
Když nad tím tak přemýšlím, tak to byl i podobný vzhled, jaký má UPlikace. Otevírala jsem to z mobilu...

Proč jsi se přihlásila?
Stránka na přihlášení vypadala vážně jako portál. Dokonce jsem na to hledala i odkaz v UPlikaci, ale bohužel jsem jej nenašla. Shibolet, Kramerius nebo Moodle - tam všude se teď přihlašuje stejnými údaji - to je možná nevýhoda toho, že jsou teď všude údaje stejné, člověk přestane dávat pozor.

Když jsem se ti ozvala ohledně průzkumu, co se ti honilo hlavou, když si přišla na to, že ti bylo odcizeno tvoje heslo? Napadlo tě vůbec, že se něco takového může stát?
Přemýšlela jsem, co a jak by vlastně šlo zneužít. Kam všude se s těmito údaji dá přihlásit. Dávám si pozor na maily žádající o změnu hesla atd., ale tady jsem to nečekala.

Byla bys pro takový portál ke sdílení materiálů? Pokud ano, co bys změnila na stávajících a přidala k novým? Kromě anonymního sdílení materiálů samotnými studenty.
Určitě bych pro takový portál byla, dle mého by bylo dobré sem zahrnou i užitečné odkazy na jiné ověřené internetové stránky. A nahrát obhájené bakalářské práce.

Možná bych k plánovanému portálu přidala i příběh, jak vlastně vznikl (jako podvodná stránka) a na co si dát pozor, případně čeho si všímat. A kde o této problematice hledat další informace.

Všímáš si zabezpečenosti stránek?
Řeším to tam, kde bych měla zadávat číslo kreditní karty, nebo telefon. Jinak bych se asi nikam nedostala, například když si hledám materiály do školy, tak to nekontroluji a přes internet věci nenakupuji. Jen jízdenky na vlak přes aplikaci Můj vlak. A kredit přes aplikaci Můj T-Mobile.

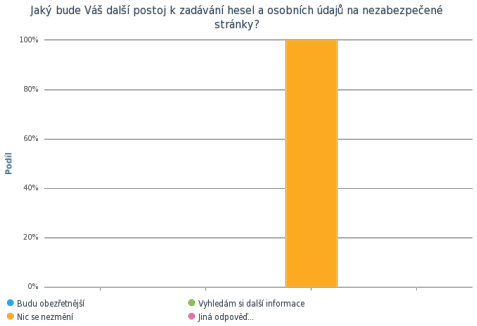
Jaký bude tvůj další postoj k zadávání hesel a osobních údajů na nezabezpečené stránky?
Dám si větší pozor, ale člověk stále riskuje a nikdy si nemůže být jistý, že je všechno v pořádku.

Stále člověk riskuje, když odsouhlasí podmínky nějaké aplikace. Kolikrát jsem se chtěla například přihlásit do nějaké soutěže od T-Mobile a po přečtení podmínek jsem si to rozmyslela, protože to bylo podmíněno založením paušálu, nebo jsem prostě podmínky nesplňovala, tak by to bylo zbytečné.

8.6 Dotazník

Stejné otázky jsme položili prostřednictvím dotazníku i ostatním. Kvůli malému počtu zúčastněných (5) jsme vybrali dva grafy. Stěžejní pro nás byl postoj k posledním dvěma tj.
(a): Všímáte si zabezpečenosti stránek?
(b): Jaký bude tvůj další postoj k zadávání hesel a osobních údajů na nezabezpečené stránky?

(a) Zabezpečenost stránek



(b) Další postoj k zadávání hesel a osobních údajů na nezabezpečené stránky

Obrázek 15: Celkový počet vs. přihlášení

U otázky (a) jsme vybraly možné odpovědi: **ANO, NĚKDY, NE**
- podle výsledků se 80% zúčastněných **NĚKDY**, načež zbylých 20% se na zabezpečenost stránek vůbec nedívá.

U otázky (b) bylo na výběr: **BUDU OBEZŘETNĚJŠÍ, VYHLEDÁM INFO, NIC SE NEZMĚNÍ, JINÁ**
- zde podle údajů z dotazníku rovných 100% odpovědělo, že **se nic nezmění**. Nicméně podle srovnání s druhým grafem to není tak závažné.

8.7 Upozorňující email

Na závěr ještě všem studentům, kteří se na stránky přihlásili, posíláme zprávu o útoku i s obecnými doporučeními, jak se, aspoň částečně, bránit před internetovými podvody a jak si správně nastavit heslo.

Zneužití hesla do portálu Stag

administrace@upgrades.cz <administrace@upgrades.cz>
Ne 02.08.2020 21:04
Komu: Klugerova Veronika <veronika.klugerova01@upol.cz>

Vážené studentky, vážení studenti,

nedávno jste se přihlásili na podvodnou stránku http://upgrades.cz/, díky níž jste svěřili své přihlašovací údaje do nesprávných rukou. Stránky Upgrades.cz byly vytvořeny za účelem odcizení hesel v rámci bakalářské práce.

Práce pojednává o specifickém druhu internetových podvodů a o vytvořených webových stránkách, nabízející výukové materiály. Sekce s přihlašovacím formulářem připomíná zadávání přístupových údajů do oficiálního IS/STAGu avšak ve skutečnosti údaje odesílá do jiné databáze.

Vaše osobní informace nebudou nikde zveřejněny a z databáze budou veškerá data odstraněna.

Obecné doporučení, jak se vyvarovat phishingu ▼
1. Neotvírejte emaily s podezřelým předmětem
   - jen tím potvrdíte existenci své e-mailové adresy a objem spamu se zaručeněznásobí.
2. Nikdy pomocí emailu nesdělujte své přihlašovací údaje
   – takové údaje e-mailem nejsou požadovány!
3. Na svém e-mailovém účtu (popř. v poštovním klientu) mějte zapnutouochranu proti spamu.
4. Neklikejte na žádné přílohy ve zprávě
   - mohlo by dojít k instalaci škodlivého softwaru
5. Neposkytujte informace o své kreditní kartě, bankovním účtu či jiné údaje
6. Neprovádějte finanční transakce na veřejném internetovém připojení
   - vaše zprávy mohou být zachyceny a váš e-mailový účet napaden

Obecné doporučení, jak by mělo heslo správně vypadat ▼
1. mělo být dostatečně dlouhé, složité a přitom snadno zapamatovatelné
   - nahrazujte písmena znaky, např. E = 3, S = $, B = 8 apod.
   - nemělo by mít logický vztah k uživateli (přezdívka, rodné číslo apod.),
2. mělo by obsahovat velká a malá písmena, čísla a speciální znaky
   - heslo skládající se z 15 náhodných písmen a číslic je přibližně 33 tisíckrát bezpečnější než heslo tvořené 8 znaky z celé klávesnice
   -heslo bude mnohem silnější, když vyberete ze všech dostupných symbolů na klávesnici, včetně interpunkčních znamének

Pro jakékoli dotazy mě prosím kontaktujte na email: administrace@upgrades.cz.
Vaše otázky ráda zodpovím.

Děkuji

S pozdravem
Veronika Klugerová

Obrázek 16: E-mail rozeslaný studentům 2

Závěr

Cílem bakalářské práce bylo upozornit na problematiku stále aktuálních internetových podvodů.

Pro simulaci podvodu využívám techniky phishingu, který patří mezi nejnebezpečnější internetové podvody vůbec. Nigerijské dopisy a phishing mají společnou věc a to to, že se pomocí falešné elektronické komunikace snaží získat citlivé údaje oběti a následně je zneužít. Nepracují jako v našem případě tedy tak, že email rozešlou pouze pár vybraným lidem, ale zprávu rozesílají mnohem větší mase.

Ze získaných dat z falešného univerzitního webu lze usoudit, že lidé stále nevěnují dostatečnou pozornost ochraně svých osobních údajů.

Z celkového počtu náhodně oslovených osob, vybraných ve skupinách na sociálních sítích, jsme obdrželi údaje od 24% z nich 9-ti dnů. I přes to, že návštěvnost webu nebyla nijak závratná, jedná se o poměrně vysoké číslo.

Kdyby byl útočník opravdový, měl by přístup například k rodným číslům nebo kreditním kartám 12-cti netušících osob. Mezi přihlášené patří převážně studenti kombinace matematiky, ale přihlašovací údaje unikly i aplikovaným informatikům!

Pokud by se tento experiment převedl na celou univerzitu jako simulovaný útok v podkapitole 5.2.1, tedy přibližně na 26 000 osob, mohlo by být podle mých výsledků zneužito 4 160 přístupových údajů za prvních 24 hodin. Při úspěšnosti 24% se jedná o 6 240! Je nutné ale podotknout, že toto číslo je i po případném započítání negativních vlivů stále vysoké a nepravděpodobné číslo. Zároveň nesmíme zapomenout na ten fakt, že simulovanému phishingovému útoku UP podlehlo přes 2 000 lidí - 10%.

Domnívám se, že je důležité stále dokola opakovat a zdůrazňovat, jak jsou internetové podvody nebezpečné, vytvářet tak různé simulace, díky kterým by případy jako v kapitole 3.5 vymizely případně jednou, by tak zmizely i snahy podvodníků. Z provedeného průzkumu je patrné, že jsou lidé neopatrní a neověřují si, kam zadávají svoje údaje. Často neví, co kontrolovat a v neposlední řadě si ani neuvědomují, o jaké informace osobního charakteru mohou přijít.

Dle mého názoru se to děje proto, že jsou internetové podvody všeobecně tak známe, že jim lidé nevěnují dostatečnou pozornost. Pro zvýšení povědomí by bylo vhodné například zavést přednášky o této problematice s možností diskuze, provádět častěji fiktivní útoky, jako 5.2.1. Co se týče studentů, myslím, že by ocenili i zapojení v případném experimentu. Ne jako „oběti“, ale jako součást skupiny, která tento podvod realizuje. Tyto skupiny by se následně mohly zabývat internetovými podvody dopodrobna, zkoumat je, případně se pokusit o jejich omezení tzn. například přijít na řešení, jakým by bylo možné internetové podvody rozeznat (na úrovni prohlížeče). Dále by se mohly ujmout seminářů, přednášek. Mohly by pořádat různé workshopy a akce spojené s touto tématikou - třeba jako akce Hackathon nebo KYPO, což je brněnská skupina, která spadá pod Masarykovu univerzitu přesněji Ústav výpočetní techniky a zabývají se simulací a zkoumaní v podstatě jakékoli „digitální hrozby“.

Conclusions

The aim of the bachelor's thesis was to draw attention to the issue of still current Internet fraud.

To simulate a fraud, I use phishing techniques, which are among the most dangerous Internet frauds ever. Advance-fee scam and phishing have in common that they use false electronic communication to obtain the victim's sensitive data and then misuse it. They do not work as in our case, so that they send the email only to a few selected people, but they send the message to a much larger mass.

From the data obtained from the fake university website, it can be concluded that people still do not pay enough attention to the protection of their personal data.

From the total number of randomly contacted persons, selected in groups on social networks, we received data from 24% of them for 9 days. Despite the fact that the website traffic was not dizzying, it is a relatively high number.

If the attacker were real, he would have access to, for example, the birth numbers or credit cards of 12 unsuspecting people. Among those registered are mostly students of the combination of mathematics, but the login data also escaped to students of applied computer science!

If this experiment were transferred to the whole university as a simulated attack in the subchapter 5.2.1, approximately 26,000 people, according to my results, 4,160 access data could be misused in the first 24 hours. With a success rate of 24%, this is 6,240! However, it should be noted that this number is still high and unlikely even after the possible inclusion of negative effects. At the same time, we must not forget the fact that over 2,000 people succumbed to the simulated UP phishing attack - 10 %.

I think it is important to keep repeating and emphasizing how dangerous internet fraud is, to create various simulations, thanks to which cases like in the chapter 3.5 would disappear once, the efforts of fraudsters would disappear. The survey shows that people are careless and do not check where they enter their data. They often do not know what to check and, last but not least, do not even realize what personal information they may lose.

In my opinion, this is because internet scams are so well known that people do not pay enough attention to them. To raise awareness, it would be appropriate, for example, to introduce lectures on this issue with the possibility of discussion, to carry out more often fictitious attacks, such as 5.2.1. As for the students, I think they would appreciate and engage in a possible experiment. Not as "victims", but as part of the group that carries out this scam. These groups could then deal with Internet fraud in detail, investigate it, or try to reduce it, e.g. to come up with a solution to detect Internet fraud (at the browser level). They could also attend seminars, lectures. They could organize various workshops and events related to this topic - such as Hackathon events or KYPO, which is a Brno's group that falls under Masaryk University, more precisely the Institute of Computer Science, and deals with the simulation and investigation of essentially any "digital threat".

Literatura

[1] *Trestní zákoník č. 40/2009 Sb., § 209 paragraf odst.1 - Podvod, ISSN 1801-8688.* [online]. [cit. 2019-2-1]. Dostupný z: ⟨https://zakony.kurzy.cz/40-2009-trestni-zakonik/paragraf-209/⟩.

[2] S.R.O., AVAST Software. *Co je sociální inženýrství? Jak ho rozpoznat a zabránit útokům | Avast* [online]. [cit. 2016--]. Dostupný z: ⟨https://www.avast.com/cs-cz/c-social-engineering/⟩.

[3] S.R.O., AVAST Software. *Co je malware a jak ho odstranit | Ochrana proti malware | Avast* [online]. [cit. 2016--]. Dostupný z: ⟨https://www.avast.com/cs-cz/c-malware/⟩.

[4] XMAN.CZ, Radomír Dohna. *Průvodce světem podvodů: trik „španělský vězeň" funguje dodnes* [online]. [cit. 2017-9-1]. Dostupný z: ⟨https://www.idnes.cz/xman/styl/podvod-e-mail-z-nigerie-spanelsky-vezen.A170902_161726_xman-styl_fro⟩.

[5] CONTRIBUTORS, Wikipedia. *Eugène François Vidocqs* [online]. [cit. 2020--]. Dostupný z: ⟨https://en.wikipedia.org/w/index.php?title=Eug%5C%C3%5C-%A8ne_Fran%5C%C3%5C%A7ois_Vidocq&oldid=971971077⟩.

[6] AGI, Ultrascan. *419 Advance Fee Fraud Statistics* [online]. [cit. 2016--]. Dostupný z: ⟨https://www.ultrascan-agi.com/assets/files/Pre-Release-419_Advance_Fee_Fraud_Statistics_2013-July-10-2014-NOT-FINAL-1.pdf⟩.

[7] *Nigerijské dopisy - Jak na webové stránky.* [online]. [cit. 2015-9-18]. Dostupný z: ⟨http://timehosting.cz/nigerijske-dopisy/⟩.

[8] *Získání majetku falešnými záminkami; Kapitola 38, Podvádění, 419.* [online]. [cit. 2006--]. Dostupný z: ⟨https://www.nigeria-law.org/Criminal⟩.

[9] AGI, Ultrascan. *Smart People Easier To Scam, 419 Advance Fee Fraud Statistics 2013* [online]. [cit. 2014--]. Dostupný z: ⟨https://www.ultrascan-agi.com/assets/files/Pre-Release-419_Advance_Fee_Fraud_Statistics_2013-July-10-2014-NOT-FINAL-1.pdf⟩.

[10] MORBURRE, Wikimedia Commons. *Example of "Nigerian scam", 1995* [online]. [cit. 2014-1-18]. Dostupný z: ⟨https://commons.wikimedia.org/wiki/File:NigerianScam.jpg⟩.

[11] ROBOT, Marvin the. *Sometimes Nigerian spam comes with near-constant belly laughs* [online]. [cit. 2016-6-30]. Dostupný z: ⟨https://usa.kaspersky.com/blog/funny-email-scam/7349/⟩.

[12] PIERS, Chris. *Incredible Nigerian Scam Involves an Astronaut Lost in Space* [online]. [cit. 2016-2-16]. Dostupný z: ⟨https://www.iflscience.com/space/scam-email-about-nigerian-astronaut-lost-space-hilarious/⟩.

[13] 419 SCAM, Alert. *Facebook Lottery scam email from Mr. Mark Zuckerberg Facebook CEO w.sedlar@utanet.at cdepartment2019@gmail.com* [online]. [cit. 2019-12-11]. Dostupný z: ⟨https://e-mailscamalerts.blogspot.com/2019/12/facebook-lottery-scam-email-from-mr.html⟩.

[14] JOHN, Radek. *Tajemství nigerijských dopisů* [online]. [cit. 2012-7-24]. Dostupný z: ⟨https://psychologie.cz/tajemstvi-nigerijskych-dopisu/⟩.

[15] S.R.O., AVAST Software. *Co je phishing? | Vyhněte se e-mailovým podvodům a útokům | Avast* [online]. [cit. 2016--]. Dostupný z: ⟨https://www.avast.com/cs-cz/c-phishing⟩.

[16] JANÁČEK, Bc. Radek. *Analýza metod detekce webových stránek s phishingovým obsahem na úrovni perimetru sítě* [online]. [cit. 2014--]. Dostupný z: ⟨https://is.muni.cz/th/dyi2v/Diplomova_prace.pdf⟩.

[17] WIKIPEDIE. *Phreaking* [online]. [cit. 2020--]. Dostupný z: ⟨https://cs.wikipedia.org/w/index.php?title=Phreaking&oldid=17179999/⟩.

[18] WIKIPEDIE. *Phishing — Wikipedie: Otevřená encyklopedie* [online]. [cit. 2020--]. Dostupný z: ⟨https://cs.wikipedia.org/w/index.php?title=Phishing&oldid=18560286⟩.

[19] JANÁČEK, Bc. Radek. *Analýza metod detekce webových stránek s phishingovým obsahem na úrovni perimetru sítě* [online]. [cit. 2014--]. Dostupný z: ⟨https://is.muni.cz/th/dyi2v/Diplomova_prace.pdf⟩.

[20] MORAMARCO, Stephen. *Phishing Definition And History* [online]. [cit. 2020--]. Dostupný z: ⟨https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/#gref⟩.

[21] WIKIPEDIE. *Phishing — Wikipedie: Otevřená encyklopedie* [online]. [cit. 2020--]. Dostupný z: ⟨https://cs.wikipedia.org/w/index.php?title=Phishing&oldid=18560286/⟩.

[22] ŽURNÁL ONLINE, redakce. *Phishingový útok na uživatele počítačové sítě UP* [online]. [cit. 2018-4-28]. Dostupný z: ⟨https://www.zurnal.upol.cz/nc/zprava/clanek/phishingovy-utok-na-uzivatele-pocitacove-site-up/⟩.

[23] WIKIPEDIE. *Simple Mail Transfer Protocol* [online]. [cit. 2019-9-18]. Dostupný z: ⟨https://cs.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol⟩.

[24] ŠKORNIČKOVÁ, Mgr. Eva. *Co považuje GDPR za osobní údaje | GDPR.cz.* Dostupný z: ⟨https://www.gdpr.cz/gdpr/osobni-udaje/⟩.

[25] JOSHI, Rushikesh. *Interactive Phishing Filter* [online]. [cit. 2015--]. Dostupný z: ⟨https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1426&context=etd_projects⟩.

[26] REKOUCHE, Koceilah. *Early Phishing* [online]. [cit. 2011--]. Dostupný z: ⟨http://arxiv.org/abs/1106.4692⟩.