
DETEKCIA FORIEM SOCIÁLNEHO INŽINIERSTVA V EMAILOVEJ KOMUNIKÁCII


AUTOR PRÁCE: EVA MARKOVÁ
VEDÚCI PRÁCE: MGR. TOMÁŠ BAJTOŠ


MOTIVÁCIA



- Človek – najslabší článok bezpečnosti
- Filtrovanie spamu nebráni útokom pomocou sociálneho inžinierstva
- Phishingové kampane sú na dennom poriadku → problémy
- Riešenia existujú, ale vo väčšine sú len v stave „výskumu“

Vaša schránka prekročila limit.

Táto pošta je z help desk.

 "Univerzita Pavla Jozefa Šafárika" <marketa.andricikova@upjs.sk>
št 15.2, 14:56
Mgr. Markéta Andričíková PhD. ▾


 "Univerzita Pavla Jozefa Šafárika používate" <5203773@upjs.sk>
po 19.2, 18:58
Ivo Kováč ▾

  Odpovedať všetkým ▾



Vaša schránka prekročila limit.

Vaša Univerzita Pa
potrebné ju aktua
inováciu:> [https://](https://upjs.weebly.com/)

 "Univerzita Pavla Jozefa Šafárika" <dasa.babcanova@upjs.sk>
pi 16.2, 9:35
Bc. Dáša Babčanová ▾

Poznámka: Ak sa v
do nového prehli
aktualizáciu správi
zakáže.
Help desk pre služ
© 2018 mail

 131 MB

Vaša Univerzita Pavla Jozefa Šafárika , priestor poštovej schránky - kvóta je plná a je potrebné ju aktualizovať kliknutím na tento webový odkaz na inováciu:> <https://upjs.weebly.com/>

Poznámka: Ak sa vám nepodarí kliknúť na odkaz, odporúčame ho skopírovať a vložiť do nového prehliadača, aby ste zvýšili kvótu pošty na aktualizáciu. Ak nepožiadate o aktualizáciu správne požadované údaje o overení, váš účet schránky sa automaticky zakáže.
Help desk pre služby IT.
© 2018 mail

Vážená Univerzita Pavla Jozefa Šafárika používate, e-mailu:


Nedávno sme zablokovali pokus o prihlásenie do vášho e-mailového konta v programe Outlook z používal váš email ilegálne a my sme prijali náležitú akciu na pozastavenie ihlásenia až do ďalšieho upozornenia.

láskavo dokončíte proces aktualizácie, aby ste zabezpečili a udržali váš e-amžite, dôjde k deaktivácii vášho e-mailového účtu. Upozorňujeme a enie kliknutím na odkaz nižšie pre verifikáciu-aktualizáciu.

[s.weebly.com/](https://upjs.weebly.com/)

dený odkaz, odporúčame ho skopírovať a vložiť do nového prehliadača.



- 
- Koncom roku 2017 užívateľ dostal priemerne **16** škodlivých emailov za mesiac (Symantec)
 - **76%** organizácií malo skúsenosť s phishingovými útokmi v roku 2017 (Wombat 2018 State of the Phish)
 - **92,4%** malvérov sú doručené cez emaily (Verizon 2018 DBIR)

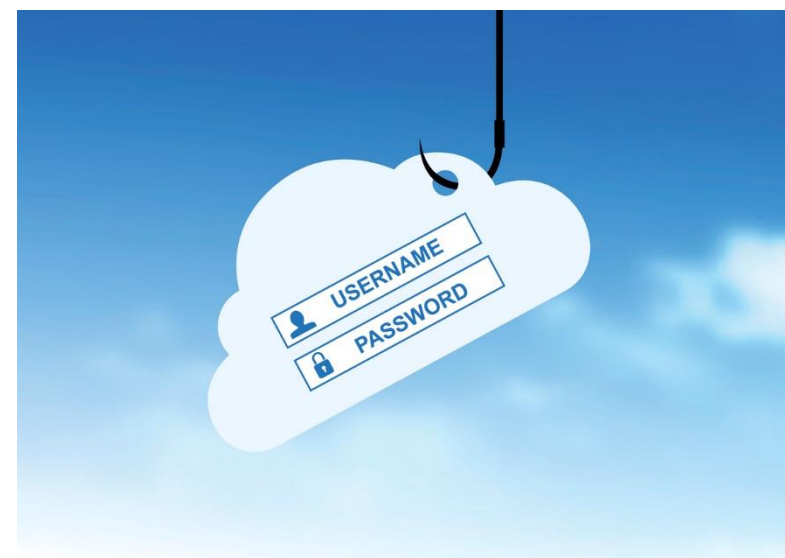
SOCIÁLNE INŽINIERSTVO

- Nástroj na získavanie citlivých údajov
- Zameriava sa na najväčšiu zraniteľnosť – človeka
- Nie sú potrebné technické schopnosti
- Phishing, spear phishing, watering hole, baiting,...



PHISHING

- Typ útoku, pri ktorom sa útočník pokúša získať citlivé informácie prostredníctvom elektronických komunikácií vydávaním sa za dôveryhodnú entitu
- Manipulácia človeka
- Emaily pôsobia dôveryhodne
- Úspešnosť závisí predovšetkým od dôveryčivosti



SPEAR PHISHING

- Cielený útok na úzku skupinu potenciálnych obetí
- Emaily sú personalizované a špecifické pre konkrétnu osobu



Administrator <meno.priezvisko@upjs.sk> v zastúpení používateľa Administrator <administrator@sluzba.sk>

Používateľ

št 27. 9

Aktualizacia platnosti hesla



Vážený používateľ účtu,

Platnosť Vášho hesla vyprší za dva dni, aby ste udržali svoj účet, prosím, [KLIKNITE SEM](#) a postupujte podľa inštrukcií, aby ste si udržali Váš e-mailový účet **ALEBO KLIKNITE TENTO LINK**:

<http://heslo.update.ponggok.com/>

Neaktualizácia vášho e-mailového účtu spôsobí jeho deaktiváciu, buďte upozornení!

IT-Help Desk,
PA 19104

IT Help Desk © 2018 VŠETKY PRÁVA REZERVOVANÉ



Final Notice <2zS@630363.capricornus.website>

muiKb@pn6cmts.uk

st 26. 9

⊘ Požiadavka na ukončenie účtu v službe Google™ bola akceptovaná.



Vážený zákazník služby Gmail™,

Odoslali ste žiadosť o ukončenie Vášho e-mailového účtu v službe Gmail. Danou požiadavkou sa začal venovať náš tím. Prosím dajte nám teda 3 pracovné dni na ukončenie vášho účtu.

Ak chcete zrušiť žiadosť o ukončenie Vášho e-mailového účtu, odpovedzte prosím na tento e-mail.

Ukončením Vášho účtu budú odstránené všetky súbory (vrátane doručenej pošty, odoslanej správy, spamu, koša, konceptov).

Ak potrebujete ďalšiu pomoc, neváhajte nás kontaktovať

S pozdravom,
služba Gmail

HOAX

- Správa, ktorá napriek svojej nezmyselnosti vyzýva na to, aby bola preposielaná ďalším používateľom systému
- Jednoduchosť a prakticky nulová cena
- Napísaním, resp. rozposlaním takejto správy sa nič nezmení



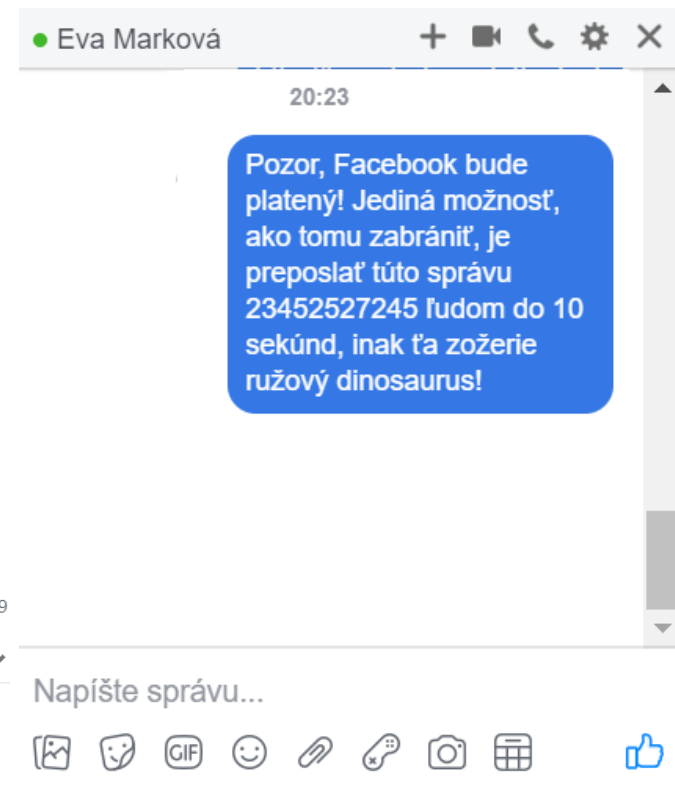
Facebook <bff@facebook.com>

meno.priezvisko@gmail.com

Facebook - BFF

Mark Zuckerberg, generálny riaditeľ Facebooku, vymyslel slovo BFF, aby sa uistil, že váš účet na facebooku je bezpečný. Dajte lajk tomuto príspevku a napíšte BFF do komentára, ak sa objaví zelená, váš účet je chránený.

Ak sa neobjaví v zelenej farbe, okamžite si zmeňte heslo, pretože ho môže niekto hacknúť (zneužiť)




PRÍSTUPY NA DETEKCIU RESP. OCHRANU VOČI SOCIÁLNEMU INŽINIERSTVU

- Blacklisty
- Heuristika
- Vizuálna podobnosť
- Dolovanie dát

BLACKLISTY

- Často aktualizované zoznamy predtým zistených phishingových URL adries, IP adries a kľúčových slov
- Neefektívne voči zero-hour útokom
- Príklady:
 - Google Safe Browsing API, DNS-Based Blacklist, PhishNet, Automated Individual White-List

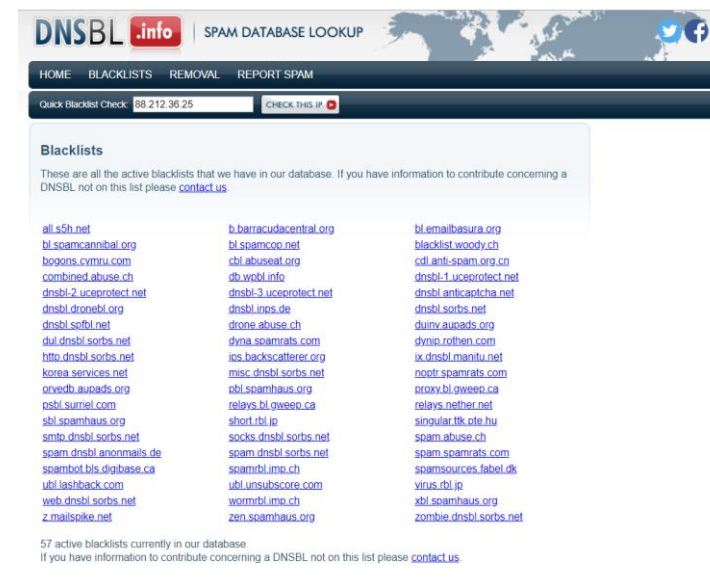


The site ahead contains harmful programs

Attackers on [this site](#) might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#) [Back to safety](#)



DNSBL.info | SPAM DATABASE LOOKUP

HOME BLACKLISTS REMOVAL REPORT SPAM

Quick Blacklist Check:

Blacklists

These are all the active blacklists that we have in our database. If you have information to contribute concerning a DNSBL not on this list please [contact us](#).

all.5ft.net	b.barracudacentral.org	bl.emailbasura.org
bl.soamcannibal.org	bl.spamc00.net	blacklist.woody.ch
bogons.cymru.com	cbl.abuseat.org	cdl.anti-spam.org.cn
combined.abuse.ch	gh.wtbl.info	dnsbl-1.ucerprotect.net
dnsbl-2.ucerprotect.net	dnsbl-3.ucerprotect.net	dnsbl.anticapcha.net
dnsbl.dronebl.org	dnsbl.imos.de	dnsbl.sorbs.net
dnsbl.sofbl.net	drone.abuse.ch	duinv.aupads.org
dul.dnsbl.sorbs.net	dyna.spamrats.com	dynv.rothen.com
http.dnsbl.sorbs.net	jcs.backscatterer.org	ix.dnsbl.manitu.net
korea.services.net	misc.dnsbl.sorbs.net	nostr.spamrats.com
onedth.aupads.org	phl.spamhaus.org	proxyl.gweep.ca
nsbl.surriel.com	relays.bl.gweep.ca	relays.nether.net
sbl.spamhaus.org	short.rbl.jp	singular.lk.cfe.hu
smt0.dnsbl.sorbs.net	socks.dnsbl.sorbs.net	spam.abuse.ch
spam.dnsbl.anonmails.de	spam.dnsbl.sorbs.net	spam.spamrats.com
spambot.bis.digibase.ca	spambtl.imo.ch	spamsources.fabel.dk
ubl.lashback.com	ubl.unsubscore.com	virus.rbl.jp
web.dnsbl.sorbs.net	wormtbl.imo.ch	xbl.spamhaus.org
z.mailspike.net	zen.spamhaus.org	zombie.dnsbl.sorbs.net

57 active blacklists currently in our database.
If you have information to contribute concerning a DNSBL not on this list please [contact us](#).

HEURISTIKA

- Charakteristiky, ktoré boli nájdené v útokoch
- Možné identifikovať zero-hour útoky
- Možnosť straty legitímnych emailov
- Príklady:
 - SpoofGuard, PhishGuard, CANTINA, A Phishing Sites Blacklist Generator

VIZUÁLNA PODOBNOSŤ WEBOVÝCH STRÁNOK

- Detekcia útokov na základe vizuálneho vzhľadu
- Príklady:
 - Classification with Discriminative Keypoint Features
 - Visual Similarity-based Detection without Victim Site Information

DOLOVANIE DÁT

- Algoritmy sa snažia namapovať vstup na požadovaný výstup použitím špeciálnej funkcie
- Príklady:
 - Bayesian Anti-Phishing Toolbar, Detecting Phishing Emails Using Hybrid Features

SYSTEM NA DETEKCIU SOCIÁLNEHO INŽINIERSTVA

- Pomocný systém
- Ľudský faktor
- Preposielanie emailov na vopred vytvorenú adresu (napr. „spam@upjs.sk“)
- Extrakcia potrebných dát z emailu
- Čo si všímať v emailoch?
 - URL adresy v tvare IP adries
 - Či URL adresa zodpovedá stringu, ktorý vidíme
 - Počet hypertextových odkazov
 - Počet rôznych domén
 - Počet bodiek v linkoch
 - Či obsahuje javascript

DATASET

- Podvrhnuté emaily
- <https://www.kaggle.com/c/adcg-ssl4-challenge-02-spam-mails-detection>
- <http://untroubled.org/spam/>

CIELE

- Analýza a spracovanie foriem sociálneho inžinierstva v emailovej komunikácii
- Porovnanie a spracovanie aktuálnych prístupov k ochrane voči sociálnemu inžinierstvu v emailovej komunikácii
- Návrh a implementácia systému na detekciu foriem sociálneho inžinierstva v emailovej komunikácii a jeho overenie

NAJBLIŽŠIE KROKY

- Spracovanie a spísanie aktuálnych prístupov k ochrane voči sociálnemu inžinierstvu
- Začiatok implementácie systému, kam sa budú preposielat' emaily

LITERATÚRA

- MANN, Ian. Hacking the human: social engineering techniques and security countermeasures. Routledge, 2017.
- BULLÉE, Jan-Willem Hendrik, et al. On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *Journal of investigative psychology and offender profiling*, 2018, 15.1: 20-45.
- GUPTA, B. B., et al. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 2017, 28.12: 3629-3654.



ĎAKUJEM ZA POZORNOST – OTÁZKY?