Phishing

Lenka Dědková

Phishing

Not to be confused with Fishing.

- Co to je?

- Criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials
  - Anti-Phishing Working Group

Skupinová aktivita

- Dvě skupiny:
  - 1. cíl: získat hesla do IS
  - 2. cíl: získat finance
  - (3. cíl: heslo na Facebook)

- Jaké principy jste ve vytváření strategie využili?
- (Představte si například, že vytváříte návod, jak udělat úspěšný phishingový útok)

- Jak by se proti takovému útoku dalo bránit?
- (Představte si, že se snažíte vymyslet návod pro uživatele, jak se nestát obětí phishingu; případně návod pro zaměstnavatele, jak v tomto směru ovlivnit své zaměstnance/studenty)

Sociální inženýrství a phishing

- SI: manipulace s lidmi, zneužívání přirozených (naučených) tendencí s cílem získat <doplňte si>
  - SI typicky zahrnuje shromažďování informací o oběti před samotným útokem za účelem vybudování důvěry

- Phishing: obvykle nezahrnuje shromažďování informací

Jak se na phishing dívá psychologie

- Persuaze – přesvědčování: centrální a periferní cesta
  - Centrální – argumenty, logické uvažování, zvažování pro a proti
  - Periferní – cokoliv ostatního, typicky emoční přesvědčování
- Heuristic-systematic model – zpracování informací
  - Systematické - kognitivně náročnější, uživatel musí mít motivaci, schopnosti a znalosti
  - Heuristické – kognitivní zkratky

Heuristiky

- Namísto pečlivého hodnocení lidé používají kognitivní zkratky (heuristiky)
  - Jednoduché, praktické, zkratkovité kroky vedoucí k rychlému posouzení situace/člověka
  - př. heuristika dostupnosti
    - Při posuzování pravděpodobnosti hodnotíme snadnost, s jakou si dovedeme daný výsledek představit
    - Slova začínající na K x slova s K na třetím místě
  - heuristika ukotvení
    - první informace vytváří porovnávací základ – v obchodech
  - Tversky & Kahneman

- Využívání jiných vodítek pro hodnocení situace než systematických

Trust

- Velkou roli v „podlehnutí“ podvodným mailům (ale i podvodům celkově) hraje důvěra uživatele
  - Vůči službě, instituci, autoritě, médiu
  - Vůči zdroji informací
  - *authority heuristic*

- Kang, Bae, Zhang, Sundar (2011): lidé často podkládají důvěru proximálním zdrojem (online news)
- Pokud podvodný email přijde od důvěryhodného zdroje, má vyšší šanci být úspěšný

Poměr nákladů a zisků

- Ekonomické teorie chování
  - Lidé při rozhodování, jak se budou chovat, zvažují a balancují mezi náklady a zisky

- „Lidské“ náklady: materiální náklady, energie, čas
- „Lidské“ zisky: úspora energie a času

- Systematické hodnocení a centrální přesvědčování jsou (obvykle) nákladnější než heuristické a periferní

Phishing

- Podle HSM tedy úspěšný phishingový útok
  - musí podnítit/usnadnit heuristické zpracování nad systematickým
  - tj. musí poskytnout jasná vodítka, která uživatelé mohou k hodnocení použít
  - a co nejvíce ztížit systematické hodnocení v případě, že se do něj někteří uživatelé pustí

Heuristická vodítka ve phishingu

- Důvěryhodnost zdroje, autorita
  - Lidé jsou naučení autority poslouchat
  - Důvěryhodnost
    - Známá instituce s dobrou reputací (banka, policie, úřad)
    - Email od důvěryhodné osoby („kamarád“, „bezpečák“, „ředitel“…)
- „Žánr“ zprávy (forma zprávy odpovídající normám podobných typů zpráv)
  - Gramatika, formální úprava zprávy, adekvátní jazyk
  - Realistický obsah zprávy

Ztížení systematického zpracování

- Co nejvíce podobná stránka
- Co nejvíce podobná URL
- Funkční odkazy a další prvky na stránce

Phishing

- Podle teorie persuaze
- Podnítit využití periferní cesty přesvědčování → emoce
  - Časový press – je třeba jednat ihned
  - Hrozba – nebo přijdete o účet/peníze/údaje/možnost získat slevu/peníze/bonus…
  - Výdělek – připíšeme vám bonus, vyhráli jste, za věrnost naší společnosti dostanete…
  - Empatie – pomozte opuštěným pejskům
  - Zvědavost – check out hot girls…

Heuristické vs. systematické zpracování

- Osobnostní charakteristiky
  - Need for cognition
- Motivace
  - Znalosti
  - Předchozí zkušenosti
  - Širší okolnosti – např. v médiích zprávy o phishingových útocích nebo neobvyklý pohyb na účtu…

Výzkumy

Rozpoznání phishingových stránek

- Dhamija et al. (2006)

- N = 22, 10 mužů, 18-56 let
- Experiment: prezentovaných 19 stránek
  - Pravých a phishingových
- Respondenti měli u každé rozhodnout, zda jde o podvodnou stránku nebo ne, následovaly rozhovory

- Celkové skóre: 6-18 správně rozpoznaných stránek (M = 11.6, SD = 3.2)

Typy respondentů podle jejich strategií

- 1. pouze obsah webu
  - 23 % (n = 5)
  - Používali pouze obsah stránky (loga, layout, grafika, jazyk, fungující linky)

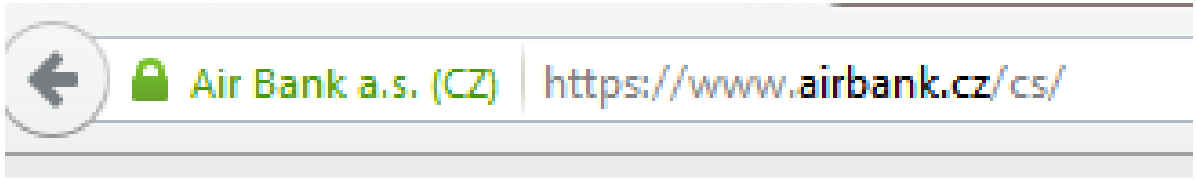
"*I never look at the letters and numbers up there* [in the address bar]. *I'm not sure what they are supposed to say*"

Typy respondentů podle jejich strategií

- 2. obsah webu a doména
  - 36 % (n = 8)
  - Kromě obsahu webu kontrolovali URL (nikoliv SSL)
  - Rozpoznali adresy s IP místo doménou jako podezřelé, ačkoliv nevěděli, co to znamená

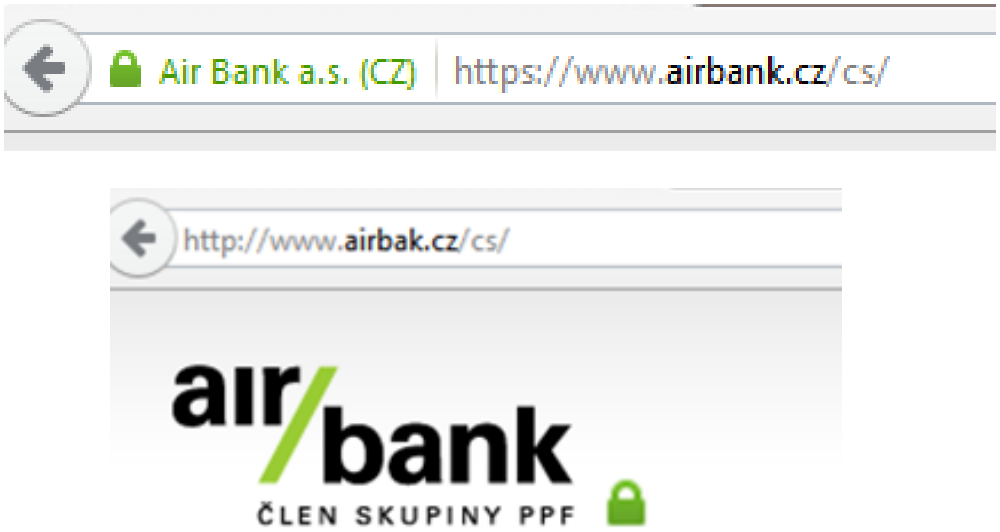
Typy respondentů podle jejich strategií

- 3. obsah webu, url a https
  - 9 % (n = 2)
  - Nehledali ikonku zámku
  - Někteří si jí předtím nikdy nevšimli



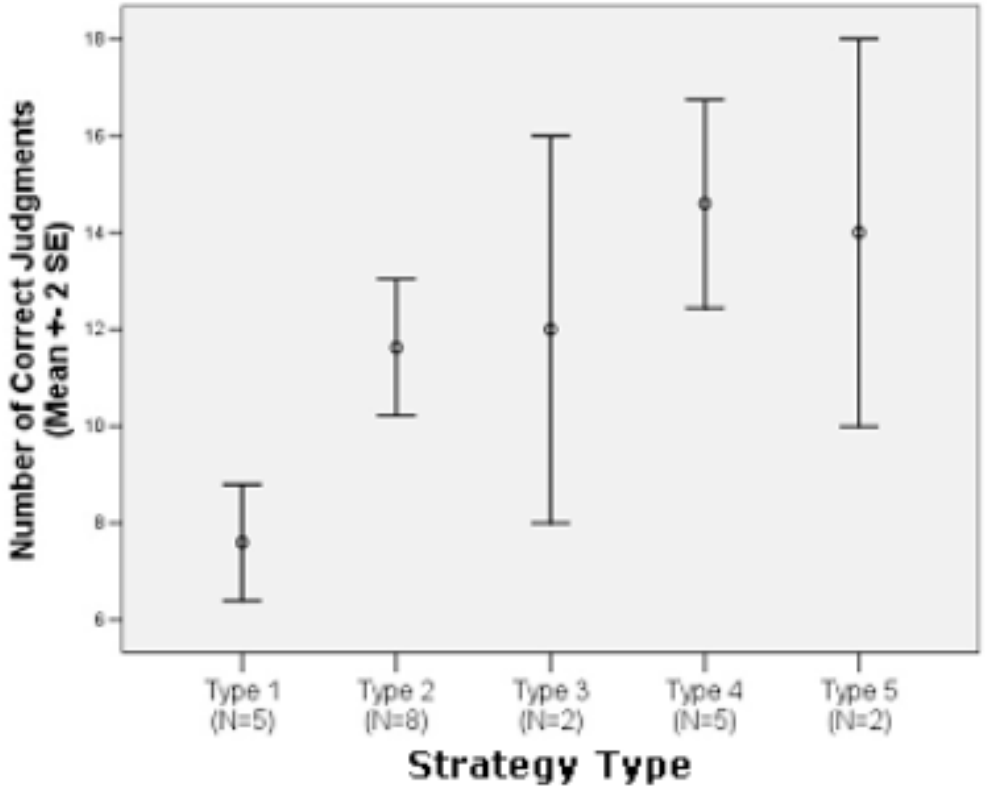
Typy respondentů podle jejich strategií

- 4. navíc i zámek
  - 23% (n = 5)
  - Hledali zámek, ale někteří připisovali větší důvěru, pokud byl v samotné stránce než u url



Typy respondentů podle jejich strategií

- 5. vše předtím + certifikáty
  - 9% (n = 2)



- Další zmíněná strategie:
  - Zadání přihlašovacího jména a hesla jako strategie ke zjištění, zda je stránka pravá nebo ne

- Po ukázání varování na certifikát podepsaný sám sebou:
  - 15 lidí (z 22) automaticky kliklo na OK bez čtení
  - 18 nevědělo, na co se dotaz ptá
    - *“I accepted the use of cookies”;*
    - *“It asked me if I wanted to save my password on forms”;*
    - *“It was a message from the website about spyware”*

Pokračování…

- Předchozí výzkum byl z roku 2006… určitě se mnohé změnilo…

- Alsharnouby, Alaca, & Chiasson, (2015)
- 24 stránek (10 ok, 14 phishing), eye-tracker
- N = 21 (12 žen), 18-51 (M = 27)
- 14 studenti (uni), 7 zaměstnanci

- Prvky:
  - Stránky se zkreslenou URL
  - Stránky s IP namísto URL
  - Fake browser
  - Pop-ups
  - SSL locks,…

Výsledky

- Jednotliví respondenti 9-22 správně (z 24)
- Pro phishingové stránky úspěšnost 53% (ale některé odhaleny omylem)
- Pro legitimní 79%

- Čas hodnocení stránek – M = 87sec, nesig. rozdíl mezi typy stránek
- Muži a ženy se nelišili, žádné věkové rozdíly (ale maličký vzorek)

- Respondenti měli tendenci rychleji se rozhodovat o stránkách, které znali (stránka vlastní banky)

Eye-tracker

- 85% času strávili sledováním obsahu stránky
- 9% sledováním formátu stránky
- 6% sledováním „areas of interest“ – míst, kde na stránkách jsou cues relevantní pro odhalení phishingu

- Rozhovory poté – nekonzistentní důvody, neporozumění

Strategie uživatelů

- Prohlížení a posouzení obsahu stránky – nejvíce reportovaná strategie
- Testování funkcionality stránky (změna jazyka, změna země, klikání na odkazy)
- Kontrola URL – nicméně hodně jich nevědělo, na co přesně se zaměřit, spíš pocitově „vypadá divně x vypadá normálně“
- Vyhledání stránky přes google a porovnání
- Přítomnost SSL indikátorů (ale i na špatných místech)

Co bylo jiné 2006-2015

- 2006 – respondenti často ani nevěděli, co je phishing nebo že se stránky dají celé napodobit
- 2015 – respondenti věděli o phishingu

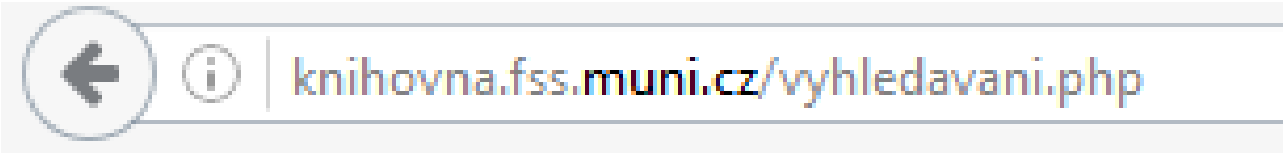
- Celkově ale – spíš neznalost, nepochopení principů fungování stránek

Ne/znalosti uživatelů

- www.mail.centrum.cz
- www.centrum.mail.cz

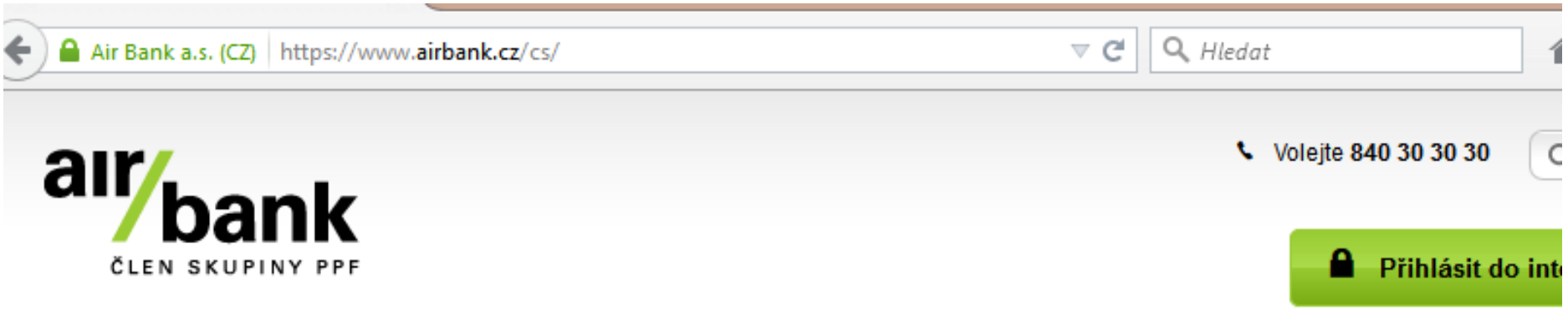
- www.bankofthevvorld.com
- www.paypai.com

- http://www.fss.muni.cz/
- http://www.fss-muni.cz/
- http://www.fss.muni.uni.cz
- http://www.fss.munii.cz

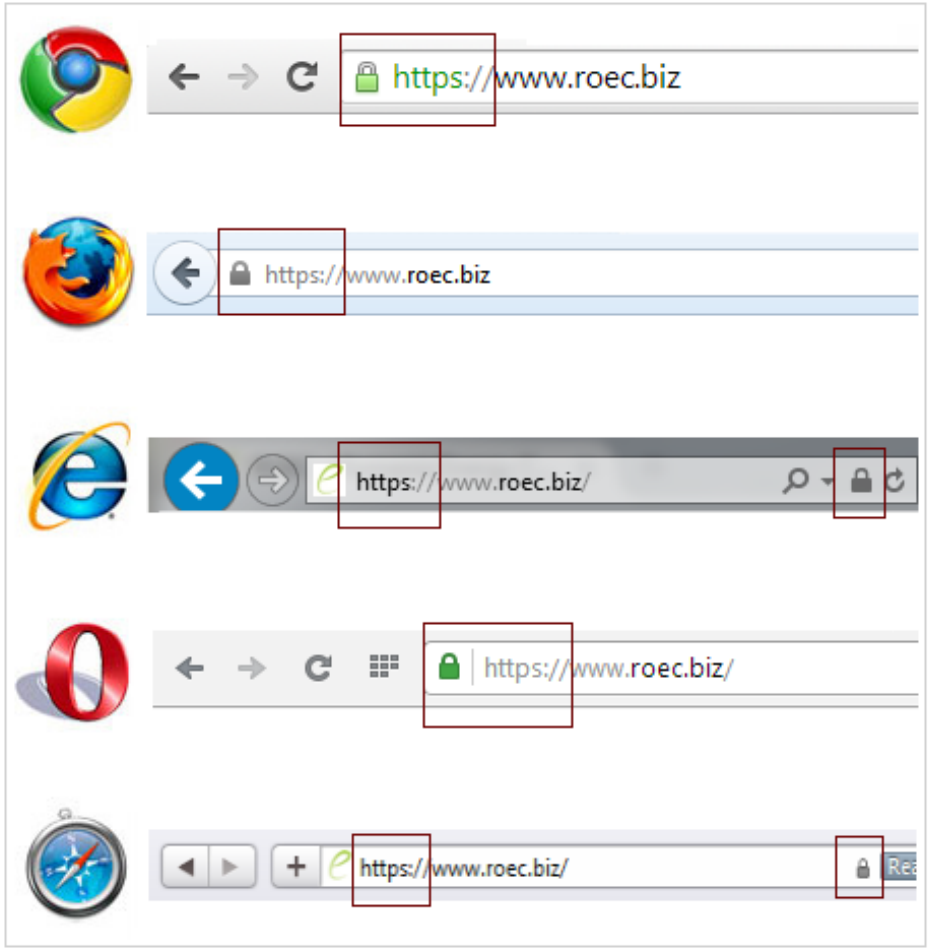


Ne/znalosti uživatelů

- Nahrazování znaků vizuálně podobnými (homographs)
  - „a“ v latince (U+0061) a cyrilici (U+0430)
- Pop-up okna…
- SSL



Ne/znalosti uživatelů



- Předchozí výzkumy byly o odhalování phishingu u lidí, kteří věděli, že mají odhalovat

- Jaká je ale úspěšnost phishingu „normálně“?
  - Obtížné zjistit – etika versus externí validita

Jagatic et al. (2005)

- Experiment, phishing hesel
- Dvě skupiny:
  - Sociální – email přišel od jejich kamaráda (zjištěno ze SNS)
  - Kontrolní – email od neznámé osoby

	Successful	Targeted	Percentage	95% C.I.
Control	15	94	16%	(9–23)%
Social	349	487	72%	(68–76)%

  - Někteří obnovovali (a odeslali heslo) na stránce více než 80x

Po skončení výzkumu…

- Jagatic et al. (2005)
- Spousta reakcí od lidí (kteří nevěděli, že jsou součástí experimentu)
  - Vztek, obviňování výzkumníků
  - Popření (psali za kamaráda)
  - Nedorozumění – někteří si mysleli, že výzkumníci se nabourali do účtu kamaráda
  - Podceňování dostupnosti informací – někteří nechápali, kde výzkumníci zjistili, kdo jsou jejich kamarádi
  - Stížnosti od těch, jejichž jména a emaily výzkumníci „zneužili“

- Etika…!

- Carella et al. (2017)

- *“We are inviting you to participate in a research study focused on internet security. This study aims to provide clear evidence of the impact that security awareness training has on individuals on the internet and determine which level of security awareness training provides participants with the best chance to security themselves in a digital world”*

- *“You may be contacted via email during this presentation”*

Častější oběti

- Ti, kteří nemají předchozí vlastní negativní zkušenost s phishingem
- Častěji ženy
- Častěji úspěšný, pokud je odesílatel opačného pohlaví (zvláště pro muže)
- Ti, kteří sami tvrdí, že mají nízké povědomí o ICT bezpečnosti
- (studenti) častěji z oborů: zdravotnictví, obchod a pedagogika
- Starší (a specificky senioři)
- Carella et al. (2017), Oliveira et al. (2017), Jagatic et al. (2005)

Wright et al. (2010)

- Studenti v online kurzu Introduction to Information Systems
- „Super secure code“ pro přihlašování ke studijním materiálům, odevzdávání úkolů apod.
  - Opakované upozorňování, že ho nesmí nikomu dát, podepsání NDA
- Po 2 měsících od začátku kurzu phishingový mail

Mail

This email is to inform you of a problem we are having with the information technology database. Due to a data collision we have lost some information and are unable to recover. In order to get the database back up and working we need to you forward us your "super-secure code." Please respond to this email with your code by the end of business today. Sorry for the inconvenience.

Jason Roth, network administrator

- N = 229
- 26 „detekovalo“ phishing (tj. nahlásili ho, zjišťovali další informace…)
  - Ale metoda…
- Kvali follow-up

- Z prediktorů signifikantní:
  - Zkušenosti s prací online
  - Obecná důvěřivost

Proces rozpoznání phishingu

- 1. vzhled mailu
  - Předmět mailu a autor
  - Text samotného mailu
    - Email v normách mailů podobného typu?
    - Povaha žádosti – co po mě chce
- 2. „aktivace“ podezření
  - Nekonzistentní s tím, co čekám
    - Chce něco, co se nemá posílat tímto způsobem
    - Problematické odůvodnění
    - Urgence vs. čas
    - Neznámý autor

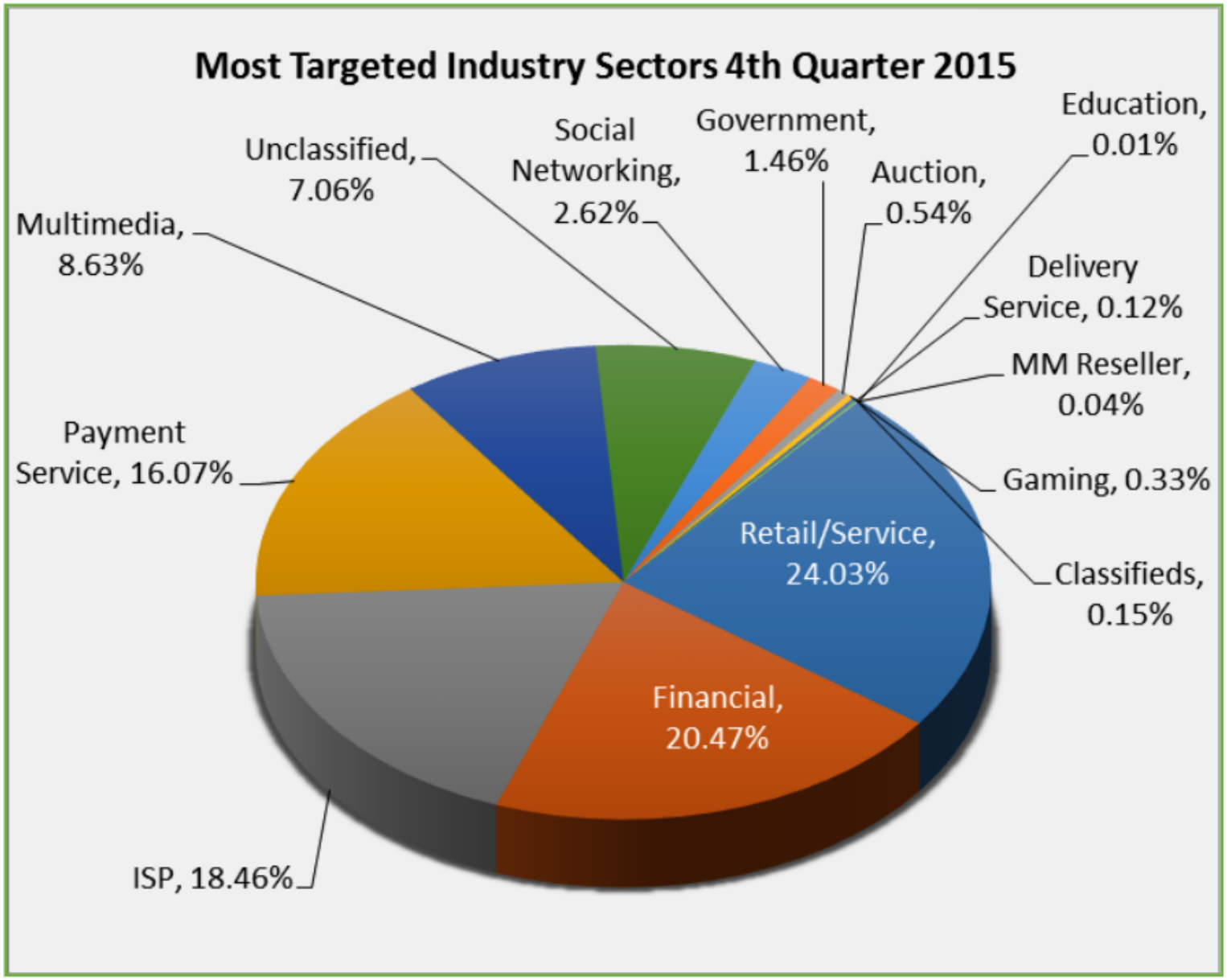
Proces rozpoznání phishingu

- 3. potvrzení podezření
  - Formování hypotéz a ověřování hypotéz
    - Hledání potvrzení oprávněnosti u jiných autorit
    - Vlastní hledání – jméno autora/společnosti,…

Anti-phishing Working Group

- http://www.antiphishing.org/
- 4Q2015:
  - 158 574 unikátních phishingových útoků
  - 47 623 unikátních domén
    - Z toho 22 679 zaregistrováno za účelem phishingu (ostatní hacked)
  - Většina stránek z USA

- Délka – hodiny – max. dny


Most Targeted Industry Sectors 4th Quarter 2015
Education, 0.01%
Government, 1.46%
Social Networking, 2.62%
Unclassified, 7.06%
Auction, 0.54%
Multimedia, 8.63%
Delivery Service, 0.12%
MM Reseller, 0.04%
Payment Service, 16.07%
Gaming, 0.33%
Retail/Service, 24.03%
Classifieds, 0.15%
Financial, 20.47%
ISP, 18.46%

Co s tím?

- Technologická řešení
  - Kde je to možné, sem s nimi
- Ale phishing (a obecně SI) profitují z lidských (a ne technických) chyb a technická řešení nedokáží odfiltrovat vše
  - Je třeba soustředit se na uživatele
  - Osobnost, motivace, schopnosti, znalosti

Efekt různých školení

- Carella et al. (2017)

- Tři skupiny po 50 účastnících (studenti), experiment probíhal během 7 týdnů
  - Kontrolní
  - Školení prostřednictvím dokumentů, které se zobrazí poté, co kliknou na phishingový email (emaily během 2., 5. a 8. týdne experimentu)
  - Školení pomocí prezentací ve třídách (jedna prezentace ve 2. týdnu)

- Porovnávají click through rates v odkazech

Efekt školení

Po 7 týdnech efekt školení prostřednictvím prezentací (i když nejdřív vyšší pokles) mizí a je srovnatelný s žádným školením

Průměr na počátku – cca polovina lidí na phishingy klikne

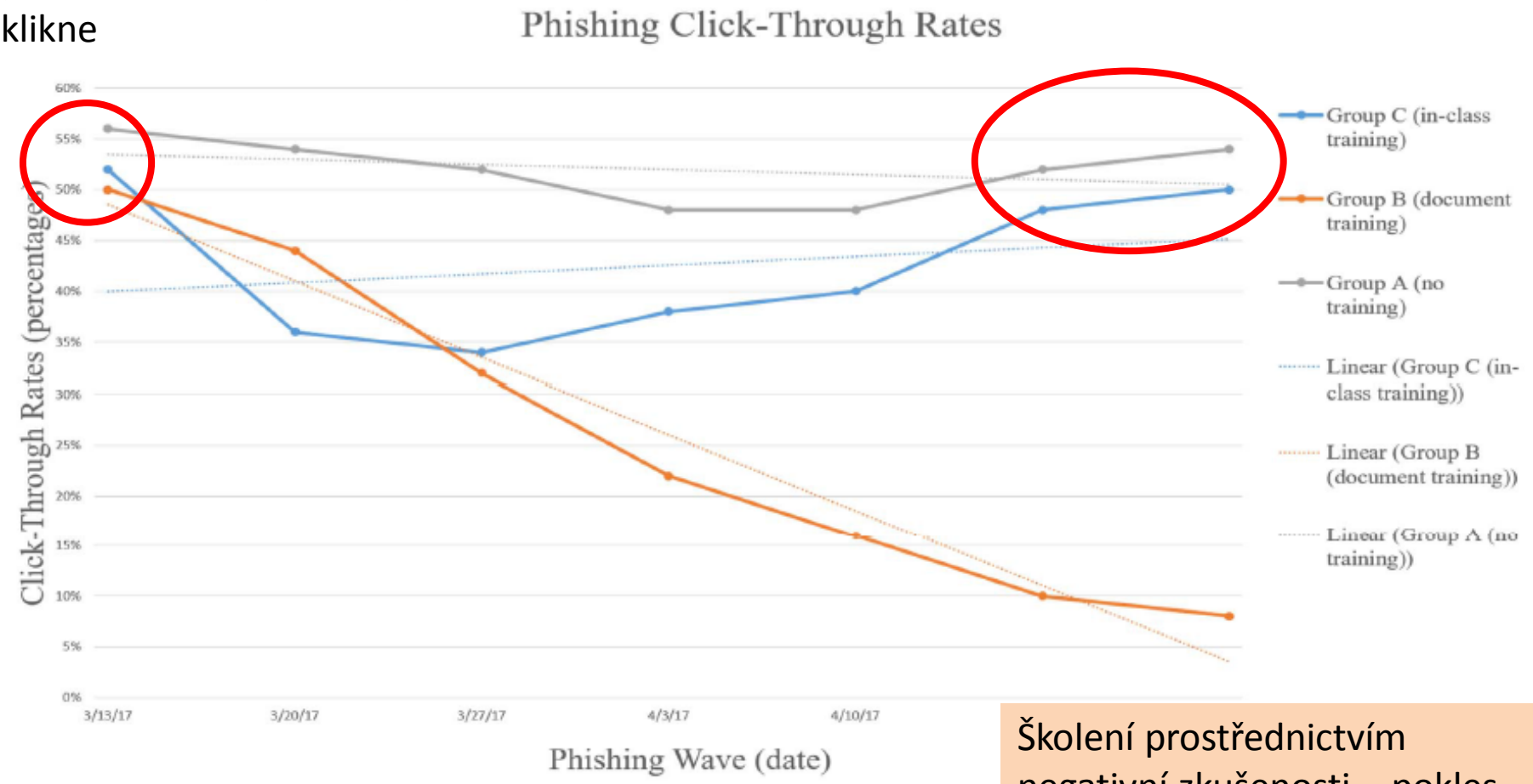


Figure 4. Phishing Click-Through Rates

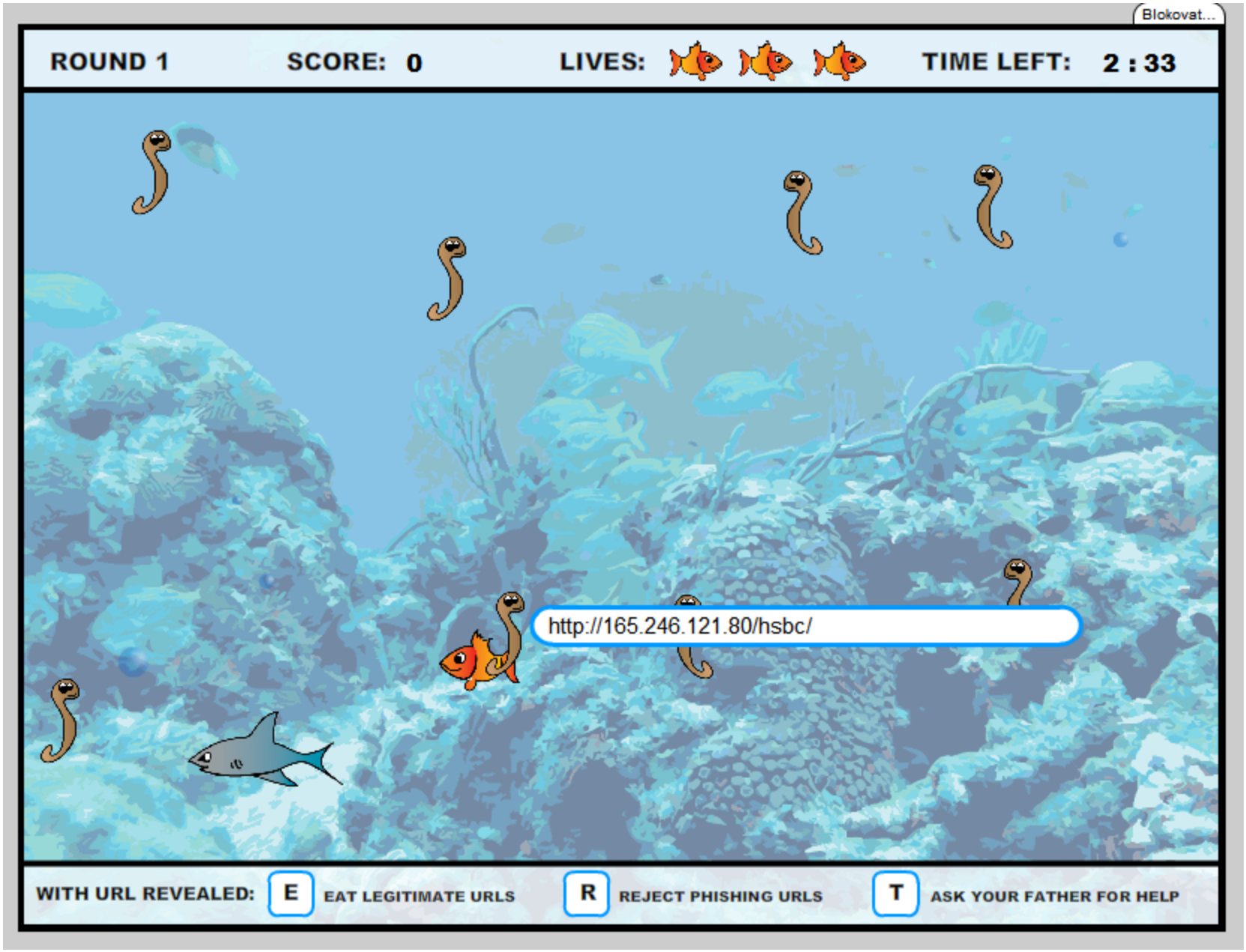
Školení prostřednictvím negativní zkušenosti – pokles na 9 %

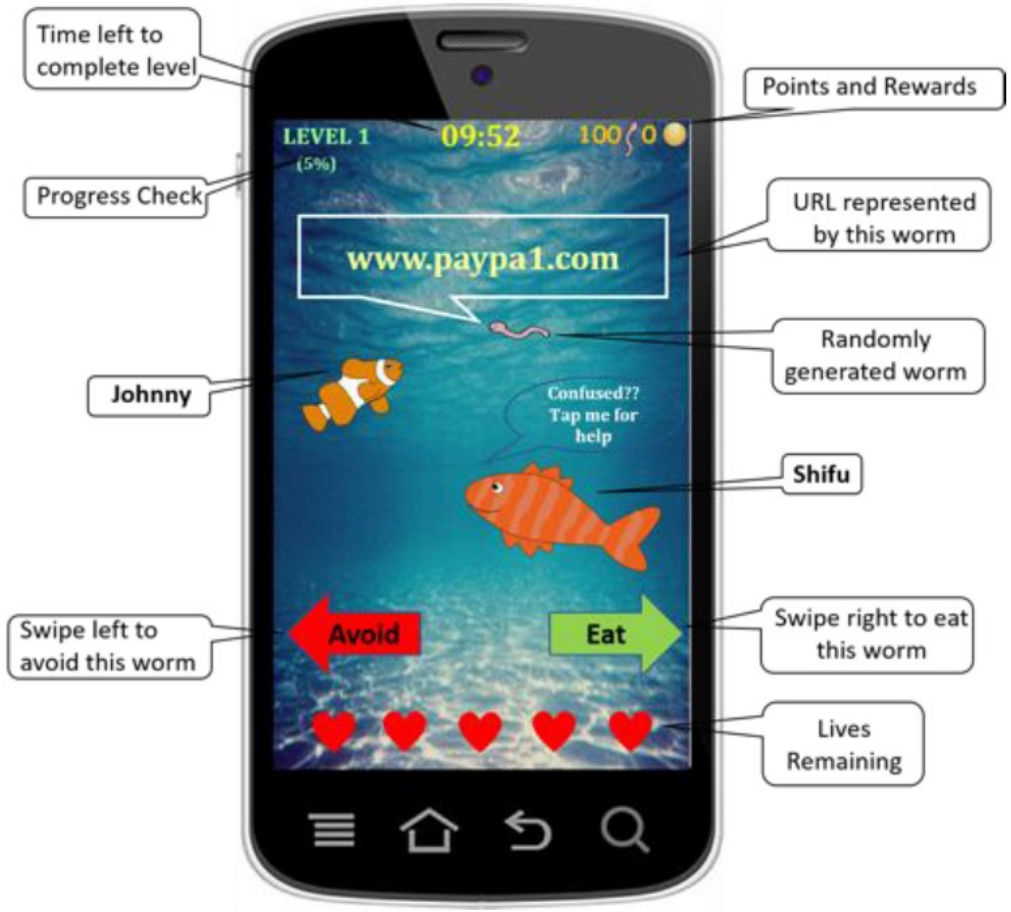
Vzdělávání

- Nejúčinnější, pokud následuje ihned po phishingovém útoku

- Anti-phishing Phil: http://www.ucl.ac.uk/cert/antiphishing/
  - Browser app
  - Po zahrání uživatelé snadněji rozpoznali pochybné stránky
  - Efekt patrný i po týdnu (otázka jak po delší době…)

- Phish Phinder – ve vývoji (Misra et al., 2017)


Blokovat...
ROUND 1
SCORE: 0
LIVES:
TIME LEFT: 2 : 33
http://165.246.121.80/hsbc/
WITH URL REVEALED:
E
EAT LEGITIMATE URLS
R
REJECT PHISHING URLS
T
ASK YOUR FATHER FOR HELP


Time left to complete level
Points and Rewards
LEVEL 1
(5%)
09:52
100
0
Progress Check
URL represented by this worm
www.paypa1.com
Randomly generated worm
Johnny
Confused??
Tap me for help
Shifu
Swipe left to avoid this worm
Avoid
Eat
Swipe right to eat this worm
Lives Remaining


LEVEL 1
(10%)
09:39
200
0
Well done!!
Now tap on the part of the URL that was malicious:
com
paypa1
www

(a)


LEVEL 1
(5%)
09:39
100
0
You have been Phished!
Look at the URL carefully. The "l" in "paypal" has been changed to "1".

(b)


LEVEL 1
(5%)
08:39
100
0
Look at the URL carefully. The "l" in "paypal" has been changed to "1". This is a common tactic used by attackers to fool users. Make sure you pay attention to each character of the URL in the future.

(c)

- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82.
- Carella, A., Kotsoev, M., & Truta, T. M. (2017, December). Impact of security awareness training on phishing click-through rates. In *Big Data (Big Data), 2017 IEEE International Conference on* (pp. 4458-4466). IEEE.
- Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.
- Fette, I., Sadeh, N., & Tomasic, A. (2007, May). Learning to detect phishing emails. In *Proceedings of the 16th international conference on World Wide Web* (pp. 649-656). ACM.
- Harris, A., & Yates, D. (2015). Phishing Attacks Over Time: A Longitudinal Study.
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.
- Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584-593.
- Luo, X. R., Brody, R., Seazzu, A., & Burd, S. (2013). Social Engineering: The Neglected Human Factor for. *Managing Information Resources and Technology: Emerging Applications and Theories: Emerging Applications and Theories*, 151.
- Kang, H., Bae, K., Zhang, S., & Sundar, S. S. (2011). Source cues in online news: Is the proximate source more powerful than distal sources?. *Journalism & Mass Communication Quarterly*, *88*(4), 719-736.
- Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work: A Journal of Prevention, Assessment and Rehabilitation*, *41*, 3549-3552.
- Misra, G., Arachchilage, N. A. G., & Berkovsky, S. (2017). Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. *arXiv preprint arXiv:1710.06064*.
- Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., ... & Ebner, N. (2017, May). Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6412-6424). ACM.
- Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation*, *19*(4), 391-416.
- Xu, Z., & Zhang, W. (2012). Victimized by Phishing: A Heuristic-Systematic Perspective. *Journal of Internet Banking and Commerce*, *17*(3), 1.