Kyberkriminalita. Phishing. Uživatelská bezpečnost a její výzkum.

Prof. David Šmahel

Jakou znáte kybernetickou kriminalitu?

Kybernetická kriminalita

Dle Policie ČR trestné činy upravené zákonem č. 40/2009 Sb:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230),
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231),
- Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).

Policie ČR: https://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx

Kybernetická kriminalita

Trestné činy upravené zákonem č. 40/2009 Sb.:

- Šíření pornografie (§ 191),
- Výroba a jiné nakládání s dětskou pornografií (§ 192),
- Navazování nedovolených kontaktů s dítětem (§ 193b),
- Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270),
- Hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355),
- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356),
- Šíření poplašné zprávy (§ 357),
- Pomluva (§ 184),
- Vydírání (§ 175), a mnohé další.

Policie ČR: https://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx

Kybernetická kriminalita

Druhy kyberkriminality

- Podvodné jednání (inzeráty nebo phishing)
- Hacking (neoprávněný přístup k systému, získání hesla, šíření škodlivývh kódů, kybernetické útoky včetně DDoS)
- Podvodné e-shopy
- Mravnostní trestné činy (pornografie, kontaktování dětí …)
- Trestné činy proti autorskému právu
- Násilné projevy a hate crime (vydírání, nebezpečné vyhrožování, hanobení rady, etnické nebo jiné skupiny)

Policie ČR: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

Kybernetická kriminalita v ČR 2022

Kybernetická kriminalita a ostatní kriminalita páchaná v kyberprostoru:

- Stálý růst této trestné činnosti: 18.554 skutků za rok 2022, což je 10,2% z celkové registrované kriminality
- Meziročně růst hackingu o 53% (2.575 za 2022)
- Podvody v oblasti nabídek přivýdělku v oblasti kryptoměn
- Trestné činy z nenávisti: 282 skutků (nárůst asi o 25%) – nejčastěji proti Ukrajincům (78), útoky proti lidskosti, útoky proti Rusům a Rusínům (50)

Policie ČR: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

Phishing

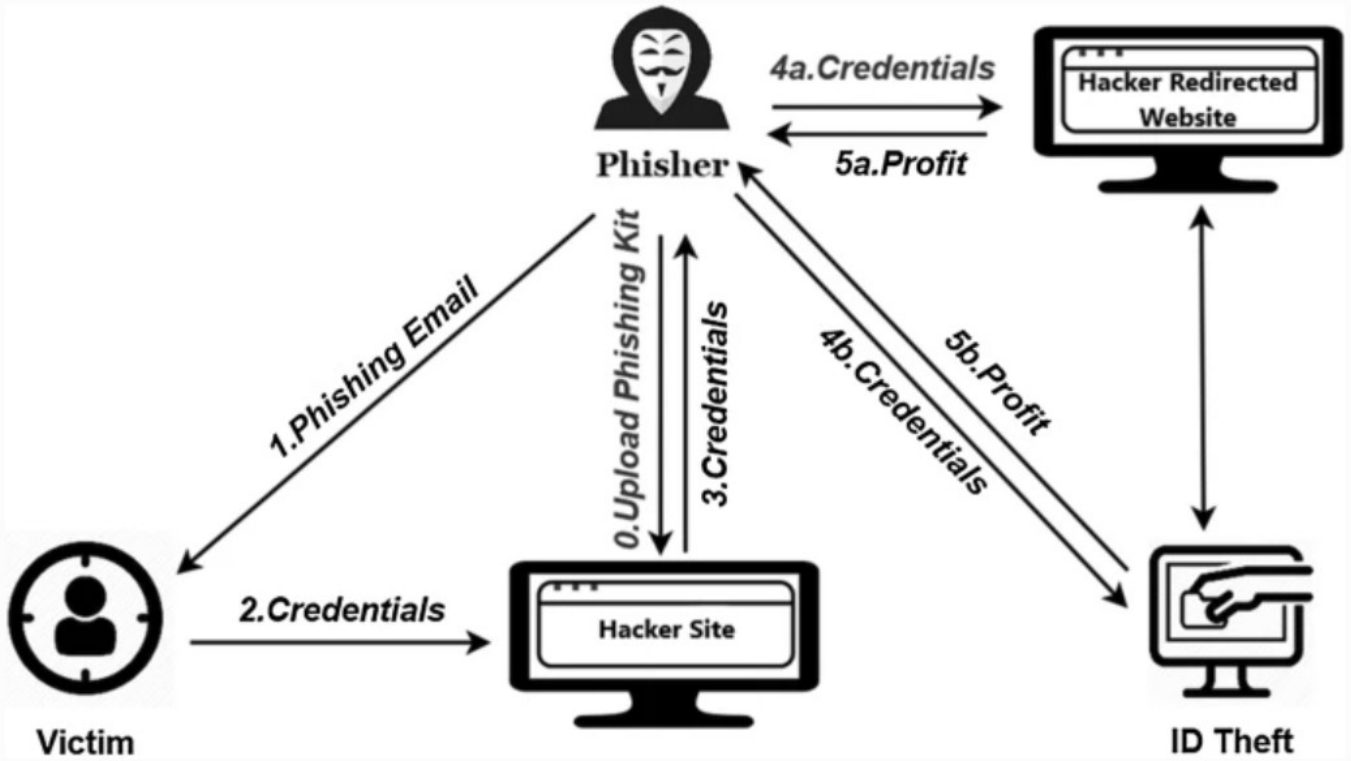
- Co to je phising?

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

ESET: „Phishing je typ kybernetického útoku pomocí technik sociálního inženýrství, kdy se útočník snaží získat důvěrná data oběti nebo spustit na zařízení oběti škodlivý kód.“

Phishing

Fig. 1



Phishing attack diagram [26]

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139-154.

Sociální inženýrství a phishing

- Manipulace s lidmi, zneužívání přirozených (naučených) sklonů za účelem získání něčeho
- Sociální inženýrství: často zahrnuje shromažďování informací o oběti před samotným útokem za účelem vybudování důvěry
- Phishing: obvykle nezahrnuje shromažďování informací

Jak se psychologie dívá na phishing

- Persuaze: centrální a periferní cesta
- Centrální - argumenty, logické uvažování, zvažování pro a proti
- Periferní – cokoli jiného, typicky emocionální přesvědčování
- Heuristiky - systematický model - zpracování informací - kognitivní zkratky

Heuristiky

- Místo pečlivého hodnocení lidé používají kognitivní zkratky (heuristiku)
- Jednoduché, praktické, zkrácené kroky vedoucí k rychlému posouzení situace
- Při posuzování pravděpodobnosti hodnotíme míru snadnosti či obtížnosti, s jakou si umíme představit výsledek
- První informace tvoří základ pro srovnávání (viz např. slevy v obchodech)
- Jsou to vlastně nesystematická vodítka pro hodnocení situace

Trust

- User trust plays a major role in "succumbing" to fraudulent emails (but also to fraud in general)
  - Towards service, institution, authority, medium
  - Towards a source of information
  - authority heuristic
- Kang, Bae, Zhang, Sundar (2011): people often build trust with a proximal source (online news)
- If a fraudulent email comes from a trusted source, it has a better chance of being successful

Poměr nákladů a přínosů

- Ekonomické teorie chování – lidé při rozhodování, jak se chovat, zvažují a balancují mezi náklady a přínosy
- „Lidské“ náklady: materiálové náklady, energie, čas
- „Lidské“ zisky: úspora energie a času
- Systematické hodnocení a centrální přesvědčování jsou (obvykle) dražší než heuristické a periferní
- Také proto je boj proti fake news drahý a obtížný

Phishing

- Úspěšný phishingový útok
  - musí podporovat/usnadňovat heuristické zpracování před systematickým
  - Tj. musí poskytovat jasné pokyny, které mohou uživatelé použít pro hodnocení, a co nejvíce ztížit systematické hodnocení

Aktivita pro studenty

- Phishing aktivita:
  - Získat finance
  - Získat heslo na Instagram
  - Získat heslo do IS

- Jaké principy jste použili?

Vytvořte návod, jak provést úspěšný phishingový útok.

Vytvořte také návod pro uživatele, jak se NEstát obětí vašeho phisingu, na co si mají dát pozor.

Heuristické podněty k phishingu

- Důvěryhodnost zdroje – autorita
  - Lidé se učí autoritě naslouchat
  - Známá instituce s dobrou pověstí (banka, policie, úřad)
  - E-mail od důvěryhodné osoby („přítel“, „ochranka“, „ředitel“…)
  - „Žánr“ zprávy – napodobení zpráv podobného formátu
- Gramatika, formální úprava sdělení, adekvátní jazyk
- Realistický obsah zprávy

Phishing

- Podporuje využívání periferní cesty přesvědčování
  - Emoce
  - Časový pres - je nutné jednat okamžitě
  - Hrozba - ztráta účtu / peněz / dat atd.
  - Možnost získat slevu / peníze / bonus
  - Výdělky - připíšeme vám bonus, vyhráli jste, za věrnost naší společnosti získáte…
  - Empatie – pomoc opuštěným psům
  - Zvědavost – podívejte se na žhavé dívky…

Phishing metody

TABLE 1 Key words for each of the Four Topics based upon Gragg's psychological triggers

Topic	Words
Factor 1: Reward	money, bank, million, cash, transfer, fund, banking, fortune, finances, capital, coin, finance, reward, price, sum, deposit
Factor 2: Urgency	help, critical, urgent, emergency, priority, dire, desperate, important, crucial, hurry, respond, please, assistance
Factor 3: Authority	authority, attorney, bank, company, firm, power, official, authorize, authorization, authorize, authorisation, lawyer, lawyers, attorneys, will, estate, business
Factor 4: Trust	trust, confidence, faith, confidential, care, custody, believe, confident, entrust, friend, mother, father, associate

Note: The words were identified based on key words synonyms as found in a thesaurus. This list was created prior to the analysis being conducted, however, it was fine-tuned to ensure it did not miss some relevant words manually postanalysis.

Stojnic, T., Vatsalan, D., & Arachchilage, N. A. (2021). Phishing email strategies: understanding cybercriminals' strategies of crafting phishing emails. *Security and privacy*, *4*(5), e165.

Phishing metody

Topic	Words
1	reply, needed, help, message, offer, urgently, get, read, fund, u
2	please, confidential, good, need, dear, day, attention, hello, greeting, id
3	content, mr, transfer, assistance, request, contact, payment, job, confirm, al
4	urgent, business, proposal, response, investment, treat, partnership, friend, dr, back

TABLE 6 Email subject header: LDA topic modeling

Topic	Words generated
1	million, late, transfer, contact, kin, class, since, assistance, decided, person
2	strong, money, fund, account, business, mr, nex, also, please, sum
3	bank, u, country, want, dollar, father, time, company, 0in, year
4	family, death, name, one, new, know, transaction, security, investment, http

TABLE 7 Email body: LDA topic modeling

Stojnic, T., Vatsalan, D., & Arachchilage, N. A. (2021). Phishing email strategies: understanding cybercriminals' strategies of crafting phishing emails. *Security and privacy*, *4*(5), e165.

Výsledky výzkumů

Phishing sites detection

- Dhamija et al. (2006)

- N = 22, 10 men, 18-56 years
- Experiment: 19 pages presented
- Original and phishing
- Respondents had to decide for each whether or not it was a fraudulent site, followed by interviews
- Total score: 6-18 correctly recognized pages (M = 11.6, SD = 3.2)

Types of respondents according to their strategies

- 1. Web content only
  - 23% (n = 5)They used only the content of the page (logos, layout, graphics, language, working links)

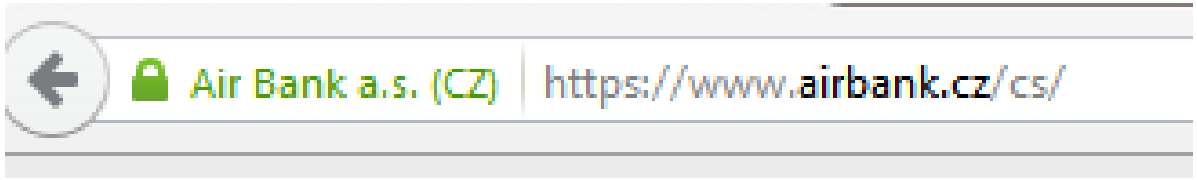
"*I never look at the letters and numbers up there* [in the address bar]. *I'm not sure what they are supposed to say*"

Types of respondents according to their strategies

- 2. Web content and domain
  - 36% (n = 8)
  - In addition to site content, they checked URLs (not SSL)
  - They recognized IP addresses instead of domains as suspicious, although they did not know what that meant

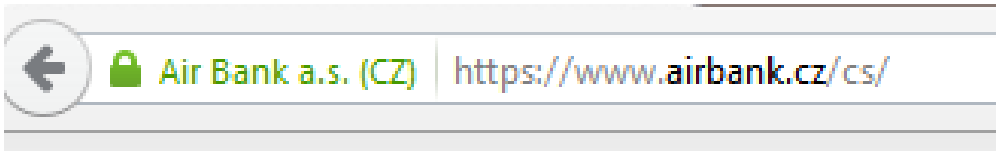
Types of respondents according to their strategies

- 3. Web content, url and https
  - 9% (n = 2)
  - They weren't looking for a lock icon
  - Some had never noticed her before



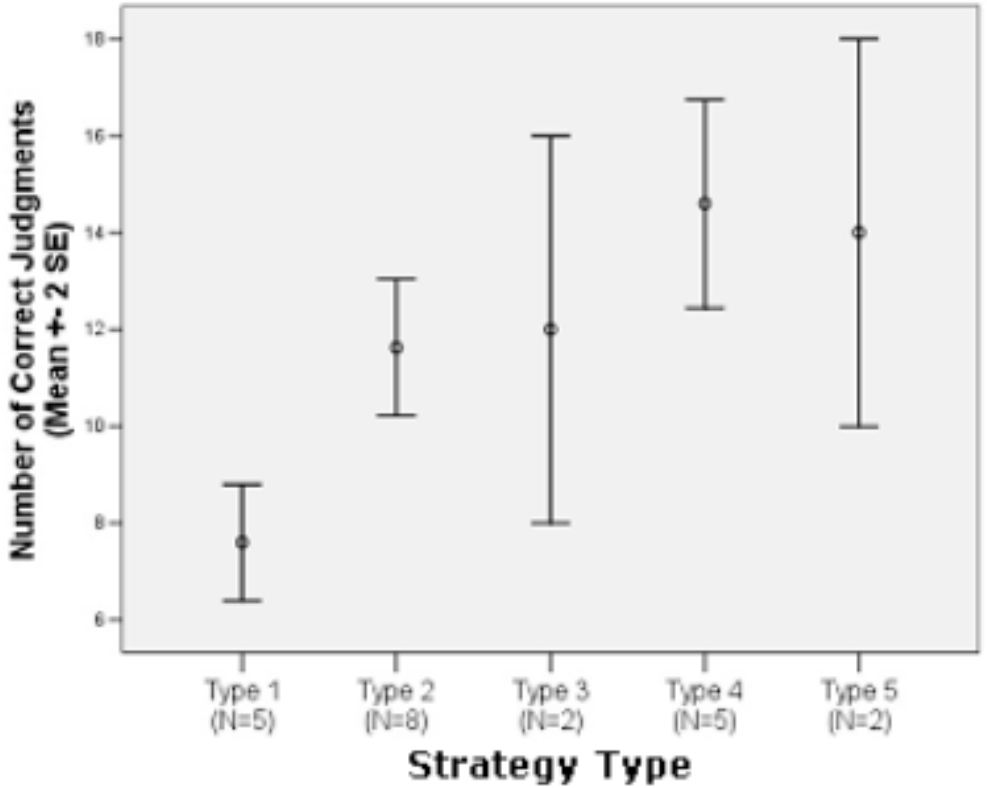
Types of respondents according to their strategies

- 4. in addition to the lock
  - 23% (n = 5)
  - They were looking for a lock, but some put more trust when it was on the site itself than at the url



Types of respondents according to their strategies

- 5. everything before + certificates
  - 9% (n = 2)



- Another strategy mentioned:
  - Entering a login and password as a strategy to determine if a page is genuine or not
- After showing the warning on the self-signed certificate:
  - 15 people (out of 22) automatically clicked on OK without reading
  - 18 did not know what the question was asking
    - *“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”*

More research

- Alsharnouby, Alaca, & Chiasson, (2015)
- 24 pages (10 mesh, 14 phishing), eye-tracker
- N = 21 (12 women), 18-51 (M = 27)
- 14 students (uni), 7 employees

- Elements:
  - Pages with distorted URLs
  - Pages with IP instead of URL
  - Fake browser
  - Pop-ups
  - SSL locks,…

Results

- Individual respondents 9-22 correctly (out of 24)
- For phishing sites, the success rate is 53% (but some were detected by mistake)
- For legitimate 79%

- Time of site evaluation - M = 87sec, nesig. difference between page types
- Men and women did not differ, no age differences (but a tiny sample)

- Respondents tended to make faster decisions about sites they knew (own bank site)

Eye-tracker

- 85% of the time they spent watching the site content
- 9% by tracking the page format
- 6% by tracking "areas of interest" - places where cues are relevant to detect phishing on the site

User strategy

- Viewing and assessing page content - the most reported strategy
- Testing the functionality of the site (change language, change country, click on links)
- URL check - however, many didn't know exactly what to focus on, rather emotionally "looks weird x looks normal„
- Search the site via google and compare
- Presence of SSL indicators (but also in the wrong places)

Differences 2006-2015

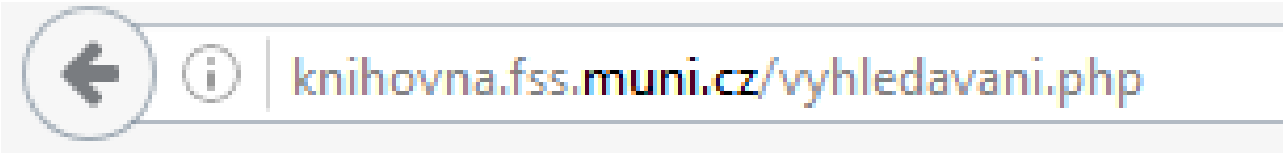
- 2006 - Respondents often did not even know what phishing was or that the site could be fully imitated
- 2015 - respondents knew about phishing
- But overall - rather ignorance, misunderstanding of the principles of operation of the site

Domain tricks

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

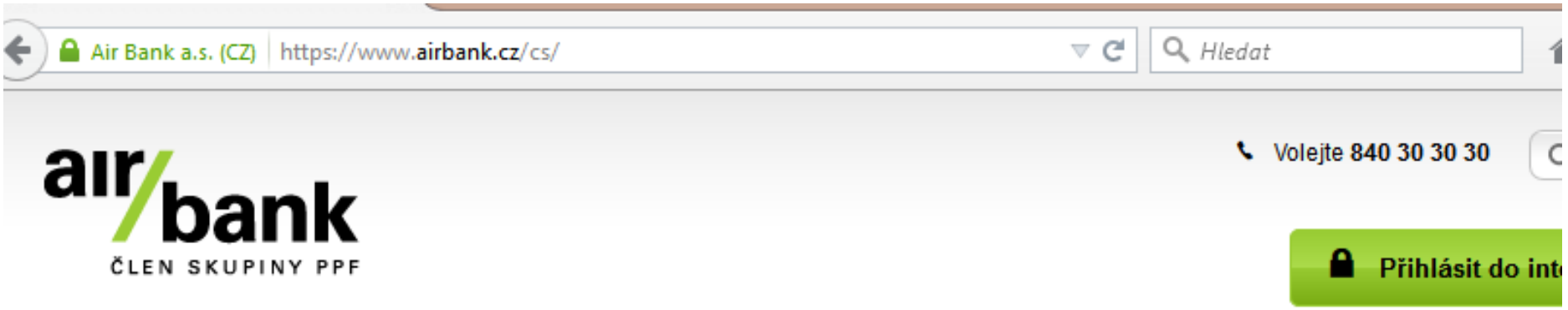
- www.bankofthevvorld.com
- www.paypai.com

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

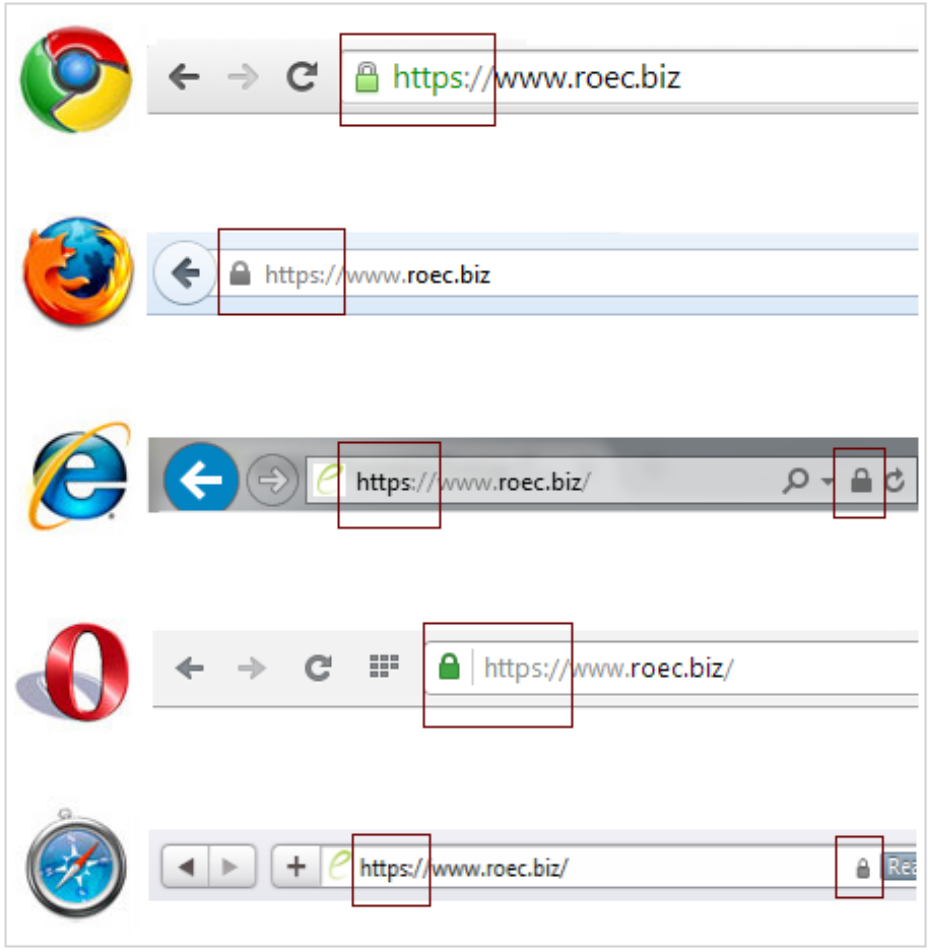


Other tricks

- Replacing visually similar characters (homographs)
- Pop-ups
- SSL



Http-Https


https://www.roec.biz
https://www.roec.biz
https://www.roec.biz/
https://www.roec.biz/
https://www.roec.biz/

What research is needed?

- Previous research has been about detecting phishing in people who knew they should detect it
- But what is the success rate of phishing "normally"?
- Difficult to determine - ethics versus external validity

Discussion: your ideas on the phising research?

Jagatic et al. (2005)

- Experimental research, phishing of passwords
- Two groups:
  - Social - email came from their friend (found from CIS)
  - Control - email from an unknown person

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

After end of the research…

- Jagatic et al. (2005)
- Lots of reactions from people (who didn't know they were part of the experiment)
  - Anger, blaming researchers
  - Denial (they wrote for a friend)
  - Misunderstanding - some thought that the researchers hacked into a friend's account
  - Underestimating the availability of information - some did not understand where researchers found out who their friends were
  - Complaints from those whose names and emails have been "misused" by researchers
- Ethics…!

More research

- 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”*

More often victims of phising

- Those who do not have a previous negative experience with phishing
- More often women
- More often successful if the sender of the opposite sex (especially for men)
- Those who claim to have low awareness of ICT security(students)
- More often from the fields: health care, business and pedagogy
- Older (and specifically seniors)

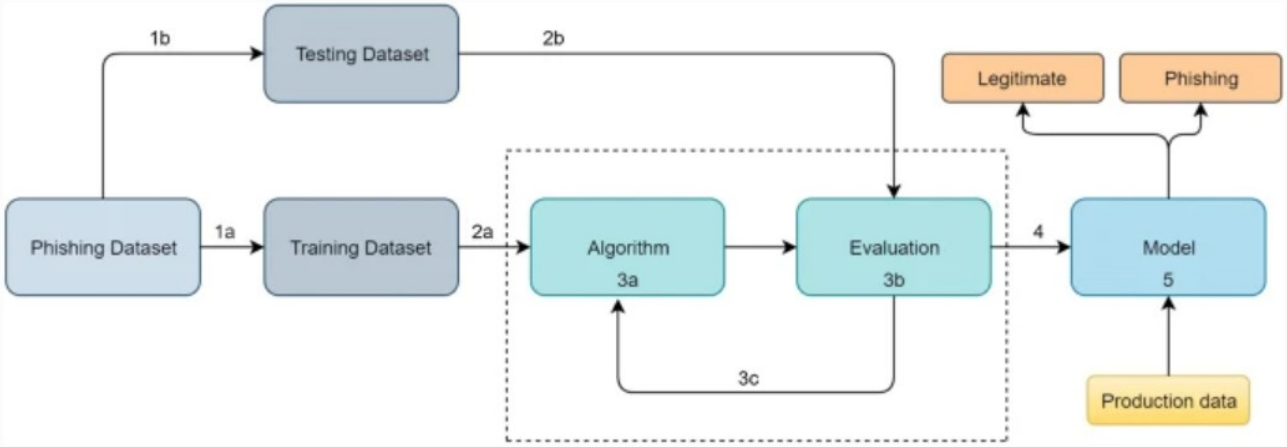
What we can do with phising?

- Technological solutions
  - Where possible, do them
- But phishing benefits from human (and not technical) mistakes, and technical solutions cannot filter everything
- You need to focus on the user
- Personality, motivation, abilities, knowledge

Phishing attack detection

- Deep learning for phishing attack detection
- Machine learning for phishing attack detection
- Scenario-based phishing attack detection
- Hybrid learning based Phishing attack detection

Fig. 6



Machine learning for phishing attack detection

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139-154.

Machine learning and phishing

Table 1 ML approaches for phishing websites detection

From: A comprehensive survey of AI-enabled phishing attacks detection techniques

Authors	Classification method	Feature selection method	Accuracy (%)
James et al. [36]	J48, JBK, SVM, NB	–	89.75
Abdelhamid et al. [9]	eDRI	–	93.5
Mao et al. [44]	SVM, RF, DT, AB	–	97.31
Jain and Gupta [34]	–	Feature extraction	99.09
Hota et al. [29]	CART, C4.5	RRFST	99.11
Ubing et al. [59]	EL	–	95.4
Chen and Chen [17]	ELM, SVM, LR, C$.5, LC-ELM, KNN, XGB	ANOVA	99.2

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139-154.

Machine learning and phishing

Table 4 Comparison of hybrid methods used in state-of-the-art

From: A comprehensive survey of AI-enabled phishing attacks detection techniques

Authors	Classification method	Accuracy (%)
Patil et al. [53]	LR, DT, RF	96.58
Niranjan et al. [48]	RC, KNN, IBK, LR, PART	97.3
Chiew et al. [19]	RF, C4.5, Part, SVM, NB	96.17
Pandey et al. [50]	RF, SVM	94

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139-154.

The effect of different trainings

- Carella et al. (2017)

- Three groups of 50 participants (students), the experiment took place over 7 weeks
  - Control
  - Document training that appears after clicking on a phishing email (emails during weeks 2, 5, and 8 of the experiment)
  - Training through classroom presentations (one presentation in the 2nd week)
  - They compare click through rates in links

Effect of education

After 7 weeks, the effect of training through presentations (although first a higher decrease) disappears and is comparable to no training

Average at the beginning - about half of people click on phishing

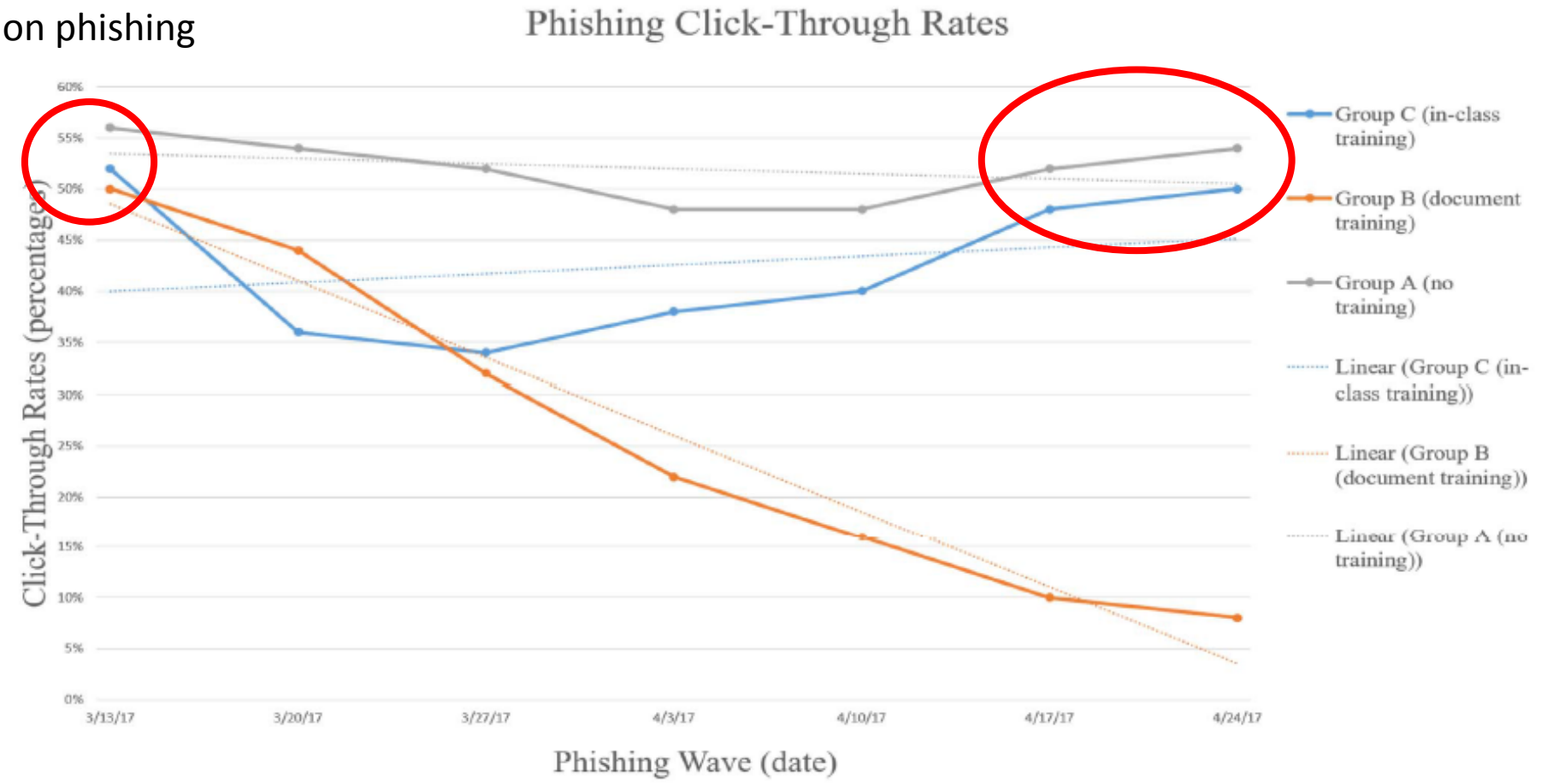


Figure 4. Phishing Click-Through Rates

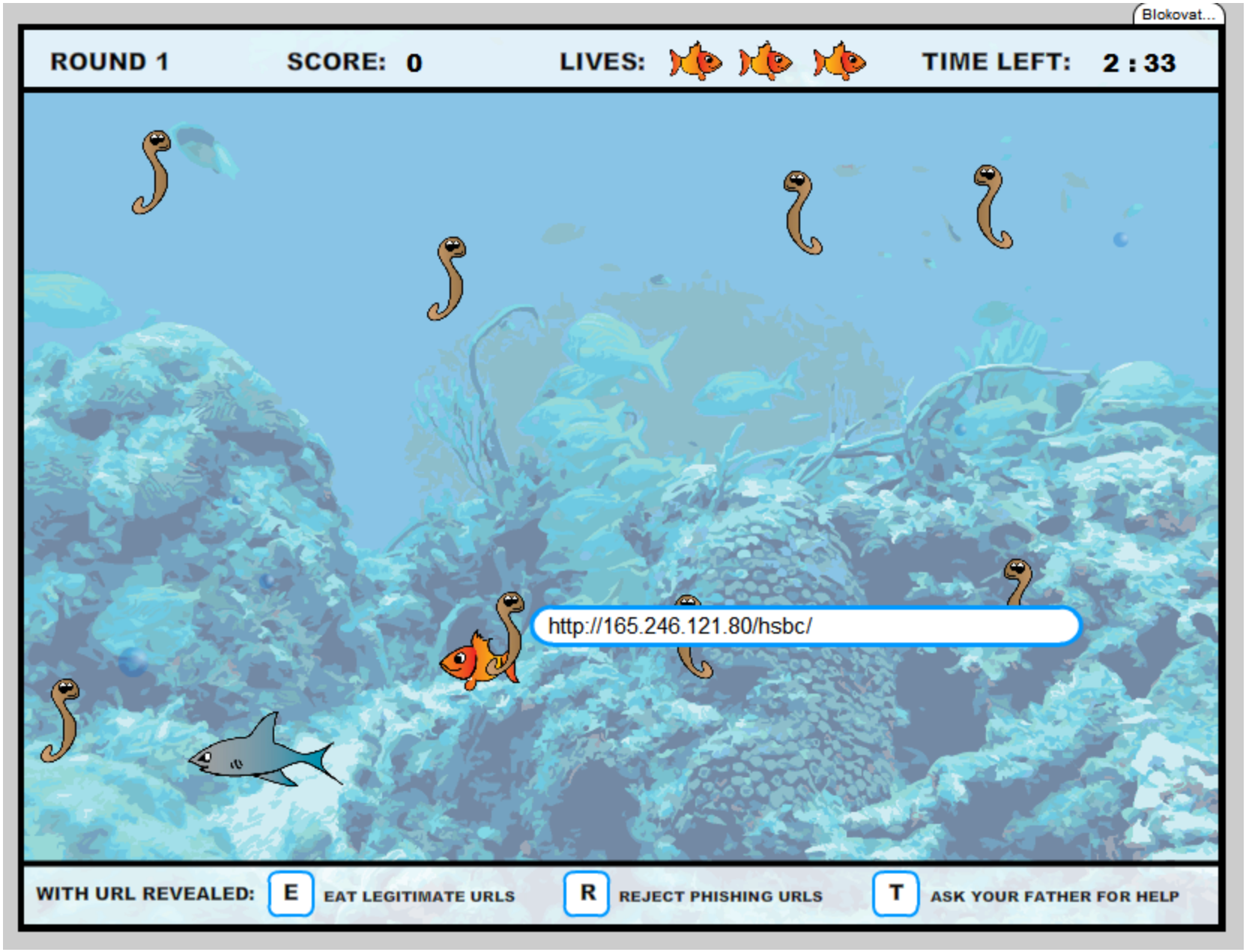
Training through negative experience - drop to 9%

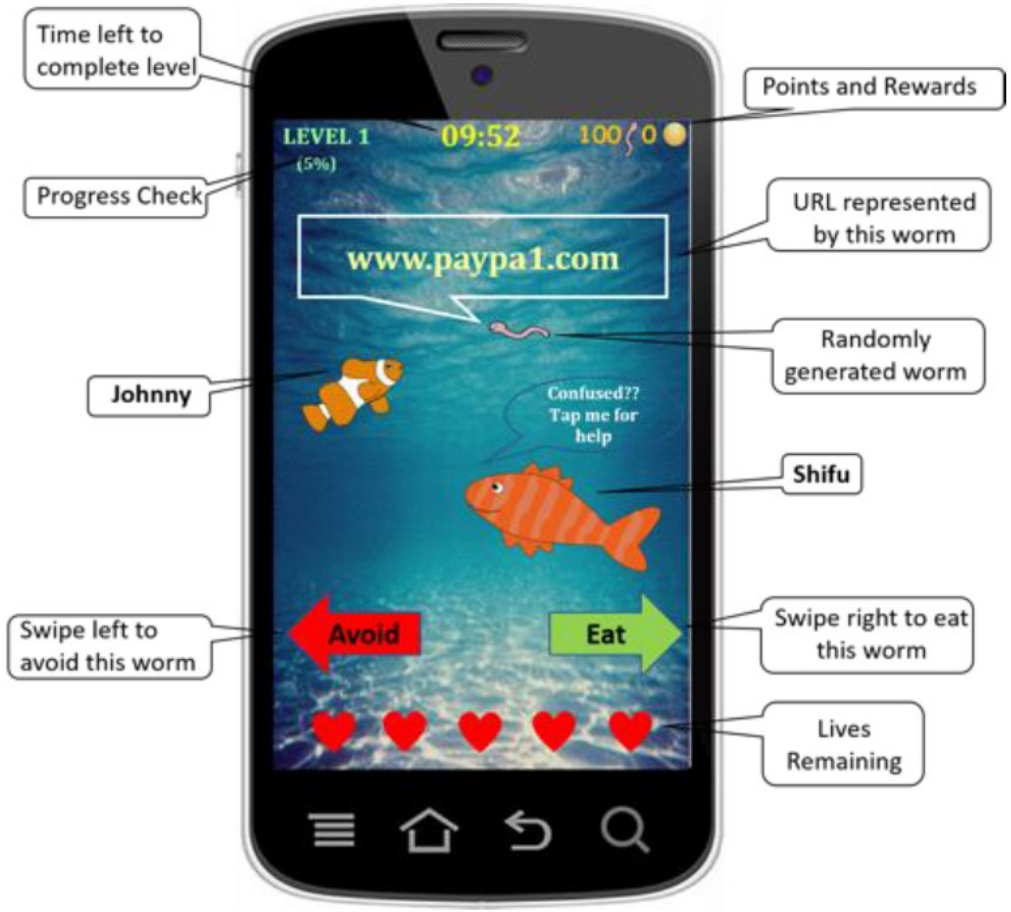
Education

- Most effective if immediately following a phishing attack

- Anti-phishing Phil: http://www.ucl.ac.uk/cert/antiphishing/
  - Browser app
  - After playing, users could more easily identify questionable pages
  - The effect is noticeable even after a week (the question of how after a long time…)

- Phish Phinder – in progress (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.