Phishing

Morgane Coat, Master's candidate

RCCP | Research Chair in Cybercrime Prevention

Briefing Note
Vol. 1 No. 5

Table of contents

The Research Chair in Cyber crime Prevention was created on the initiative of the University of Montreal, Desjardins and the National Bank of Canada. Led by Benoît Dupont, researcher at the International Centre for Comparative Criminology at the University of Montreal, its mission is to contribute to the advancement of research on cybercrime phenomena from the perspective of its prevention.

Definition and scope

Phishing is defined as "[a]ny email **falsely claiming to be from a legitimate organization** such as a financial institution, business or government agency **in an attempt to have the consumer surrender private and personal information**. The email may request or direct the consumer to visit a website where they are asked to update or provide personal and/or financial information".[1] In 2018, phishing was **the most reported type of online fraud in Canada**, with **1,966 victims filing 4,417 reports to the Canadian Anti-Fraud Centre for total losses of nearly $100,000**.[2] [3] **Approximately 1 in 14 people** targeted by phishing click on the link or open the attachment sent with the email.[4]

Victim profile

Most recent studies argue **that all individuals, regardless of socio-demographic characteristics** (e.g., sex, age, level of education, financial status), **are vulnerable to being targeted by phishing emails, clicking on links they contain and divulging personal information**.[5] [6] [7] [8] [9] However, **women seem to have a harder time distinguishing between fraudulent and legitimate web pages** once they've navigated to them from a link in a fraudulent email.[10]

Risk and protective factors

Factors that influence who gets targeted by phishing attempts

Many **online routine activities** (such as banking, making reservations, shopping and using social media) **increase people's risk of being targeted by phishing attacks**.[11]

It has also been shown that people with "**digital copying**" behaviour—meaning people who frequently copy, share and use software or digital content—**increase their risk of being targeted by phishing scams**. Since this behaviour is not always legal, it can further expose people to attacks by cybercriminals.[12]

Moreover, **security mecahnism** like antivirus software, email filters and intrusion detection systems **are not entirely effective** at protecting potential victims since they can't always stop phishing emails from reaching inboxes.[6,13]

Factors that influence who clicks on links and replies to phishing emails

The more people have experience with Internet and **the more they spend time online, the less likely they are** to reply to a phishing email.[14,15]

Both company employees and individuals are more likely to click on a fraudulent link **when the email contains a personal message or appears to come from someone they know**.[8,16,17]

Within companies, it has been shown that employees are **more likely to reply to a fraudulent email** when it contains **an element of urgency or comes from an authority figure**.[16,17] Workplace-specific factors, such as **the degree of exposure to internal and external emails**, the use of **centralized inboxes**, **employee workloads**, **whether or not employees suffer from information overload in the workplace** and **the extent to which social and technical support enhances employees' perception of their self-efficacy** (e.g., peer support, banners and help interfaces) have also been said to **influence the likelihood of clicking** on a phishing email.[16,19,20]

Habits and routine are also likely to increase someone's risk of falling victim to a phishing scam.[16,19,21]

People who **underestimate the likelihood of cyberattacks and their own vulnerability** to phishing attacks are more likely to click on a fraudulent email.[22] Moreover, two studies show that within the same country, **foreign nationals are less likely to pick up on cues in fraudulent emails** than nationals of the same country.[9,23]

Factors that influence who can detect fraudulent web pages opened from phishing emails

It has been shown that even more seasoned Internet-users **have a harder time detecting** fraudulent web pages when they contain **pop-up windows or images and icons of any kind** (such as animated graphics, images or (fake) security logos copied from Google).[10,24]

Some **people ignore or don't pay much attention to key cues**, such as the address bar, status bar and security logos. **Others don't necessarily trust security technology**, like SSL, to begin with. Others still are wary of mismatching domain and brand names (which can happen with third-party hosting of secure web pages).[10,24]

People who spend **more time inspecting a web page will not necessarily be more successful at detecting whether it's fraudulent**. There is an **anchoring effect** when it comes to detecting fraudulent web pages, meaning that cognitive bias leads a person to rely too heavily on the first piece of information offered. Spending more time inspecting a web page therefore doesn't necessarily help people detect fraudulent web pages any better.[10 24]

Recommendations

Training programs and public awareness campaigns need to be put out there in a variety of ways:[8 9 13 15 17 22]

- **Fraud Prevention Month;**
- **Raising public awareness through the media**
- **Warnings and tips** provided by financial institutions on their websites
- **Simulation exercises** to help people recognize fraudulent web pages and emails

These campaigns and training programs should put more emphasis on the following points:[7 12 24 18 19]

- **Behaviours that expose users** to phishing scams and **behaviours people can adopt to avoid being victimized**
- The **limitations of anti-fraud technologies**
- **The tangible consequences of phishing attacks**
- **Different cues that can help people recognize** and distinguish fraudulent emails and web pages from legitimate ones

Within organizations, experts recommend taking employees' specific work circumstances into account, in particular their **routine**, **habits and workload**, and even the **number of emails they receive**. Moreover, the use of **decision-making tools**, such as warnings, banners and updates about threats, can be very helpful to employees. **Checking with a peer** when in doubt is also recommended. When an employee reports an email, it's also recommended that supervisors **provide them with feedback** so they don't think reporting the email was a waste of their time. [19 20]

Study limitations

Among all these studies, **there is no consensus as to who should be considered a phishing victim** (opinions range from people who simply received fraudulent emails, to those who clicked on a link, to those who suffered a financial loss, to those who provided personal information).

Official statistics underestimate phishing cases since they're often reported under other categories of fraud, such as identity theft or hacking, which can result from phishing.[26] Moreover, many victims never realize that they have been targets of fraud.[27]

Most phishing researchers built their theoretical framework around **Cohen and Felson's routine activities theory**, which states that three factors must converge for a violation to occur: a **motivated offender**, an **accessible target** and the **absence of capable guardians**.[28] Very few other theories on phishing have been explored at this time.

References

[1] Canadian Anti-Fraud Centre (CAFC). (2019). *Mass Marketing Fraud: Recognize, Reject and Report it! Scam Digest: Ask us about fraud: A guide to recognizing and avoiding mass marketing fraud.* First Canadian Edition.

[2] Canadian Anti-Fraud Centre. (2019). Unpublished data.

[3] Whereas simple phishing consists of a broad attack not targeting any specific group (see, Leukfeldt, E.R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering*, *4*(5), 1–7), there is also a variant, called spear-phishing, which consists of a phishing email targeting specific people or groups, about which the fraudster will have conducted some preliminary research (see Chaudhry, J.A, Chaudhry, S.A and Rittenhouse, R.G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, *10*(1), 247–256). In 2018, in Canada, 197 reports of spear-phishing were made to the CAFC for losses of over $523,000 (for 116 victims).

[4] Verizon Business RISK Team (2017). 2017 Data breach investigations report. 10th edition. Verizon Business.

[5] The studies explain these results by the fact that the fraudsters appear to conduct broad attacks on the general population, without targeting specific groups.

[6] Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555.

[7] Jansen, J. and Leukfeldt, E. R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91.

[8] Moody, G. D., Galletta, D. F. and Dunn, B. K. (2017). Which phish get caught? An exploratory study of individual susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564–584.

[9] Broadhurst, R., Skinner, K., Sifnotis, N, Matamoros-Macias, B. and Ipsen, Y. (2018). Phishing and Cybercrime Risks in a University Student Community. *International Journal of Cybersecurity Intelligence and Cybercrime*, *2*(1), 4–23.

[10] Iuga, C., Nurse, J. R. C. and Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*(8), 1–20.

[11] Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396–411.

[12] De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L. and Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*, *35*(5), 1277–1287.

[13] Hutchings, A. and Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'Net'?.Current Issues in Criminal Justice, 20(3), 433–45.

[14] Horton, M. and Wimmer, H. (2017). Email phishing susceptibility in a public school setting: identifying at-risk educators. *International Journal of Cyber Society and Education*, *10*(1), 31–46.

[15] Wright, R. T. and Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273–303.

[16] Vishwanath, A., Herath, T., Chen, R. and Wang, J. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586.

[17] Gordon, W. J., Wright, A., Aiyagari, R. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA network open*, *2*(3), 1–9.

[18] Alseadoon, I. M. A. (2014). The impact of users' characteristics on their ability to detect phishing emails (Doctoral dissertation, Queensland University of Technology).

[19] Williams, E. J., Hinds, J. and Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1–13.

[20] Conway, D., Taib, R., Harris, M., Berkovsky, S., Yu, K. and Chen, F. (2017). A qualitative investigation of bank employee experiences of information security and phishing. In *Thirteenth Symposium on Usable Privacy and Security {SOUPS}*, Santa Clara, CA, 115–129.

[21] Vishwanath, A., Harrison, B. and Ng, Y. J. (2015). Suspicion, cognition, automaticity model (SCAM) of phishing susceptibility. *Communication Research*. DOI: 10.1177/0093650215627483.

[22] Halevi, T., Memon, N. and Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015).

[23] Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., Calic, D. and Lillie, M. (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. In *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, 1–12.

[24] Dhamija, R., Tygar, J. D. and Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 581–590.

[25] Downs, J.S., Holbrook, M. B. and Cranor, L.F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the second symposium on Usable privacy and security*, 79–90.

[26] Australian Competition and Consumer Commission (ACCC). (2019). Targeting Scams: Report of the ACCC on Scams Activity 2018.

[27] MacGibbon, A. (2005). *Australian e-Commerce Safety Guide 2005*.

[28] Cohen, L.E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *4*, 588–608.