Internet Fraud and Phishing Attacks - a European Perspective

Dorel Paraschiv[1], Liviu Toader[2], Maria Nițu[3] and Ștefan Negrea[4]
[1)2)3)4)] The Bucharest University of Economic Studies, Bucharest, Romania.
E-mail: dorel.paraschiv@ase.ro; E-mail: liviutoader2005@yahoo.com
E-mail: maria.nitu@rei.ase.ro; E-mail: stefannegrea@outlook.com

Please cite this paper as:
Paraschiv, D., Toader, L., Nitu, M. and Negrea, S., 2021. Internet Fraud and Phishing Attacks - a European Perspective. In: R. Pamfilie, V. Dinu, L. Tăchiciu, D. Pleșea, C. Vasiliu eds. 2021. *7th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Foggia, Italy, 3-5 June 2021. Bucharest: ASE, pp. 394-400
DOI: 10.24818/BASIQ/2021/07/051

Abstract

The IT developments and the expansion of e-commerce in recent years have generated a number of advantages for consumers, companies, but at the same time and with the same rapidity have developed online fraud which represents a real problem not only for the European countries, but also for the rest of the world. As a result of the restrictions imposed on the Covid-19 Pandemic and the relocation of the activity, mainly in the online environment, most payments were made through e-banking platforms and many employees worked from home, which contributed to the increase in the number of cyber-attacks, online fraud, especially phishing messages.

The objective of the paper is to present the cybersecurity environment along side its main threat - phishing, using the qualitative research method. And, using the quantitative research method, we can provide an overview of the correlation between individuals who are able to identify phishing messages, by possessing different degrees of internet literacy skills and those who possess lower internet literacy skills, thus unable to recognize phishing messages. Although there are methods that can reduce these threats, such as computer literacy and user education, criminals are able to constantly adapt and evolve bypassing them, in some cases succeeding in carrying out their illegal activities.

Keywords

Phishing, European Union, cyberspace, internet literacy, user education.
DOI: 10.24818/BASIQ/2021/07/051

Introduction

Along with the rapid expansion of e-commerce in the last couple of years, online frauds- phishing, email compromise, investment scam (Norris, Brookes and Dowell, 2019), committed through social engineering or online payment systems (Europol, 2020), have become a major problem in many European countries. Fraud covers a wide range of criminal activities united by some form of misrepresentation by a party to secure an advantage for that party or cause a disadvantage to others (Button and Cross, 2017). Different types of frauds have occurred long before the Internet and the evolution of the technology, especially related to digital communication, e-commerce and on-line payments, has only changed the means through which these offences are executed, not the desire and willingness of the offenders to engage in fraudulent activities. Technology and the widespread of Internet and social networking opened up new ways to perpetrate frauds and to industrialize old ones (Button and Cross, 2017), Phishing being a popular method used to steal sensitive information and personal data of users, through email or malicious websites (Alkhalil, et al., 2021).

Access to Internet expanded from traditional desktop computers to a wide range of mobile devices, including mobile phones and tablets, via mobile data networks that are able to achieve very fast connection speeds via 5G technology, as well as reliability, which outperforms the previous technologies (Singh, Casson and Chan, 2021). Also, new forms of social interaction, that were almost non-existent before the widespread of mobile computing, emerged through the wide range of social media platforms available today, thus people expose their personal data (Sahoo and Gupta, 2019), becoming vulnerable to various attacks. Technology substantially changed the way people buy goods and services and manage their finance through on-line banking systems.

Review of the scientific literature: Cybersecurity and Opportunities for on-line fraud

Technological progress in recent years has allowed communication and information technologies to create new opportunities for companies, consumers, governments, but also to generate a number of risks and vulnerabilities that can cause major harm to the actors involved (Nam, 2019). Cybersecurity is a combination of "computer security and securitization" (Lee and Kim, 2020, p.2), the ability to defend and protect cyberspace from possible attacks (NIST IR, 2011), in order to preserve the integrity of information, its availability and confidentiality (Lezzi, et al, 2018). At European level, attention has been focused on cybersecurity, and the EU NIS Directive 2016/1148 on the security of information and networks aimed at protecting digital and essential services, needs domestic capacity in the field of cybersecurity and an intensification of cooperation within the EU (Iaiani, et al., 2021). The criminals behind the attacks can be: activists, terrorists, criminals or dissatisfied employees (Iaiani, et al., 2021), and the means of attack are various: phishing, disruptive malware, online scams, data-harvesting malware (Interpol, 2020).

Phishing is a form of cyber attack, which creates an apparently legitimate website, but tries to illegally take sensitive personal data/information (Yang, et al., 2021), being an "automated configuration of social engineering" (Ghanzi-Tehrani and Pontell, 2021, pp.316) by which attackers use the internet in an illegal and fraudulent manner. Phishing websites can be of two types: concocted (fictitious sites for monetary gains) and spoof (imitating sites to transmit malware or identity theft) (Chen, et al., 2020).

Illegitimate on-line activities are correlated with their legitimate counterparts. Yar, et al. (2019) consider the Internet as a set of "social practices" through which some people will create distinct opportunities for offending. One of the main characteristics of many cyber related frauds is the geographical distance between the offender and the victim, which makes it easier for the offender to commit the fraud and harder to be detected by the victim (Duffield and Grabosky, 2001). A relevant example is phishing, in which case the potential victims receive an e-mail or message that looks like it's issued by a legitimate organization, such as a bank or other service provider, and requires a certain security sensitive action from the user, such as a password reset or disclosure of other private information. This example illustrates how the new technologies generate opportunities for fraud, as phishing probably would not have been possible at a large scale before the e-mail because it would have required a lot of effort and resources from the offender.

Just as businesses can use the technology to penetrate new markets or reach new consumers more cheaply, this is also true for cyber criminals (Button and Cross, 2017). The fraudsters moved from paper letters to e-mail, as now they can send out millions of e-mails at little or no costs. Such mass e-mail scams often include a scenario where the potential victim is asked to pay a small amount of money up-front in return for a promised large amount in the future (Smith, et al., 1999). Globalization is another important aspect of cyber-crime, as offenders will try to avoid detection and prosecution by exploiting the geographical jurisdictional boundaries, while expanding their cyber-crime horizons by targeting potential victims all around the world.

Phishing is the most common form of identity fraud

Identity Fraud is one of the most common form of fraud, as the victims are deceived into disclosing personal, sensitive information or participating in a fraudulent transaction rather than being persuaded to do so based on the belief that they will receive something valuable in return. Another form of identity fraud is represented by phishing scams, where the offenders impersonate an official body, such as a bank, government agency or service providers, in order to trick the victim into disclosing personal information, such as passwords, credit card numbers (Yang, et al., 2021), date of birth, pin codes and so on. Phishing attacks are generally initiated via an e-mail of an instant message which include a hyperlink to a deceptive internet website, which reproduces into detail the original website and appears to be legitimate but is in fact controlled by the offender. (Chaudhry, et al., 2016). Although phishing is one of the oldest types of cyber attack, originating in the early 1990s, it is still one of the most damaging and widespread type of attack, which can lead to major financial losses.

According to Deloitte (2019), 90% of data breaches in businesses are caused by phishing, with a 3.92 million USD average total cost of a data breach. A *Phishing and Email Fraud Statistics 2019*, presented by Retruster.com (2019) shows that 76% of businesses reported being a victim of phishing attacks in 2018, while 30% of the phishing messages get opened by the targeted users. According to the same report (Retruster, 2019), the total number of phishing attempts registered an increase with 65% in 2018, compared to the previous years. Technological advances and newly found vulnerabilities, combined with frequency of attack and the diversification of attack techniques increase the chances of a successful phishing attack. Even experienced users fail to detect around 29% of phishing attacks, while untrained ones are expected to successfully detect even less (Chaudhry, et al., 2016).

A phishing attack consists of three components (Chaudhry, et al., 2016):

- **The lure** represents the first step of a phishing attack and most commonly takes the form of a message that appears to be sent by a legitimate source, such as a bank, a government authority or a service provider. This message contains a hyperlink to the hook, which is the second component of a phishing attack. Link manipulation is done by fraudulently redirecting the potential victim to a fake website through different channels like e-mails, text messages and social media, described hereby as a hook. The usage of subdomains, hidden or misspelled URLs are some of the techniques used to trick the potential victims into accessing a fake website (Deloitte, 2019);

- **The hook** represents a malicious website that mimics the original website of a legitimate institution. The user is therefore tricked into disclosing confidential or personal information to this website as if the information was requested by the legitimate institution;

- **The catch** is the last phase, referring to the actual usage of the fraudulently collected information by the attackers. (Jakobsson and Myers, 2006).

All three components of a phishing attack typically include a series of technical tricks to make it more convincing for the potential victim, such as: modifying the apparent sender of the message or making it look like the message originates from a person the victim is familiar with, using logo, images and a visual style inspired by or copied from the original source, hiding and encoding the URL or making the message look more authentic by including security advice (Chaudhry, et al., 2016).

Research methodology

The article aims to provide an overview of the correlation between the population who identifies phishing messages by possessing various degrees of the internet literacy skills and the population who possesses lower internet literacy skills, thus being unable to recognise phishing messages. To achieve this objective, the first part of the article presents a qualitative research regarding cybersecurity and the main threat – *phishing* and its steps.

Next, a perspective on the phishing attacks in the European countries, is presented, as well as a quantitative method by combining data from Eurostat regarding the correlation between individuals who received “phishing” messages and individuals who have never used the internet in order to validate the hypothesis that a higher degree of internet literacy skills leads to identifying phishing messages.

Results and discussions - Phishing attacks in the European Union

According to Eurostat (2021), in the European Union, 25% of all individuals reported receiving fraudulent phishing messages. Denmark was the most affected by phishing attacks, as 45% of its' citizens declared they received fraudulent messages in 2019, followed by France and Sweden, both with 39% of individuals and Netherlands, with 38% of individuals. On the other hand, in Lithuania only 3% of the population was affected by phishing attacks via fraudulent messages. Latvia and Poland were also less affected by phishing attacks, with 6%, followed by Bulgaria and Greece, where 8% of population declared they received fraudulent phishing messages in 2019 (Eurostat, 2021).

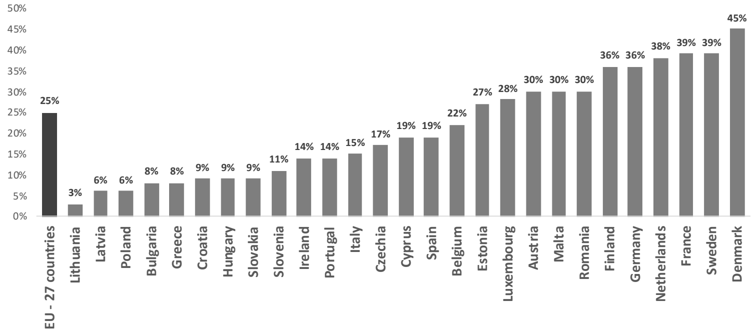

Figure no. 1. Individuals who received fraudulent *phishing* messages (%), 2019
Source: Eurostat, Security related problems experienced when using the internet, 2021

The data presented in Figure no. 1 are based on general population surveys, therefore it is reasonable to assume that it mainly reflects the ability of the general population of a specific country to identify and detect a potentially malicious internet message, either by human or machine detection, rather than the total number of actual phishing attacks registered in a specific country. The ability of a country's general population to identify a potentially malicious internet message is directly proportional to its' internet literacy skills, so a higher rate of detection of phishing attack corresponds to higher rate of internet literacy skills and vice versa. In order to validate this assumption, it is first necessary to make an assessment of each country's general population internet literacy skills. One main indicator used to make this assessment is the relative number of individuals who have never used the internet in each European country. A higher percentage of this population will suggest a lower degree of internet literacy skills nationwide. According to Eurostat (2021), in the entire European Union, an average of 10% of total individuals have never used the internet, while the remaining 90% of the population possess different degrees of computer skills and knowledge about the internet usage. While there are still a few exceptions, the most developed countries have lower internet illiteracy rates. Countries like Netherlands, Sweden and Denmark registered the lowest internet illiteracy rates, of 2% of the total population, while Bulgaria (24%) has the highest percentage of people who have never used the internet, more than double of the European Union average of 10%.

The Figure no. 2, referring to the percentage of individuals who have never used the internet (Eurostat, 2021), actually illustrates each country's internet illiteracy rate.

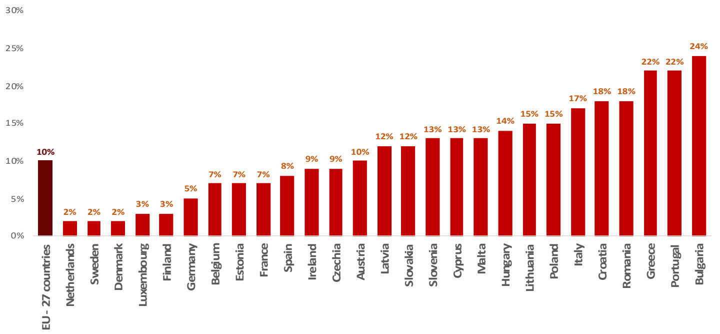

Figure no. 2. Individuals who have never used the internet (%), 2019
Source: Eurostat, Individuals - Internet use, 2021

The next step towards validating the hypothesis is to combine the information regarding the percentage of individuals who received fraudulent phishing messages and the percentage of individuals who have never used the internet in all the European countries and search for a statistically relevant correlation.

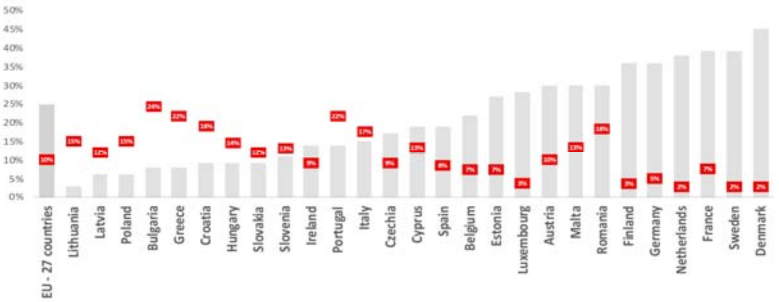

Figure no. 3. Individuals who received fraudulent "phishing" messages and individuals who have never used the internet (%), 2019

Sources: Eurostat, Security related problems experienced when using the internet and Eurostat, Individuals - Internet use, 2021

The combined data depicted in Figure no. 3 suggest a negative correlation between the two datasets: countries that registered a lower percentage of the population who declared receiving phishing messages, generally have a higher internet illiteracy rate among the general population, while most of the countries registering a higher percentage of malicious phishing attacks among the general population, have a lower internet illiteracy rate, therefore a large percentage of the population possess the necessary knowledge, abilities and technical means to access the internet with various degrees of digital and IT proficiencies.

Table no. 1. Individuals who received fraudulent *phishing* messages and individuals who have never used the internet (%), 2019

	Lithuania	Latvia	Poland	Bulgaria	Greece	Croatia	Hungary	Slovakia	Slovenia	Ireland	Portugal	Italy	Czechia	Cyprus	Spain	Belgium	Estonia	Luxembourg	Austria	Malta	Romania	Finland	Germany	Netherlands	France	Sweden	Denmark
Individuals who have never used the Internet (%)	15%	12%	15%	24%	22%	18%	14%	12%	13%	9%	22%	17%	9%	13%	8%	7%	7%	3%	10%	13%	18%	3%	5%	2%	7%	2%	2%
Individuals receiving fraudulent messages (%)	3%	6%	6%	8%	8%	9%	9%	9%	11%	14%	14%	15%	17%	19%	19%	22%	27%	28%	30%	30%	30%	36%	36%	38%	39%	39%	45%

Sources: Eurostat, Security related problems experienced when using the internet and Eurostat, Individuals - Internet use, 2021

Correlation is a measure of a monotonic relationship between two variables, either positive or negative. Therefore, in correlated data, a change in the magnitude of one variable is associated with a change in the magnitude of the other variable, either in the same direction, for positive correlation, or in the opposite direction for negative correlation. The Pearson correlation, commonly abbreviated as *r*, describes a linear relationship between two continuous, random variables, ranging from -1 to +1 (Schober, et al., 2018).

The Pearson correlation coefficient for the datasets shown in Table no. 1, for a total number of 27 countries is -0.73. According to Schober et al. (2018), in a conventional approach to interpreting a correlation coefficient, the observed value of -0.73 indicates a strong negative correlation, as it's absolute magnitude ranges between 0.70 and 0.89. The t-test absolute value is 5.308, with a corresponding p-value of 0.0000168. The p-value is considerably smaller than the significance level (α =0.05), indicating that the determined correlation coefficient is statistically relevant. Therefore, we can conclude that there is a strong negative corelation between the number of individuals who received fraudulent phishing messages and the number of individuals who have never used the internet, expressed as percentages of the total population, in the European Union countries.

Conclusion

The strong negative correlation between the percentage of the population who received phishing messages and the percentage of population who have never used the internet in all the European Union member states validates the hypothesis that the ability of the general population of a European country to identify a potentially malicious internet message, either by human or machine detection is strongly correlated with the degree of internet literacy skills among its citizens. Computer literacy and user education represent some of the most efficient methods to prevent phishing attacks. In most of the cases, the victims do not realize that they have been scammed, therefore the first step in defending oneself is the detection of the attack itself. The individuals' ability of using electronic communication, combined with basic analytical skills play a major role in successfully identifying phishing attacks. Some individuals may be more knowledgeable about internet security issues, either from previous experience or due to specific trainings, and possess the ability to identify a suspicious message or link faster or more accurate than other less experienced users. But most individuals do not have a good knowledge regarding the user interaction models of the systems they generally use, so it becomes easier for attackers to mimic the interface of some familiar web pages or internet applications and trick the users into transmit their personal information to the offenders (Chaudhry, et al., 2016). In addition to human detection of potential malicious messages, software tools and algorithms became increasingly efficient in detecting and neutralizing phishing attacks. Internet fraud will never be eradicated, and the methods used by the offenders will continue to evolve and adapt to the new technologies. Still, the threats can be minimized through computer and internet literacy and technological education for the general public, combined with widespread usage of end-user safeguard software solutions and up-to-date server-side security measures.

Acknowledgment

This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.

References

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I., 2021. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3, Article number: 563060.

Button, M. and Cross, C., 2017. *Cyber Frauds, Scams and their Victims*. Oxford: Routledge.

Chaudhry, J.A., Chaudhry, S.A. and Rittenhouse, R.G., 2016. Phishing Attacks and Defenses. *International Journal of Security and Its Applications*, 10(1), pp.247-256.

Chen, Y., Zahedi, F.M., Abbasi, A. and Dobolyi, D., 2021. Trust calibration of automated security IT artifacts: A multi-domain study of phishing-website detection tools. *Information & Management*, 58(1), Article number: 103394.

Deloitte, 2019. *Understanding phishing techniques.* [pdf] Available at: <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf> [Accessed 10 March 2021].

Duffield, G. and Grabosky, P., 2001. *The Psychology of Fraud*. Trends and Issues in Crime and Criminal Justice, no. 199. [pdf] Canberra: Australian Institute of Criminology. Available at <https://www.aic.gov.au/sites/default/files/2020-05/tandi199.pdf> [Accessed 6 March 2021].

Europol, 2020. *How criminals profit from the Covid-19 Pandemic*, [online]. Available at: <https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic> [Accessed 13 May 2021].

Eurostat, 2021. *Individuals-Internet use,* [online] Available at: <https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ifp_iu> [Accessed 10 March 2021].

Eurostat, 2021. *Security related problems experienced when using the internet,* [online] Available at: <https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_cisci_pb> [Accessed 10 March 2021].

Ghanzi-Tehrani, A.K. and Pontell, H.N., 2021. Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims & Offenders*, 16(3), pp.316-341.

Iaiani, M., et al, 2021. Analysis of Cybersecurity-related incidents in the process industry. *Reliability Engineering and System Safety*, 209, Article number: 107485.

INTERPOL, 2020. *Global landscape on Covid-10 cyberthreats.* [pdf] Available at: <file:///C:/Users/nitumaria11/Downloads/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf> [Accessed 5 March 2021].

Jakobsson, M. and Myers, S., 2006. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. New Jersey: Wiley.

Lee, C.S. and Kim, J.H., 2020. Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts. *Computers & Security*, 97, Article number: 101995.

Lezzi, M., Lazoi, M. and Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, 103, pp.97–110.

Nam, T., 2019. Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society,* 58, Article number: 101122.

NIST IR 7298, 2011. *Glossary of key information security terms, Revision 1*, [online] National Institute of Standards and Technology, US Department of Commerce. Available at: <https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf> [Accessed 5 March 2021].

Norris, G., Brookes, A. and Dowell, D, 2019. The psychology of internet Fraud Victimisation: A systematic Review. *Journal of Police and Criminal Psychology*, 34, pp.231-245

Retruster.com, 2019. *Phishing Statistics and Email Fraud Statistics,* [online] Available at: <https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html> [Accessed 10 March 2021].

Sahoo, S.R. and Gupta, B.B., 2019. Classification of various attacks and their defence mechanism in online social networks: a survey, *Enterprise Information Systems*, 13(6), pp.832-864.

Schober, P., Boer, C. and Schwarte, L.A., 2018. Correlation Coefficients: Appropriate Use and Interpretation. *Anesthesia & Analgesia*, 126(5), pp.1763-1768.

Singh, G., Casson, R. and Chan, W., 2021. The potential impact of 5G telecommunication technology on ophthalmology. *The Royal College of Ophthalmology*, *Eye*, [online] Available at: <https://www.nature.com/articles/s41433-021-01450-z> [Accessed May 13, 2021].

Smith, R.G., Holmes, M.N. and Kaufmann, R.G., 1999. *Nigerian Advanced Fee Fraud. Trends and Issues in Crime and Criminal Justice, no. 121.* [pdf] Canberra: Australian Institute of Criminology, Available at: <https://www.aic.gov.au/sites/default/files/2020-05/tandi121.pdf> [Accessed 10 March 2021].

Yang, L., Zhang, J., Wang, X., Li, Z., Li, Z. and He, Y., 2021. An improved ELM-based and data preprocessing integrated approach for phishing detection considering comprehensive features. *Expert Systems with Applications*, 165, Article number: 113863.

Yar, M. and Steinmetz, K.F., 2019. *Cybercrime and Society.* 3rd Edition. London: SAGE Publication.