РОЗДІЛ 2.
ОБЛІК ТА ФІНАНСИ

2.FEJEZET.
SZÁMVITEL ÉS PÉNZÜGYEK

CHAPTER 2.
ACCOUNTING AND FINANCE

DOI: 10.58423/2786-6742/2024-6-223-234
UDC 65.012.8:343.23

Nina POYDA-NOSYK
DSc in Economics, Professor, Professor at the Accounting and Auditing Department
Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education,
Beregove, Ukraine
ORCID ID: 0000-0002-5378-8028
Scopus Author ID: 57223373444

Botond Géza KÁLMÁN
Associate Professor at the Department of Economics and Management
Janos Kodolany University
Budapest, Hungary
ORCID ID: 0000-0002-5378-8028
Scopus Author ID: 57215096515

Szilárd MALATYINSZKI
Associate Professor at the Department of Economics and Management
Janos Kodolany University
Budapest, Hungary
ORCID ID: 0000-0002-1624-4902
Scopus Author ID: 58992302300

THE HUMAN FACTOR OF INFORMATION SECURITY: PHISHING IN CYBERCRIME

Анотація. *У даній статті досліджується обізнаність громадськості щодо практики фішингу в Угорщині, наголошується на мінливому розвитку кіберзлочинності та стратегічній важливості інформації в сучасному суспільстві. Дослідження вивчає методи та фактори, що сприяють успішним схемам фішингу, використовуючи статистичні дані для покращення розуміння та механізмів захисту від таких атак. Заглиблюючись у методи та психологічні тригери, які використовуються для обману жертв, дослідження має на меті забезпечити всебічне уявлення про фішингові загрози. Дослідження вивчає, чи впливають демографічні відмінності, освіта та використання Інтернету на сприйнятливість до фішингових атак. Перевіряються два основні припущення: 1) демографічні фактори впливають на знання та*

ставлення до фішингу та 2) люди часто не розпізнають спроби фішингу. Підкреслюючи важливість захисту на основі процесів над суто технічними інструментами, дослідження підкреслює, що рішення та знання користувача є вирішальними для захисту від фішингу. Безпека на основі процесів, включаючи блокування шкідливих сайтів і сповіщення користувачів, має важливе значення, причому значна відповідальність лежить на постачальниках послуг, державних і національних органах безпеки. Однак роль користувача є критично важливою як найслабша ланка в ланцюжку безпеки. Обговорюються технологічні досягнення в методах захисту, зазначається, що в міру того, як ці методи стають ефективнішими, зловмисники зміщують увагу з систем на персонал, який ними керує. Ця зміна підкреслює зростаюче значення людського фактору в безпеці в Інтернеті. Інциденти фішингу часто залишаються непоміченими, оскільки компанії вважають за краще компенсувати збитки, а не виявляти вразливі місця, побоюючись значної втрати клієнтів. Дослідження підкреслює цінність інформації як мішені для злочинців, так і як важливого знання для запобігання. Захист даних і поширення знань є важливими завданнями в боротьбі з IT-злочинністю, що підкреслює необхідність постійних досліджень і підвищення обізнаності.

Ключові слова: *кібербезпека, користувач, фішинг, інформація, дані.*

JEL Classification: L86, D83, K24, C88, L63

Absztrakt*. Ez a tanulmány az adathalász gyakorlatok köztudatát vizsgálja Magyarországon, hangsúlyozva a kiberbűnözés változó környezetét és az információ stratégiai fontosságát a mai társadalomban. A kutatás a sikeres adathalász sémákhoz hozzájáruló módszereket és tényezőket vizsgálja, statisztikai adatok felhasználásával az ilyen támadások megértésének és védekezésének javítására. Az áldozatok megtévesztésére használt technikák és pszichológiai kiváltó okok megismerésével a tanulmány átfogó képet kíván nyújtani az adathalász fenyegetésekről. A kutatás azt vizsgálja, hogy a demográfiai különbségek, az iskolai végzettség és az internethasználat befolyásolja-e az adathalász támadásokra való hajlamot. Két elsődleges feltevést tesztelünk: a demográfiai tényezők befolyásolják az adathalászattal kapcsolatos ismereteket és attitűdöket, és hogy az egyének gyakran nem ismerik fel az adathalász kísérleteket. A tanulmány kiemeli a folyamatalapú védelem fontosságát a tisztán technikai eszközökkel szemben, és hangsúlyozza, hogy a felhasználói döntések és ismeretek kulcsfontosságúak az adathalászat elleni védekezésben. A folyamatalapú biztonság, beleértve a rosszindulatú webhelyek blokkolását és a felhasználók értesítését, alapvető fontosságú, amely jelentős felelősséggel tartozik a szolgáltatókra, az állami és nemzetbiztonsági szervekre. A felhasználó szerepe azonban kritikus, mivel a biztonsági lánc leggyengébb láncszeme. Megvitatják a védelmi módszerek technológiai fejlődését, megjegyezve, hogy amint ezek a módszerek egyre hatékonyabbak, a támadók figyelmüket a rendszerekről az azokat üzemeltető személyzetre helyezik át. Ez az elmozdulás aláhúzza az emberi tényező növekvő jelentőségét az internetes biztonságban. Az adathalász incidenseket gyakran nem jelentik be, mivel a vállalatok inkább vállalják a veszteségeket, mintsem felfedjék a sebezhetőséget, tartva attól, hogy jelentős ügyfélveszteséget okoznak. A tanulmány hangsúlyozza az információ értékét, mind a bűnözők célpontjaként, mind pedig a megelőzés szempontjából kulcsfontosságú tudásként. Az adatok védelme és az ismeretek terjesztése alapvető feladat az informatikai bűnözés elleni küzdelemben, hangsúlyozva a folyamatos kutatás és tudatosság szükségességét.*

Kulcsszavak: *kiberbiztonság, felhasználó, adathalászat, információ, adatok.*

Abstract*. This study investigates public awareness of phishing practices in Hungary, emphasizing the evolving landscape of cybercrime and the strategic importance of information in contemporary society. The research examines the methods and factors contributing to successful phishing schemes, employing statistical data to enhance understanding and defense mechanisms against such attacks. By delving into the techniques and psychological triggers used to deceive victims, the study aims to provide a comprehensive view of phishing threats. The research explores whether demographic differences, education, and internet use influence susceptibility to phishing attacks. Two primary assumptions are*

tested: that demographic factors affect knowledge and attitudes about phishing, and that individuals frequently fail to recognize phishing attempts. Highlighting the importance of process-based protection over purely technical tools, the study stresses that user decisions and knowledge are crucial in defending against phishing. Process-based security, including blocking malicious sites and notifying users, is essential, with a significant responsibility resting on service providers, state, and national security agencies. However, the user's role is critical as the weakest link in the security chain. Technological advancements in defense methods are discussed, noting that as these methods become more effective, attackers shift their focus from systems to the personnel operating them. This shift underscores the increasing significance of the human factor in internet security. Phishing incidents often go unreported as companies prefer to absorb losses rather than reveal vulnerabilities, fearing significant customer loss. The study emphasizes the value of information, both as a target for criminals and as crucial knowledge for prevention. Protecting data and disseminating knowledge are essential tasks in combating IT crime, underscoring the need for ongoing research and awareness.

***Key words**: cybersecurity, user, phishing, information, data.*

Problem description. In the nearly half century since its publication, significant advancements have occurred in computer technology and computer networks. Presently, the Internet and digitization have permeated domains traditionally reliant on analog devices, spanning from timepieces to television broadcasting to telecommunication systems. The exponential growth is evidenced by the surge in Internet users from one hundred thousand in 1990 to 4.2 billion by 2018. Contemporary society heavily relies on mobile, hybrid, and web applications to enhance efficiency in both business operations and daily activities. Despite the convenience brought about by new devices such as smartphones and digital banking services, the evolution of the Internet is not devoid of challenges.

The Internet landscape also harbors detrimental aspects, exemplified by the proliferation of illicit activities within the gray or dark zones, including piracy, drug trafficking, pornography, and various forms of cybercrime. The financial gains from cybercrime are steadily increasing, propelled by technological advancements that equip malefactors with sophisticated tools at decreasing costs and the widespread adoption of the Internet, rendering cybercriminal activities lucrative investments.

The escalation of cybercrimes is exacerbated by misconceptions regarding online security, like the belief that sensitive data is primarily stored on well-secured corporate servers rather than on end-user devices. Recent incidents, such as the unauthorized access to over 1 billion official personal records from the Indian government database in 2018, debunk this notion. The World Economic Forum (WEF, 2019) has identified cybercrime as a prominent global risk with severe repercussions, particularly emphasizing the effectiveness of phishing and social engineering techniques in modern cybercriminal operations. Phishing, a prevalent cybercrime, poses threats to individuals, organizations, critical infrastructure, and national security. Its deceptive nature makes it challenging to detect well-crafted attacks, underscoring the pivotal role of user vigilance in thwarting cyber threats.

Malicious phishing is one of the most widespread cybercrimes [24, 28, 29, 30]. It equally threatens individuals, companies, the operation of critical infrastructure and the

state itself [33]. Its basic element is deception, so it is difficult to recognize well-prepared attacks. The responsible decision of the user is therefore the most critical element in any system [4, 6].

Analysis of recent research and publications. There are many examples of the typification of cybercrimes in the literature. The authors often list a large number of possible activities, from virus and worm attacks to e-mail messages all the way to identity theft, or following Z. Nagy [22], they talk about the indefinable scope, mass and high damage value of delicts.

The functional infrastructure is the primary basic service of the information society, which ensures the production, transmission, processing, acquisition and use of information [11]. The supporting infrastructure ensures its uninterrupted operation. The global IIS is a set of networks providing global information traffic, the best known of which is the Internet. Users are connected to the global network via the national infrastructure. The protection IIS ensures the protection of devices and networks used to store, manage, retrieve and display information [12]. However, this second definition of cybercrime ignores that in addition to/instead of IIS, the attack may also target the user. The entire range of targets is therefore fully formulated by Poonia [25].

Phishing, a form of cybercrime, involves perpetrators masquerading as reputable entities or organizations and initiating contact with their targets via email, phone, or text message. Through deceptive means, the criminals coax the targets into divulging "sensitive" information, including personal identification details, financial data (such as bank account and credit card information), and passwords. Subsequently, the acquired information is exploited to inflict financial harm or perpetrate identity theft [13, p. 3]. Hence, phishing can be construed as a type of social engineering tactic deployed to manipulate individuals into compromising their confidential data.

The definition of Whittaker et al. [32] approaches the problem of phishing sites in a similar way. According to them, the phishing site illegitimately presents itself as belonging to a trusted third party, inducing the user to behave in a way that he would only do at the request of the trusted third party. According to the division of the Europol European Cybercrime Center (2018), however, the social engineering is not a method of phishing, but a superordinate concept and hypernym. Kiss et al. [16] emphasize two characteristics of phishing. Firstly, the deception employed in phishing is indirect, implying that there is no direct interaction between the perpetrator and the victim. Secondly, the victim voluntarily furnishes the requested data to the phisher through online channels. The diverse terminology associated with the concept signifies the absence of a universally standardized definition. Nevertheless, it is unequivocal that phishing hinges on two essential components: the presence of a computer and access to the Internet. Furthermore, a third critical factor, termed the human factor, encompasses both the perpetrator and the user. Noteworthy common attributes of phishing include organizational structures, division of labor among perpetrators, and the utilization of automation in executing fraudulent activities.

Phishing and related research are based on scientific theories. Theoretical criminology deals not only with theories about the development and conditions of crimes, but also with victims and perpetrators. Since my own research related to this

thesis focuses primarily on the former, in this chapter I review the theories related to victimization. Early theories primarily dealt with the classification of phishing attack methods and their treatment as a process [14]. Later, theories describing and explaining circumstances, causes and motivations using the knowledge of related sciences appeared. One of these is the TTAT created by Liang and Xue [18]. The theory scrutinizes and elucidates potential strategies for mitigating technological hazards, with a primary focus on assessing what individual users can undertake to avert such dangers. The scrutiny of user behavior holds paramount importance, as it is evident that the user constitutes the most vulnerable link in information technology security [2].

Gupta et al. [9] classified the types of phishing as follows: technological and social an engineering type is separated.

Highlighting previously unresolved parts of the overall problem. An investigation conducted in Hungary in 2019 aimed to assess public awareness of malicious phishing practices, emphasizing the evolving landscape of cybercrime and the strategic importance of information in contemporary society.

The study delves into the morphology of cybercrime, focusing on the modus operandi and factors contributing to the success of phishing schemes. It elucidates the techniques and psychological triggers employed in deceiving victims, drawing insights from statistical data to enhance understanding and defense mechanisms against phishing attacks. Additionally, criminological theories pertaining to IT-related crimes and victimization are explored to elucidate the underlying causes and preventive measures against cyber threats.

Goals of the article. This article aims to explore whether demographic differences, education, and internet use are related to susceptibility to phishing attacks. To address this research question, data from the literature and original research results were utilized.

The objective was to test two initial assumptions: first that knowledge and attitudes about phishing exhibit demographic differences; and second, that individuals often fail to recognize phishing attacks. The idea of this paper was to highlight the importance of the topic and the need for appropriate and conscious defense against phishing. While technical tools such as spam filters, anti-viruses, and firewalls play a significant role, process-based protection is deemed more critical than technical security. Process-based security includes blocking malicious sites and notifying users, which is a responsibility of service providers, state, and national security agencies. However, the user is a crucial link in the security chain, as the success or prevention of a cyber attack in a phishing situation often depends on user decisions. In this context, the role of knowledge and information is paramount, enabling end users to make informed decisions.

Presentation of the main research material. Figure 1 shows the percentage of crime types using the world's 2018 cybercrime statistics [23].

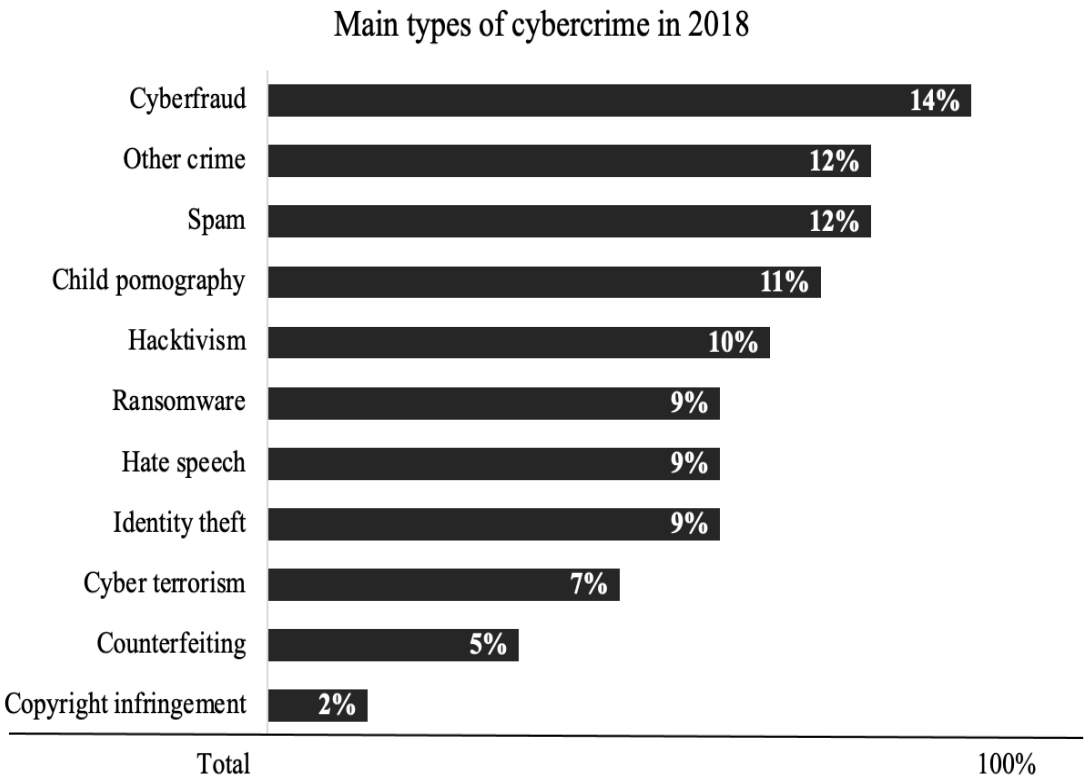

Fig. 1. Distribution of the main types of cybercrime in 2018*

**Source: own editing based on [23]*

Phishing is not included as a separate category here, which can occur as part of many forms of crime, from identity theft to internet fraud and spamming to cyber terrorism. Based on the figure, among online crimes, cyber fraud and spamming are the most common, but from the point of view of social danger, child pornography and hate speech are the most important. Their frequency is not far behind spam. From the point of view of strategic-tactical danger, however, cyber terrorism should be highlighted, mainly due to the destruction of infrastructure and communication. However, since 2012, phishing has been listed separately in the FBI's cybercrime statistics. The number of victims and the financial loss caused by phishing is increasing every year, which clearly shows the topicality and importance of the topic.

Phislabs' statistical analysis [24], the most frequently affected target sector, e-mails, accounts for a quarter of all cases. However, actions related to financial matters and payment services together account for even more, more than a third of all cases (Figure 2).

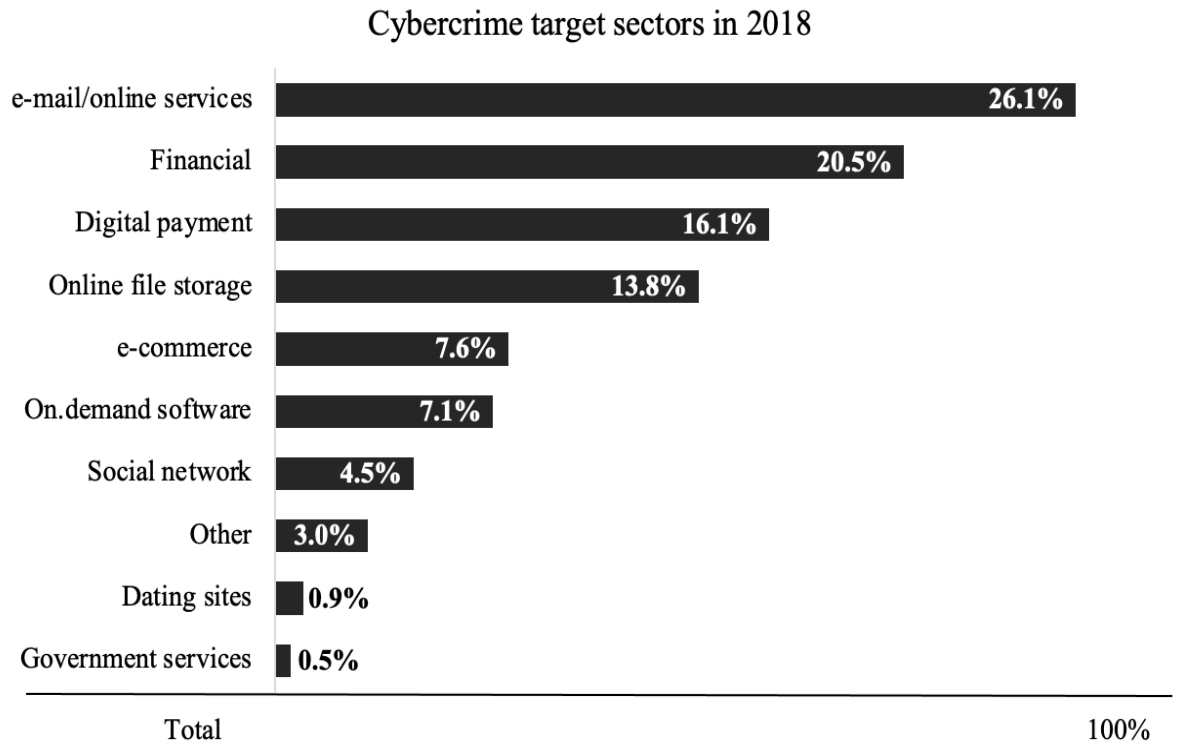

Fig. 2. Target sectors of cybercrime*

**Source: own editing based on [24].*

Among the traditional phishing attacks, those aimed at opening especially malicious attachments have increased significantly, also using attachment types such as pdf or arj, which were thought to be safe for a long time. Cybercriminals have also made significant improvements in phishing techniques implemented via mobile devices: 21% more clicks were made on links to phishing sites from Facebook pages optimized for mobile devices than in the case of the computer-optimized version [8].

Anti-phishing organisations regularly publish statistics on the topic of phishing. Also an international consortium called Working Group (hereinafter: APWG; 2010-2018), which was founded in 2003 and now has more than 3,000 members. Among others, they are members of world-famous security companies such as BitDefender, Symantec, McAfee, as well as business "giants" such as ING Group, VISA, MasterCard, or American Bankers. Association. Their quarterly publication describes not only the current involvement and risk statistics, but also the most common techniques, the most attacked sectors (currently the banking sector and e-commerce) and, for example, the domains that are most often used by phishing cybercriminals. The top 20 list of these countries, e.g. In the fourth quarter of 2018, ".com" sites were in the lead with an overwhelming advantage, but several African countries (Mali, Gabon, Central African Republic) also ranked high (just think of the “Nigerian letter” method). Comparing the data of older publications (Q4 2009) with the latest (Q4 2018), the trends are also clearly visible. Between 2009 and 2018, the number of phishing sites detected per month increased from 30,000 to 50,000. The most vulnerable sectors, however, have always

been financial and payment services that can be linked to money (almost 50% of all attacks target these, but this value is supplemented by the use of the webmail sector to obtain banking data, for example through phishing). The statistics also show that the goals have changed over the course of a decade, and instead of money, information has increasingly become the valuable "booty". PhishLabs [24] reported similar trends.

Finally, it is important to mention that Europol also has its own statistics. According to them, phishing has been reported in nearly 75% of EU member states, and phishing investigations are underway in 40%. Based on these data, the expected trend of phishing shows an increasing trend. Since the body's statistics only include closed - or ongoing - cases, the most frequently used technique is the installation of malware (malicious program) on the target person's device for the purpose of data theft. Although the trend of phishing is on the rise, fortunately most of the targeted people already recognize that something is wrong - and only 4% click on the link [7].

There are many theories related to cybercrime and phishing. Some theories focus on victims, specifically the causes and factors of victimization. These theories of victimization are the focus of this research as well, as it aims to understand why and how individuals become victims in cyberspace.

Criminological theories are categorized in various ways in the literature. From the system described by A. Borbíró [3], theories more closely related to phishing were highlighted. The foundation of this research on cybercrime is Cohen and Felson's [5] routine activity theory, which posits that three factors are necessary for a crime to occur:

- A motivated offender (capable and willing to commit the crime),
- An attractive target,
- Inadequate supervision/guarding (lack of personal or equipment protection).

The theory is also valid for online crime, as Pratt, Holtfreter and Reisig [26], Maimon et al. [20], and Jansen and Leukfeldt [15] have proven with their studies.

The diversity of cybercrimes that the perpetrators also act on the basis on multiple motivations [21]. The same can be said about the victims. Several factors contribute not only to becoming a criminal but also to becoming a victim, as outlined in [17]. For example, the desire for importance, fame or money can make individuals susceptible to frauds, such as the classic "Nigerian letter" scheme. The need to feel important can also manifest itself in self-indulgence. For this reason, someone can become a victim of phishing, identity thieves or cyberbullying due to their Facebook activities. Money is also the motivating factor when the user decides to download illegal content or hacked programs instead of legitimate content. This is because in general, not only does he infringe copyrights, but he also becomes a victim, for example, as a result of malicious programs being downloaded without his knowledge. A typical example of this is when installing a hacked antivirus actually installs malware, which even disables existing protection. Since money is the most important motivational factor, the attacks on it can be many. Any crime can occur, from phishing that obtains bank card data and online banking access to physical card theft [30]. It is much rarer, but it also happens that someone clicks on a phishing link out of a desire for knowledge. A much more common

motivation is curiosity. In addition to the desire for entertainment and ideological influences, comfort, laziness or impatience often override common sense.

From the early days of theoretical criminology, the researchers of crime theories investigating biological causes were and are still being investigated in many areas. Lombroso only studied anthropological characteristics, today the field of genetics and neurotransmitters is the target of the studies. Related to this is the description of the role of the amygdala and stress in relation to phishing [10]. In human decisions, behavior is controlled by ancient brain areas such as the limbic system and one of its areas, the so-called amygdala. The paths starting from here pass through areas of the brain that are developmentally ancient regions, older than the cortical fields responsible for logical thinking, and primarily play a role in triggering instinctive actions. However, instinctive decisions usually take place among the options that can be taken into account on average, the individual specification of the given situation is then completely left out of the calculation. Hadnagy and Fincher [10] list a number of manipulative techniques, all of which have in common that the adrenal glands release stress hormones into the blood, which raise the blood pressure, the heart rate accelerates, the pupil dilates, all the body's essential blood supply is reorganized to the muscles - in short, the body prepares to "run" or hit" in response. This is the so-called Canon emergency response, which is extremely useful for survival, and then it goes off and everything goes back to rest. A constant state of excitement, on the other hand, damages the body - this is stress defined by János Selye.

Another modern offshoot of early biological theories is the theory of intelligence. The distribution of the population based on intelligence level follows a Gaussian curve. It can be assumed that the victims can be located in any part of the bell curve. However, as a result of the sophisticated methods of phishing, anyone can become a potential victim. The success achieved by the user in this area has two basic conditions: the perceived threat and the motivation that develops as a result. The relationship between these and the result of their combined effect on users is illustrated by the following matrix (Table 1)

Table 1.

TTAT[1] matrix*

The nature of the threat		
	can be detected	*not detectable*
avoidable	action	no action
cannot be avoided	no action	no action

**Source: own editing based on [18].*

Routine action is suitable for explaining victimization. The third factor of the routine action theory, defense, is discussed in itself by Rogers' defense motivation theory of cognitive sociology [27]. According to this, he decides whether the subject implements defensive behavior based on the evaluation of two factors. One is the degree of threat, and the other is the assessment of whether it is worth protecting yourself. The extent of the threat is determined by the expected severity of the event and the

[1]Technology Threat Avoidance Theory

vulnerability of the threatened party, as well as the advantage/disadvantage resulting from the situation. In judging the response, the decision is made on the basis of how effective the response is, as well as the defense itself and how big the victims are with the defense. These factors are described similarly to mathematical equations:

$$\begin{array}{l} \text{severity + vulnerability} - \frac{\text{benefit}}{\text{drawback}} = \text{threat} \\ \text{efficiency - casualties} = \text{response} \\ \hline \text{threat + response} = \text{defense motivation} \end{array} \quad (1)$$

As the end result of the "system of equations", the defense motivation level is determined. This level dictates whether individuals under attack will defend themselves and, if so, what method they will choose for their defense.

Conclusions and prospects for further research. Technological progress continues to develop new defense methods against online attacks. Many of these methods are so innovative and significant that they are protected by patent law, such as Gupta et al.'s method for filtering out phishing websites. As the effectiveness of defense methods increases, malicious attackers often shift their focus from targeting systems to targeting the personnel operating them. Consequently, the role of the human factor in internet security is becoming increasingly important.

Phishing, unfortunately, shares a high level of latency as a crime. Companies often choose to remain silent and absorb the losses rather than disclose their vulnerabilities, as admitting to such weaknesses can lead to significant customer loss.

Research indicates that information is a valuable asset. This applies to both the data targeted by criminals and the knowledge about prevention. Protecting data and disseminating knowledge are key tasks in efforts to combat IT crime, a point to be emphasised in further research.

References

1. Anti-Phishing Working Group (2009-2018) Phishing Activity Trends. Available from: https://www.antiphishing.org/resources/apwg-reports/ (last accessed: February 2, 2024)
2. Arachchilage and Love, S. (2013). A game design framework to avoid phishing attacks. Computers in Human Behavior 29 (3), 706-714. DOI : https://doi.org/10.1016/j.chb.2012.12.018
3. Borbíró, A. (2016). Kriminológiaelmélet: bűnözésmagyarázatok (Theory of Criminology. Crime Explains – in Hungarian) In: Borbíró, A., Gönczöl, K., Kerezsi, K., Lévay, M. (szerk.). Kriminológia. Budapest: Wolters-Kluwer, 29-313. o.
4. CERT Insider Threat Team (2013). Unintentional Insider Threats: A Foundational Study. Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744 (last accessed: March 3, 2024)
5. Cohen, LE and Felson, M. (1979). Social Change and Crime Rate Trends : The Routine Activity Approach. American Sociological Review, 44 (4), 588-608. DOI : 10.2307/2094589
6. Cranor, LF (2008). Framework for Reasoning About the Human in the Loop. Proceedings of Usability, Psychology & Security (UPSEC). Available at: https://www.usenix.org/legacy/event/upsec08/ tech/full_papers/cranor/cranor.pdf (last accessed: April 4, 2024)

7. Europol (2018). Internet organised crime threat assessment (IOCTA). Available from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (last accessed: May 5, 2024)
8. Gupta, S. and Kumaraguru, P. (2014). Emerging Phishing Trends and Effectiveness of the Anti-Phishing Landing Page. APWG Symposium you Electronic Crime Research (eCrime). 36-47. DOI: 10.1109/ecrime.2014.6963163
9. Gupta, BB, Nalin, A., & Kostas, P. (2017). Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. Telecommunication Systems. DOI : 10.1007/s11235-017-0334-z
10. Hadnagy, C. & Fincher, M. (2015). Phishing Dark Waters – The Offensive and Defensive Sides of Malicious Emails, Indianapolis: Wiley. Available from: https://the-eye.eu/public/Books/HumbleBundle/phishingdarkwaters.pdf (last accessed: June 6, 2024)
11. Haig, Zs. & Várhegyi, I. (2005). Hadviselés az információs hadszíntéren (Warfare on the information battlefield – in Hungarian). Budapest: Zrínyi Kiadó.
12. Haig, Zs., Hajnal, B., Kovács, L., Muha, L. & Sik Z. N. (2009). A kritikus információs infrastruktúrák meghatározásának módszertana (Methodology for defining critical information infrastructures – in Hungarian). ENO Advisory Kft.
13. Jakobsson, M. & Myers S. (2007). Phishing and countermeasures: understanding the increasing problem of electronic identity theft John Wiley & Sons, Inc.
14. Jakobsson, M. (2005). Modeling and Preventing Phishing Attacks. In: Patrick A.S. & Yung M. szerk., Financial Cryptography and Data Security Berlin: Springer, 89-108. o. DOI: 10.1007/11507840_9
15. Jansen, J. and Leukfeldt, R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading lake Victimization. International Journal of Cyber Criminology, 10 (1), 79-91
16. Kiss, T. & Parti K., Prazsák G. (2019). Cyberdeviancia (Cyberdeviance – in Hungarian). Budapest: Dialóg Campus Kiadó, Budapest.
17. Kovács-Angel, M. (2019). 8 év börtönt kaphat az etikus hacker, aki szólt a Magyar Telekomnak egy biztonsági résről (The ethical hacker who told Magyar Telekom about a security hole could be jailed for 8 years – in Hungarian). 24.hu. január 27. Available: https://24.hu/belfold/2019/01/27/etikus-hacker-telekom/
18. Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly 33 (1), 71-90. DOI: 10.2307/20650279
19. Long, RM (2013). Using Phishing to Test Social Engineering Awareness of Financial Employees. MSc. Eastern Washington University. doi : 10.13140/RG.2.1.3846.0565
20. Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily Trends and Origin of Computer-Focused Crimes Against a Large University Computer Network: An Application of the Routine-Activities and Lifestyle Perspective. British Journal of Criminology 53 (2), 319-343. doi : 10.1093/ bjc /azs067
21. Mendi-Kozma, L. (2016). A kiberbűnözés egyes aspektusai – az online zaklatás (Some Aspects of Cybercrime - Online Bullying – in Hungarian). Károli Gáspár Református Egyetem Állam-és Jogtudományi Kar
22. Nagy, Z. A. (2009). Bűncselekmények számítógépes környezetben (Crimes in a computer environment – in Hungarian). Budapest: Ad Librum Kft.
23. Noah, M., Nurse, JRC, Webb, H., & Goldsmith, M. (2019). Cybercrime Investigators are Users too! Workshop on Usable Security (USEC 2019). San Diego: Internet Society, California, February 24. DOI : 10.14722/usec.2019.23032
24. PhishLabs (2019). 2018 phishing trends & intelligence report. Available from: https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf (last accessed: 5 January 2024)

25. Poonia, AS (2014). Cyber Crime : Challenges and its Classification. International Journal of Emerging Trends & Technology in Computer Science 3 (6), 119-121. He. Available: https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf (last accessed: 4 April 2024)
26. Pratt, TC, Holtfreter, K., & Reisig, MD (2017). Routine Online Activity and Internet Fraud Targeting : Extending the Generality of Routine Activity Theory. Journal of Research in Crime and Delinquency 47 (3), 267-296. He. doi : 10.1177/0022427810365903
27. Rogers, RW (1975). Protection motivation theory of fear appeals and attitudes change. Journal of Psychology 91 (1), 93-114. He. doi : 10.1080/00223980.1975.9915803
28. Scamwatch (2019). Scam statistics. Available: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics (last accessed: January 1, 2024)
29. Symantec (2019). Internet Security Threat Report. Available from: https://www.symantec.com/security-center/threat-report (last accessed: February 2, 2024)
30. Verizon (2019). 2018 Data Breach Investigations Report Executive Summary. Available: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (last accessed: Janruary 1, 2024)
31. World Economic Forum (WEF) (2019). The Global Risks Report 2019. Genf: WEF. Available: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (last accessed: June 6, 2024)
32. Whittaker, C., Ryner, B., & Nazif, M. (2010). Large-scale automatic classification of phishing pages. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. San Diego, Feb. 28 - March 3. Internet Society.
33. Wueest, C. (2014). Targeted Attacks Against the Energy Sector. Symantec. Avialable: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf (last accessed: May 5, 2024)