ECONOMY AND FINANCE • VOL. 10. ISS. 1 • MARCH 2023 • DOI: 10.33908/EF.2023.1.1

FINANCIAL SECURITY IN CYBERSPACE – PÉNZ7 THEMATIC WEEK

Elemér Terták – Levente Kovács[1]

ABSTRACT

The 9th PÉNZ7 (Money Week) event series, raising financial and entrepreneurial awareness with interactive tools, was organised between 6–10 March 2023. We were happy to welcome this year the 1.5 millionth student participating in the financial thematic week, which was the result of almost ten years' efforts and relentless work of about 1700 schools.

The focus of this year's PÉNZ7 was on *'Modern Financial Management and Digital Security'*, chosen by consultation with the Ministry of Economic Development, the Ministry of Culture and Innovation, the Ministry of Finance, the Hungarian Banking Association, and the Foundation Pénziránytű and Junior Achievement Hungary together with the responsible project manager Ministry of the Interior. Our paper provides an overview of the different aspects of digital security in finance. Our aim is to share practical knowledge and advice on the topic with teachers and students.

JEL classification: A20, G2, O30

Keywords: financial culture, cyber risk, financial security

1 THE 'EXPLORATION' OF CYBERSPACE

The mechanisms of the economic space that had evolved and got established over hundreds of years started to change in the 1970s upon the appearance of computers. In the 2000s, the emergence of web-based services and widespread access to the Internet (which changed from one personal computer per household to one smartphone per capita, '[allowing] these households to reach digital services at least at a basic level' (Terták–Kovács, 2020:376) opened a new venue for services, commerce, finance and information exchange. That digital space, by nature, can

1 *Elemér Terták*, Chair of the Supervisory Board of K&H Bank Zrt. E-mail: elemertertak@gmail.com.
Levente Kovács, Secretary General of the Hungarian Banking Association, Professor at the University of Miskolc. E-mail: kovacs.levente@bankszovetseg.hu.

meet existing, induced or imagined consumer needs in a cost-effective way. As such, this novel space offers attractive opportunities and conditions to both service providers and service users and is characterized by continuous evolution and renewal *(Poletaeva* et al., 2019).

As a consequence of the continuous and rapid development of the digital space, legislators cannot keep pace with the constantly changing legal relationships it hosts. One might say jokingly that it's something the Romans had omitted from their law codes. As a result, timely and sufficient regulation of the digital version of traditional and novel services provided and used in this space, and of the associated rules of procedure, processes, guarantees, liabilities and risks lagged behind. In the era of global services, such a deficiency can be remedied only globally (as national-scale regulation alone is not sufficient) which, however, is a lengthier process.

There are three potential limits to the further development of the digital space: scarcity of service solutions that may be digitalized, scarcity of digital solutions on the providers' side, or consumer readiness to embrace new digital solutions. *Sándor Csányi*, CEO of the largest Hungarian Bank identified the limits to development as follows: 'let customers use products and services according to their habits and needs, so that everybody can go through the phases of digitalization at their own pace' (*Kovács–Sipos*, 2017:24). In other words, digitalization can spread only as fast as the adaptive capacity of consumers allows. As the pandemic made working and learning at home, almost fully digital banking, home-delivery of goods etc. widespread, people overcome their aversion to using digital solutions, which meant a decade's progress in only a few months. This affected all areas of the economy (Terták–Kovács, 2020).

The digital space now in mass use took in inexperienced users from almost all levels of society, whose reservations against these new platforms were addressed by offering IT solutions which are easy to understand even for beginners and especially user-friendly. However, user's arrival in the digital space and massive use of the new solutions was not accompanied by adequate assessment and awareness of the risks entailed. Cyberspace has thus become a treasure trove for fraudsters, where attempted fraud and different types of fraudulent activities can proliferate – unfortunately with increasing success. Joint effort under a broad cooperation between legislators, IT and finance professionals, and financial education and awareness-raising among consumers is the only effective cure for this epidemic.

2 THE RISKS OF DIGITAL FINANCE

The most ground-breaking changes in the monetary and financial system were also effected by the aforementioned acceleration of technological progress (*Bangó–Pintér*, 2022). What is conceptually new about the ongoing changes is that they affect the substance of money, while the earlier changes mainly had formal implications. The evolving new technologies contributed primarily to efficiency and convenience also in the area of finance, and a significant facilitator of their spreading was the curiosity, receptiveness and trust of younger generations towards digital solutions.

However, the new technological possibilities, especially instant execution, necessarily come with new risks. Many youngsters lack the necessary knowledge and self-control and succumb easily to temptations from the Internet – with typically irreversible consequences considering instant payment/execution. The consumer awareness blog of a financial institution[2] provides instructive examples, showing that even the most well-informed consumers can be deluded by attractive discounts. Huge price discounts are misconceived as a once-in-a-lifetime opportunity and often encourage unnecessary purchases. Most readers may be familiar with promotions where a tempting offer (e.g., content services, entry fee etc.) redirects users to a registration page in a foreign language, where they are required to enter their name, card details and/or mobile phone number to get the promotional discount. After a free, however, very short trial period, they suddenly find themselves as subscribers to premium rate text messages or to a monthly subscription fee of EUR 20–40 if not cancelling the service on time. However, not every application or service sends a notification before the end of the free trial, but charges users automatically. Moreover, the cancellation process may be difficult and mostly requires adequate knowledge of a foreign language. 'Tricky' applications of this kind are called 'fleeceware' in the literature. The European Commission and the Consumer Protection Cooperation Network (CPC) of EU Member States have taken steps against such malicious commercial practices, but it will take time until they could completely be eliminated.

However, even completely fair commercial offers, or ones which are just too enticing for teenagers and young adults not having sufficient funds, may lure them into a debt trap due to the availability of cashless instant payment. The payment methods used in e-commerce, such as payment on delivery, by PayPal, credit card or in interest-free instalments not only make purchases attractive but also easy, as payment can be made in fact with a mouse click, which is definitely a lot simpler

2 See https://blog.provident.hu/tudatos-vasarlas (in Hungarian).

than rummaging around in the wallet for money. Impulse buying is hindered but cannot be prevented by two-factor authentication, introduced for security reasons. Therefore, each of us is responsible for developing the necessary self-restraint to avoid impulse buying.

The grave consequences of irresponsible online purchases are elucidated in a 2015 survey by the market research company GfK, carried out on behalf of the Association of German Banks (BdB)[3]. Based on this survey, 31% of young Germans have run up debt at least once due to goods and services purchased online, and 8% could not repay the accumulated debt with their own resources.

When starting vocational education or earning regular income from work, several youngsters get even worse off financially, as they have to cover a larger share of their costs of living than they are used to from own resources pocketed in the form of student grants or salaries (*Szakács* et al., 2016). Many are dizzied by the freedom of getting financially independent and tempted into overspending. The result is generally indebtedness to parents, negative bank account balances and high overdrafts with onerous interests (*Lentner*, 2013). It is because of these risks that experts advocate the inclusion of consumer and financial education as a compulsory subject in school curricula – an idea welcomed by most youngsters. It is also a priority for the PÉNZ7 event series to help young people learn how to manage their finances more responsibly by teaching them relevant knowledge.

Responsible financial and smart money management means much more than avoiding debt – a truth that Generation Z (people now aged 18–25) must swiftly learn. Despite the fact that this generation is the most risk-averse of all, they have scored lowest in a 2018 study of TIAA Institute on financial education.[4]

Only 46% of respondents from Generation Z felt confident in the area of finance – the lowest rate compared with baby boomers (people aged 58–74), Generation X (people aged 42–57) and Generation Y (people aged 26–41). Generation Z were the first for whom life became unimaginable without smartphones and social media, spending approx. 6.5 hours daily on average on their smart devices. Still, they seem to be the least literate in the areas of comprehending risk and insuring.[5]

3 https://www.schuldnerberatung.de/ebook-verschuldung-jugendlicher.pdf, 2019 (in German). The Swiss Federal Statistical Office collected similar results in 2020: https://www.bfs.admin.ch/bfs/de/home/statistiken/wirtschaftliche-soziale-situation-bevoelkerung/einkommen-verbrauch-vermoegen/verschuldung.html (in German).

4 https://gflec.org/wp-content/uploads/2018/04/TIAA-Institute-GFLEC-2018-PFinIndex-Press-Release-FINAL.pdf.

5 https://www.tiaa.org/public/institute/publication/2018/millennial-financial-literacy-and-fintech-use.

'Financial awareness' should be mentioned at this point, which is a more complex concept than 'financial literacy'. While financial literacy can generally be obtained by learning, financial awareness also has a bearing on mentality, general approach and behaviour – factors which are undeniably even more important in financial decision-making (*Veresné–Varga*, 2018).

In financial education, the methodological focus is often on giving simple advice and general guidelines, while financial awareness cannot be developed without due attention and time dedicated to the complexity of the subject, i.e. making sure that students are made familiar with and understand its depth and nuances.

Now that finance has gone digital, financial competence is inseparable from the appropriate digital competences. While – as mentioned before – younger age groups are digitally well-versed, they are not necessarily equally well-prepared in the area of finance to ensure and maintain an adequate level of security.

2.1 Digital competences

It is not only reckless spending that poses a threat. In a survey on the increasingly widespread use of digital financial services, *Réka Szobonya*, senior lecturer at the Budapest Business School, found that respondents performed almost 30 percentage points lower in their answers to questions regarding digital competences than on a financial knowledge test (Szobonya, 2021), while there was a positive correlation of medium strength between financial knowledge and digital competences. It should be highlighted that respondents' performance showed substantial variation in the respective sub-areas of digital competences, with the weakest results in digital data security (*Table 1*).

Table 1
Average results achieved concerning digital competences (%)

Area of competence	Male	Female	Jointly	Significance
Communication and collaboration	6.85	6.65	6.80	0.91
Obtaining information	34.90	30.79	32.60	0.25
Device protection	37.94	34.55	36.20	0.25
Digital data security	84.44	84.70	84.50	0.91
Digital competences jointly	41.05	39.19	40.05	0.27

Source: Szobonya, 2021

Regional differences in digital competences are also significant (see *Table 2*).

Table 2
Distribution of users based on the number of digital financial services used, by type of settlement and region

	Number of digital financial services used			
	3 or more	**2**	**1**	**None**
Capital	13.8	14.9	36.2	35.1
City with county rank	11.9	16.1	30.1	42.0
Other city	7.8	18.6	27.1	46.5
Village	7.4	12.8	22.8	57.0
Budapest	13.8	14.9	36.2	35.1
Southern Transdanubia	19.5	22.1	19.5	39.0
Central Transdanubia	15.8	18.7	25.2	40.3
Southern Great Plain	0.8	11.6	33.3	54.3
Northern Great Plain	0.0	10.5	25.0	64.5

Source: Szobonya, 2021

3 CYBERCRIME AROUND THE WORLD AND IN HUNGARY

The current level of digital competence as presented above is by no means satisfactory. Especially regarding that an increasing trend has been observed in cybercrime in recent years both worldwide and in Hungary, as already mentioned. Cybercrime includes all kinds of malicious attacks aiming at financial gain or damage by unauthorized access to personal data, disruption of digital transactions, or distortion or alteration of information. Insufficiently stored or protected data are an easy target for cyberattacks. The most shocking observation is, however, that in the case of 9 in 10 cyberattacks, the human factor – lack of caution or negligence by users – is at the source of the damage caused. Based on surveys, almost 75% of the damage derives from the opening of phishing emails, billions of which are circulated around the world every day. Although Internet service providers and corporate servers deploy different methods to contain them, unfortunately, almost 20% of the spam mails slip through security filters, half of which are eventually opened by careless recipients, who may even respond to them.

There are very different actors behind cybercrime, including frustrated employees, industrial spies, malicious hackers, drug dealers, illegal gambling operators, criminal organizations, terrorist groups or states in conflict. The offences are

committed using computers, computer networks or other digital communications channels (e.g., social media platforms). They may target individuals, business groups and even governments.

The number of criminal acts committed online almost tripled around the world between 2017 and 2021, and the amount of damage caused by those acts grew almost fivefold. In 2021 alone, more than 847 000 cases were reported to the competent authorities, with an associated total damage of USD 6.9 billion.

Currently, the Criminal Code of Hungary does not include – and will probably not include for some time to come – a separate chapter on cybercrime. The reason for that is that cybercriminals constantly invent novel and previously non-existent practices to commit offences, which the legislation simply cannot keep pace with. However, the provisions of the Criminal Code on the breach of information systems or data may be mentioned for reference[6]. The stale legal definition it provides has in fact a wide practical application and can also be used by law enforcement bodies for these new criminal practices.

For the same reason, Hungary does not keep separate statistics on cybercrime. Of course, instances of 'breaches of information systems or data' are recorded in the crime statistics, but they do not differentiate according to how the crime was actually committed, e.g. if there was an increase in the number of ransomware or denial-of-service cases, since they belong under the same offence. According to data of the Criminal Statistics System (Belügyi Statisztikai Rendszer, BSR) of the Ministry of Interior, in 2018, there were only 200 reported cases of breach of information systems or data. In 2020, the number of cases more than quadrupled to 830, and continued to grow in 2021. There was a spectacular increase also in the prevalence of related criminal offences; in 2018, 1 100 and a few cases of information system fraud were reported to the police, while the corresponding figure was 3 400 in 2020 (Cybercrime, 2022).

3.1 Protection against cybercrime in Hungary

As most Hungarians still consider cybercrime as something different from traditional crime, many believe that it is the responsibility of a dedicated police department. In reality, cybercrimes are treated as any other crime, and come within the competence of police stations, or in more serious cases, of police headquarters. Now every station has at least 1 or 2 colleagues who have a good knowledge of

6 Offences defined in Section 423 of Chapter XLIII (Breach of Information System or Data) of the Criminal Code (Act C of 2012).

the field. In addition, due to the specificities of cybercrime, a Cyber Crime Division has been established within the National Bureau of Investigation (Nemzeti Nyomozó Iroda, NNI), currently operating with a staff of over 100. The Division having national competence is a centre of expertise for detecting the most serious cybercrimes, and also provides professional support for police investigations, when necessary, as well as training to police personnel. It is an organizational unit of the police and not to be confused with the National Cyber Security Institute of Hungary (Nemzeti Kibervédelmi Intézet, NKI).

The NKI, operating within the Special Service for National Security (Nemzetbiztonsági Szakszolgálat, NBSZ), is responsible for cybersecurity in general. For example, when a critical infrastructure is attacked, the NKI analyses logs, traces back the source of the attack, provides support for recovery and reports to the police whenever a crime is detected. It is also tasked with the operation of a national contact point which is the domestic coordination body for high-impact cyber incidents within the European Union, receiving incident reports and reporting to international partner organizations (*Csaba*, 2019).

Increased digitalization goes hand in hand with increased cybersecurity risk, which may be mitigated by reinforcing the protection of retail and corporate digital products and services. For that purpose, the Supervisory Authority of Regulated Activities (Szabályozott Tevékenységek Felügyeleti Hatósága, SzTFH) was established in Hungary based on Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification to perform the official cybersecurity certification tasks of digital products. The aim of certification is to guarantee compliance of the information and communications tools and services available for purchase and use by citizens and businesses with the continuously evolving standards of cybersecurity.

In an international comparison, Hungary's level of development in terms of legal, technical, organizational measures and cooperation in the area of cybersecurity is moderate based on the 2020 survey of the International Telecommunication Union (ITU), operating within the organization of the UN in Geneva[7]. Hungary ranked 35th among the 63 listed countries, preceded by Slovakia and followed by Israel. 17 EU countries ranked higher on the list than Hungary.

7 ITU: Global Cybersecurity Index 2020.

3.2 The most frequent types of cybercrime

Each year, Europol publishes the Internet Organised Crime Threat Assessment[8], a 40–60 page report on developments in cybercrime. The report is based primarily on trends instead of hard statistical data as cybercrime is characterized by high latency. It is clear from the report that Hungary is affected in the same way as other European countries, showing that cybercrime is a transnational phenomenon, with no specifically Hungarian traits (*Halmai*, 2021).

However, year over year, the frequency and types of the cybercrimes committed changes. The most common types of cybercrime in the last three years were phishing, non-payment and non-delivery scams, and personal data breaches. Phishing means theft and misuse of the personal or financial data of victims. The data are obtained through messages or websites created specifically for that purpose. In non-payment or non-delivery scams, the scammer does not pay for the goods/services ordered, or in the case of the latter, does not fulfil an already paid order. In personal data breaches, data containing confidential information is obtained fraudulently by installing malware or deception of the victim.

A significant share of cybercrimes remains latent, either because victims are too ashamed to report them, or not even realize that they have fallen victim to cybercrime. For example, in a denial-of-service attack (see below), criminals use botnets consisting of tens of thousands of compromised private computers which provide the resources required for the attack. The average user may only notice that his/her computer has become slower, and it takes longer to load data, but has no idea that a virus is behind all that.

Which are the most common mistakes that expose users to cybercrime? According to law enforcement bodies, well- or even tolerably informed users are not so easy to trick. Most attempts are quite unsophisticated and follow the same pattern. Therefore, they are easy to identify.

Many users are hooked in only because they are heedless. For instance, when a provider is requesting personal data in an email, they comply, despite the fact that they are not clients of that provider and the text of the message reveals that it was not drafted by a native Hungarian speaker. Often, users visit websites or download software which are likely to be infected by viruses, and they reckon with it, yet do not take the risk seriously, and fail to update their operating systems regularly or install antivirus software. These examples indicate that the average

8 Europol: Internet Organised Crime Threat Assessment (IOCTA). The most recent publication concerns 2021.

level of risk-awareness of many users is fairly low, considering that no specific IT knowledge is required for using the aforementioned security tools.

The risks of such low awareness have been multiplied by the COVID-19 pandemic, forcing many tenderfoots to the Internet to work from home. These new users were not prepared for the perils of the Internet. Readiness to use the new 'e'-platforms was not accompanied by thorough knowledge of 'e'-applications, and inexperienced users were often overconfident. As a consequence, many users do not consider data as a most valuable asset, but simply an accessory to their work, used out of necessity.

It is also commonly observed that while cybercriminals continuously come up with seemingly novel tricks, if we strip away the technicalities, we find that there is nothing new under the sun. After all, the essence of cybercrime, too, is to deceive the targeted person. The cause of cybercrime victimization is predominantly the frailty of the victims. Therefore, the best way to limit cybercrime is to prevent it from happening. This may seem a truism applicable to all kinds of crime, nonetheless it has great practical benefit, particularly in cyberspace. The most effective protection for users is to consciously prepare for defending themselves from potential attacks, by regularly updating and installing antivirus software on their computers and smartphones, and by heeding the advice and recommendations communicated periodically by their bank, Internet service provider or cybersecurity organizations.

To contribute to effective defence, the following part of the paper presents some of the newer techniques used by cybercriminals in recent years and relevant advice on protection against them.

3.3 The most harmful types of cybercrime

3.3.1 Business email compromise

In 2021, scams called 'business email compromise' or BEC caused the greatest financial damage, amounting to USD 2.4 billion. In these cases, attackers take control of the email server of a company and use it to send messages to potential victims, urging them to pay a certain amount of money by bank transfer under seemingly convincing pretexts. The email addresses of victims are obtained in more and more cases by hacking social media platforms and mail systems. The sums transferred by unsuspecting victims are converted immediately into a cryptocurrency, making it difficult to trace and recover their money. Honest businesses rarely ask for money from their clients in email campaigns. Therefore, when such a request is received from the email address of a well-known company, it is advised to contact them first to check the authenticity of the request.

3.3.2 Romance scams

Victims of confidence or romance scams have also been cheated out of significant sums. These were the third most lucrative form of cybercrime for perpetrators. In confidence or romance scams, perpetrators approach victims through dating services with feigned romantic intentions, and after establishing a closer relationship with them, ask for personal data or money for various invented reasons. Common sense is the most effective defence against such attempts. Rationally, anyone asking for a larger sum from their new partner instead of asking for a bank loan should not be trusted.

3.3.3 Investment scams

Of the different types of cyberspace fraud, investment scams have become increasingly 'popular'. The number of cases rose sharply in recent years. Scammers entice prospective victims with exceptionally lucrative investment opportunities. In most cases, the offer concerns a cryptocurrency investment with the promise of returns several times above the market average. The sum to be invested should generally be provided in a cryptocurrency as well. Initially, the electronic balance statements confirm generous returns in the investment's growing value, but when the time comes for most investors to realize the accrued profit, the bubble pops, and they find themselves waiting in line at liquidators to recover the invested sum and the promised returns – with little hope. Common sense is again the only effective defence against these scams. One must ponder if it is possible to generate returns above the market in the long term in an honest way. And even if it was possible, why would anyone share this knowledge instead of exploiting it entirely for their own benefit?

3.3.4 Ransomware

Ransomware attacks are free of all pretence. A malicious software is used which instantly blocks or encrypts the data stored on the targeted devices or in entire IT systems. Viruses of this type generally land from pornographic or gambling websites on the computers of victims. It also has a reason: perpetrators assume that few of the wronged users will admit to their families or the police that they had visited websites of this kind. The aim of attackers is again to get money by demanding ransom from the owner for returning the stolen information. Recently, the ransom paid each year by victims had amounted to hundreds of millions of US dollars. Ransomware attacks may be fended off by avoiding visits to, and more importantly downloads from, unknown and obscure sites. Files already downloaded should not be installed in any case. Backing up our IT systems and files regularly is also crucially important. This enables fast recovery and minimum

loss of data when the computer system must be reinstalled due to a ransomware attack or crash of the operating system.

3.3.5 Denial of service

Denial-of-service (DoS) attacks are performed by flooding a computer or a network with superfluous information in order to prevent it from fulfilling users' requests. Distributed denial-of-service (DDoS) attacks are basically the same, but the attack comes directly from a network of computers. The technique is employed by some attackers to launch other attacks during the time the network is overloaded. Botnets, or zombie networks as they are called sometimes, target and overload the target's processing resources. Botnets are at different geographical locations and are therefore difficult to track down. Possibilities to prevent these attacks are limited. The smartest thing to do when the network gets suspiciously slow is to disconnect our computer to minimize the risk of viruses sneaking in.

3.3.6 Man-in-the-middle attacks

Man-in-the-middle (MITM) attacks involve hackers intercepting communications between two parties to steal confidential information. MITM attacks are the most frequent when an unsecure Wi-Fi network is used. Attackers insert themselves into the 'middle' of the conversation between the guest user's device and the public Wi-Fi modem, and hijack confidential information or install phishing software onto the guest's device using malicious codes. The most effective protection against such attacks is obviously to avoid communicating sensitive data through public Wi-Fi networks, e.g., connecting to our e-bank or making payments.

3.3.7 Phishing

Phishing attacks deploy misleading communications, e.g., emails, to trick the receiver into opening the message and following its instructions, such as providing their credit card's PIN and/or CVV. Their purpose is to steal sensitive information, e.g., credit card data or online banking credentials, or to install malicious software on victims' computers. They may be tackled by treating these messages with suspicion and refraining from fulfilling the requests included in them, recalling that banks never ask for sensitive personal data in email (Pásztor, 2018).

3.3.8 Password attacks

Attackers may get access to an array of confidential information by obtaining passwords. A strategy used in cyberattacks targeting passwords is trust-based manipulation, drawing heavily on human interactions and usually involving deception of people into breaking standard security rules. Other types of password attacks include gaining access to password databases and brute-force attacks. For the latter, hackers use the method of 'credentials stuffing', i.e. inserting user credentials from hacked databases on a series of other platforms. This may harm especially users who use the same password for several different websites, as it provides perpetrators access to multiple accounts. The best protection is to secure connections involving sensitive data transfers with a different password and to avoid using passwords derived from our name, date and place of birth or address.

3.3.9 Spoofing

Cyberattacks of this type are accomplished by creating a replica of the website of the victim's financial service provider, i.e., a site that closely resembles the original in both appearance and functionality. Victims are manipulated in an email into visiting the 'spoofed' website and entering their credentials unawares. Attacks of this kind may be circumvented by closely scrutinizing the URL of the website.

4 CLOSING COMMENTS

In the foregoing, some potential threats in cyberspace have been presented. Targeted training and good practices are the most effective defence against these threats. For the 9th Pénz7, a lecture titled 'Financial security in cyberspace' was prepared on commission of the Hungarian Banking Association and made available on the website www.penz7.hu. The lecture formed part of the content of classes held in public schools during the thematic week of 6–10 March 2023. Exciting financial quizzes and content from popular competitions are also available for download from the website.

The class material referred to above was prepared for the financial week in cooperation with the National Cyber Security Institute and the National Bureau of Investigation. Their experts contributed real-life examples and practical advice to the material.

The class is started off with an exciting website (https://threatmap.checkpoint.com), showing cyberattacks in progress around the world at the time of opening the website in real-time. It displays the source, target and scale of each ongoing attack. It is a dynamic map revealing in a spectacular manner that millions of

cyberattacks happen in a single day. Attacks are carried out non-stop in different parts of the world, and target governments, companies and individuals alike. The website also shows the main types of malware used in the attacks. The dynamic image helps everybody realize that they may as well be victims if they fail to protect themselves. Although Hungary can be considered safe in some respects (e.g. the number of debit card fraud cases is one of the lowest in Europe), we may get in danger any time, for example, when surfing on foreign websites.

The shocking visit to this website is followed by practical advice on how to navigate safely in cyberspace. Topics discussed in this part of the class include: how to reduce the risks of online payment, what is the most important financial data to protect, where and how to store our data, available/recommended online payment methods, available secure payment solutions, and the ever recurring topic of how to generate a good password/PIN code.

The final part of the class begins with an overview of the most recent types of fraud attempts. Then information on ransomware and recommendations for prevention and protection are provided. At the end of this part and the whole lesson, students are made familiar with types of fraud where (naturally scam) investments with incredibly high returns or prizes are offered. This paper is complementary to the class material.

It serves the same purpose, i.e., to provide – building on the previously prepared class material – a useful aid to raising financial awareness and adequately managing the risks of modern financial services in cyberspace.

REFERENCES

Bangó, Péter – Pintér, Éva (2022): The digital financial solutions pathway for generations. In: Csiszárik-Kocsir, Ágnes – Popovics, Anett – Fehér-Polgár, Pál [eds.] (2022): XVII. FIKUSZ 2022 International Conference: *Proceedings*. Budapest, Magyarország: Óbuda University Keleti Károly Faculty of Business and Management, 622–636.

Csaba, László (2019): A költségvetési és bankunió: vízválasztó a többsebességes EU-ban A költségvetési és bankunió: vízválasztó a többsebességes EU-ban [The Fiscal and Banking Union as the Great Divide in 'Multi-Speed' Europe]. In: Halmai Péter [ed.] (2019): *Tagállami integrációs modellek: A gazdasági kormányzás új dimenziói az Európai Unióban* [Integration Models of the Member States – New Dimensions of Economic Governance in the European Union]. Budapest, Magyarország: Ludovika Egyetemi Kiadó, 167–181.

Halmai, Péter (2021): A Gazdasági és Monetáris Unió rendszerének egyes sajátosságai [Some Systematic Features of the Economic and Monetary Union]. In: Halmai Péter [ed.] (2021): *Európai perspektívák* [The Future of the Economic and Monetary Union – European Perspectives]. Budapest, Magyarország: Ludovika Egyetemi Kiadó, 199–288.

Kovács, Levente – Sipos, József [eds.] (2017): *Ciklusváltó évek, párhuzamos életrajzok* [Cycle Changing Years, Parallel Biographies]. Magyar Bankszövetség, ISBN 978-963-331-407-4.

Lentner, Csaba [ed.] (2013): *Bankszabályozás – pénzügyi fogyasztóvédelem* [Bank Management – Bank Regulation, Financial Consumer Protection]. Budapest, Magyarország: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN: 9789630855914.

MABISZ (2022): Kiberbűnözés Magyarországon: már a rendőrségi statisztikákban is kimutatható a dinamikus növekedés [Cybercrime in Hungary – Police Statistics Confirm Dynamic Growth]. *Biztosítási Szemle*, 11.01.2022, https://mabisz.hu/szemle/?p=49132.

Pásztor, Szabolcs (2018): The Future of Commercial Banks – Survival or Failure? *Izvestiya: Mezhdunarodnyy teoreticheskiy i nauchno-prakticheskiy zhurnal*, 23(4), 71–88.

Poletaeva, Vladislava –Perepelitsaí, Denis –Arhangel'skaya, Tat'yana – Zaripov, Il'yas – Pásztor, Szabolcs (2019): The Research Task of Banks and Authorized Government Institution Interests in Manufacturing Companies' Investment Projects Congruence. *International Journal of Mechanical Engineering and Technology* (IJMET), 10(2), 1603–1609.

Szakács, Attila – Szakács, Zsolt – Zéman, Zoltán (2016): A takarékoskodás, a biztosítások és a banki kölcsönök kapcsolata [The Relationship between Savings, Insurances and Bank Loans]. In: Bene, Sz. [ed.] (2016): XXII. Ifjúsági Tudományos Fórum [22nd Youth Scientific Forum]. Keszthely, Magyarország: Pannon Egyetem Georgikon Mezőgazdaságtudományi Kar, 1–6.

Szobonya, Réka (2021): Kompetenciák a pénzügyek területén – lakossági felmérés tapasztalatai [Competences in the Field of Finance – Results of a Population Survey]. *Pénzügyi Szemle*, 66(2).

Terták, Elemér – Kovács, Levente (2020): A szociális védelem és a társadalmi kohézió kihívásai válsághelyzetben a pénzügyi szférában [Challenges to Social Protection and Social Cohesion in Crises in the Financial Sector]. *Pénzügyi Szemle* 65(3).

Veresné Somosi, Mariann – Varga, Krisztina (2018): Tudass tudatosan! A pénzügyi tudatosság, felelősség fejlesztése környezetünkben: Susánszky János Esettanulmánymegoldó verseny középiskolásoknak [Susánszky János Esettanulmánymegoldó verseny középiskolásoknak [János Susánszky Case Study Competition for secondary school students], case study]. University of Miskolc, Faculty of Economics, 18 p.