ECONOMY AND FINANCE • VOL. 11. ISS. 1 • MARCH 2024 • DOI: 10.33908/EF.2024.1.2

FINANCIAL LITERACY IS THE BEST PROTECTION FROM CYBERCRIME

Levente Kovács – Elemér Terták[1]

ABSTRACT
As a "side effect" of the stormy digitisation of financial services, cybercrime has taken its toll. Therefore, financial service providers must continuously strive to protect the wealth entrusted to them and preserve their reputation. Law enforcement agencies in all countries highly support these efforts, since their core tasks include safeguarding their citizens' financial security and maintaining financial stability. However, customers of financial institutions are also accountable for the safety of their assets, notably by taking care of passwords, computers and network connections. This paper is primarily dedicated to teachers and educators participating in improving financial literacy so that, on the one hand, they can obtain a comprehensive picture of the different manifestations of financial crime and the means to protect themselves against it. On the other hand, it is aimed at elevating the level of their financial literacy to be able to provide professional answers to the questions raised by their target audience.

JEL codes: A20, G2, O30

Keywords: financial literacy, cybercrime, risks, financial security

1 A FEW THOUGHTS ABOUT THE RELEVANCE OF CYBERCRIME

Digital transformation, including a revolution of mobile telephony, has fundamentally changed the provision of financial services all over the world (Pásztor – Szijártó, 2016; Poletaeva et al., 2019). The Coronavirus pandemic in 2020 significantly boosted the process since – due to health protection – there was a considerable increase in remote work, remote schooling and digital commerce, which resulted in growing numbers and value of digital financial transactions. In the digital age, protecting data and financial records is as important as bank vaults

1 *Levente Kovács*, secretary general of the Hungarian Bank Association, university professor at University of Miskolc, corresponding author. E-mail: kovacs.levente@bankszovetseg.hu.
Elemér Terták, member of the Presidium of the Hungarian Economic Society. E-mail: elemertertak@gmail.com.

and safes were in the past to keep cash, securities, or related documents securely. International cyberspace as the site of transfer for higher and higher amounts of digital money has inevitably attracted the attention of cyber criminals and increased the risk, frequency and gravity of cyber attacks they committed (Terták–Kovács, 2023). Cybercriminals focus on data theft and phishing to loot their victims' bank accounts. In addition, they use fraud and deceit or turn off their victims' devices to blackmail them to pay significant amounts. According to the first report of Interpol, the International Criminal Police Organisation, which turned 100 years old last year, published on the global trends of crime last year, about two-thirds of the police of 195 member states deemed money laundering, internet fraud, phishing and the spread of ransomware[2] to be the most significant threats of our age (NZZ, 2022). Together, they are all ingredients of digital financial crime.

Digital financial crime today is a version of white-collar crime[3] covering a wide range of fraudulent activities (Weisburd et al., 1994). It includes every crime committed by utilising or with the assistance of digital devices assaulting financial enterprises or money markets, such as banks, Fintech companies, creditors, and, naturally, any holders of funds (Croall, 2009). Committing financial criminal acts using information and communication technologies is particularly attractive for organised crime gangs since they can gain high profits. At the same time, the risks they take globally are relatively low (Lyng, 2005). In addition, investigating such crimes requires high-level technological and finance-technical knowledge, which renders catching the perpetrators more difficult. This is particularly true for internet fraud and other crimes in which several countries are affected, so international collaboration is needed to uncover them (Katona, 2021).

Organised criminal gangs operating worldwide exploit the differences between national provisions on the security of the digital space, which often makes collaboration between the law enforcement agencies of different countries cumbersome (Weisburd et al., 1994). It is not simply the result of differences between the legal definitions of criminal acts but also because, in the case of cybercrime, territorial jurisdiction may differ from one country to the other. In addition, police connections, which are used to cooperate reasonably, have often been replaced by newly set up cyber-protection organisations of different types. As a result, the authorities involved had to suspend collaboration in their investigation until

2 During ransomware attacks, the data stored on computers are made inaccessible by installing malware programs. Phishing means data theft using fake websites or e-mails.

3 The term "white-collar crime" usually refers to non-violent or not directly violent criminal acts of a financial nature committed mostly by people in the higher strata of society using their higher professional knowledge and positions in so-called "white-collar" jobs.

the responsible jurisdiction is unambiguously clarified. The Convention on Cybercrime adopted in Budapest in 2001 by the Council of Europe helped those problems a lot because – despite many deficiencies in regulating cyberspace – it identified a clear set of tasks for the Member States on how to manage in their national laws the acts of cybercrime which were already quite rampant at the time. However, the Convention needs a facelift considering the technological, legal and practical developments over the more than two decades since its adoption (Kraszнay, 2021). One crucial reason amendments are necessary is that in the meantime the data protection requirements known in the EU as GDPR entered into force. These are, of course, very important because complying with them could have an unforeseen and unintentional side effect by hindering the quick joint actions by investigating agencies.

Last but not least, it is important to draw attention to the fact that individual and organizational vulnerabilities, such as the lack of victims' financial awareness, risk assessment or self-defence (Dunn, 2007; Walklate, 2017), greatly facilitate criminals' actions (Lyng, 2005). It is also reflected in the experience of the Hungarian Financial Conciliation Board (abbreviated: PBT)[4], a body resolving disputes between consumers and financial businesses under the auspices of the National Bank of Hungary (MNB). They established that 77% of payments-related complaints had to be rejected because the facts indicated customers were responsible for the damages sustained due to their own carelessness. The Hungarian undertaking Cyber Shield is an initiative worth international attention to promoting structured assistance for individual defence.[5] As part of it, the relevant government agencies, authorities, market players and the Media Union Foundation as a communication partner conduct coordinated communication campaigns about cybersecurity risks and how to defend themselves from these risks. In addition to spreading information about protection, the undertaking has facilitated joint actions by the relevant authorities and the enterprises of the financial sector, as well as the establishment of effective strategies for prevention and defence.

4 The Financial Conciliation Board is an out-of-court forum for settlement operated under the auspices of the National Bank of Hungary since 1 July 2011 to resolve disputes between consumers and financial businesses. Its primary objective is to promote the parties' agreement. If that is not achievable, it can pass an order or make a recommendation if a service provider has violated some legal provisions. Procedures by PBT are free of charge, no procedural fees or duties have to be paid, and you do not have to have legal representation, either.

5 The website of the Cyber Shield is available at: https://kiberpajzs.hu/.

2 HAS CYBERCRIME BECOME MORE DANGEROUS IN OUR DAYS?

As technology develops in the age of digital transformation, not only does the range of financial services expand and the speed of transactions increase, but – as has already been mentioned – the methods of financial crime also keep improving and changing fast (Szóka, 2021). The internet, stretching across the globe, allows criminals access to data, information and the sources they need to commit their crimes while simultaneously reaching many victims. (Orbán, 2023; Tertán-Kovács, 2023). As a result of globalisation, criminals have also increased cross-border activities, while criminals from different countries frequently join forces. In that regard, globalisation has become a fact in financial crime (van Dijk. 1999; Shivaraj, 2023), which hinders the successful detection and prevention of their crimes. Another obstacle is that criminals use cryptocurrencies that are not subject to complex international regulations to hide and forward their spoils (Katona, 2021).

The consequences of financial crime are highly harmful to individuals, businesses, and other legal entities. In addition to the loss of funds and property, the human victims of financial crime also suffer long-term emotional, psychological and health harm (Davies et al., 2003; Dubb, 2007). Beyond the cut down of their profit and/or assets, the defrauded enterprises may also lose their reputation and their clients' trust, which is critical for continuing their business operations. Further, widespread financial crime may undermine the population's confidence in the safe functioning of money markets, which – as a result – will drive up the fees of financial services and the costs of borrowing.

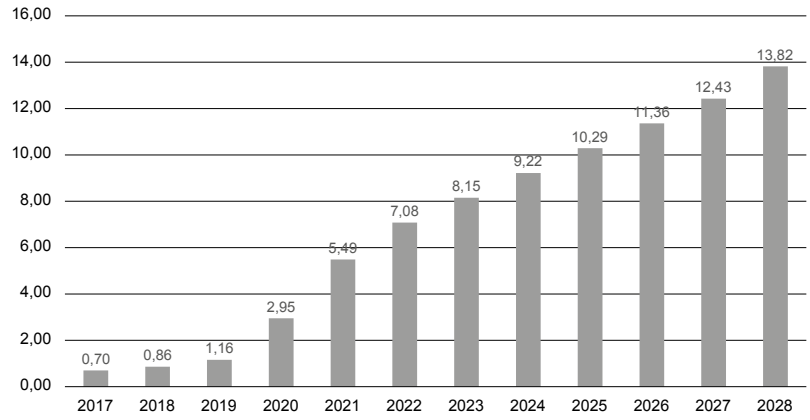
Financial crime, however, is harmful not only at the national level but also at the global level. For instance, criminals can move significant amounts of money around the globe with the help of money laundering, making those funds inaccessible, i.e., they cannot be seized to be used to reduce the damage they have caused. In addition, fraud and forgery at an international scale can weaken national currencies and push back investments, all of which may eventually damage the economies of different countries (van Dijk, 1999).

Globalised financial crime, including cybercrime, is difficult to track due to its nature. All the damage caused is even more challenging to quantify. For instance, the exact estimation of all the money laundered in a year is somewhat tricky, so the data relating to financial crime, including money laundering, are often based on experts' estimations only. Accordingly, the damages caused by financial crime make up for 3-5% of the global GDP; in other words, financial crime can be regarded as one of the most profitable industries in the world, which renders fighting it more difficult. With the direct damage incurred by the victims of financial crime, the whole of the economy may have to shoulder additional costs to remedy

the damage and strengthen cybersecurity. Such grave consequences can explain why governments and financial institutions undertake significant efforts to overcome financial crime (van Dijk, 1999).

Figure 1 illustrates the damage caused by cybercrime from 2017 to the present and its projected amount till 2028.

Figure 1
Estimated global costs of cybercrime 2017–2028 (billion USD)



Source: Statista, 2023

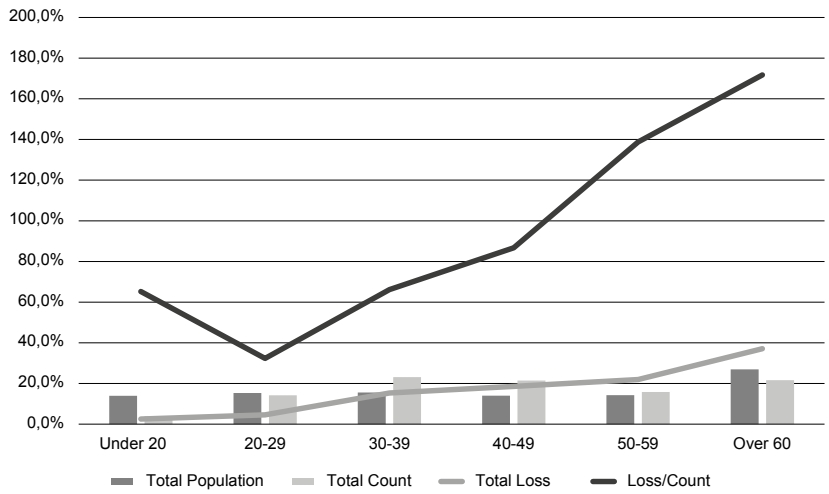
Cybercrime keeps growing all the time. The number of victims of online crime has increased 16 times since 2001, while financial losses have grown over 570 times. The number of cybercrime victims has surpassed 7 million, and their losses have reached at least USD 80 billion over the past 22 years (AAG IT, 2023). Agile digitisation was the main factor behind its fast growth. While only one-third of the world's population had internet access in 2007, at the dawn of the revolution of mobile banking, by the middle of 2023, it had gone up to two-thirds of the population, which has increased by 1.2 billion. Forecasts predict a (mere) 70% increase in financial losses by 2028, but even this (slower) rate exceeds by one and a half times the expected growth rate of the global GDP during the same period (Surfshark, 2023). The intensity of cybercrime is closely related to international developments. Following the great global financial crisis of 2008, economic losses attributable to cybercrime increased by 115% in 2009. In the first year of the Coronavirus pandemic in 2020, the number of victims of cybercrime surged by 69% compared to 2019, reaching its current peak. Price rises, and inflation peaked in most parts of the world in 2022 when damages caused by cybercrime increased by almost 30% compared to the previous year.

Although full-scale reliable data about digital financial criminal acts committed worldwide are not yet available, the comparison of national criminal statistics reflects striking differences between countries regarding the number of crimes per one million internet users or the frequency of certain offences committed. Social, cultural and economic factors can explain the differences. However, their correlations have not been revealed yet. Globally, Great Britain and the US had the highest number of cybercrime victims per one million internet users in 2022. On the other hand, in neighbouring Canada, having a similar level of industrialisation as the US, the equivalent numbers were an eighth of those in the US. Surprisingly, the number of cybercrimes per one million internet users in Europe reached only a fraction of that found in English-speaking countries.

Concerning different types of crimes, phishing had the highest number of victims globally, while investment fraud was the forerunner regarding the value of the damage caused. The high frequency of phishing can be explained by internet penetration and linguistic causes because it can be committed the easiest in the languages spoken by most people, where many people have internet access simultaneously. Accordingly, phishing is the most frequent in the countries using English and Chinese. On the other hand, the intensity of investment fraud correlates with the size of the given countries' securities market or the ratio of securities and bonds in the financial assets of households in those countries.

However, the distribution of cybercrime victims by age differs in different countries. The US FBI Internet Crime Complaint Center received 800,944 reports in 2022. The total damage from the reported cases was USD 10,300 billion. *Figure 2* illustrates the numbers and values of written complaints broken down by age groups.

Figure 2
Numbers, value and distribution of crime complaints in the US in 2022



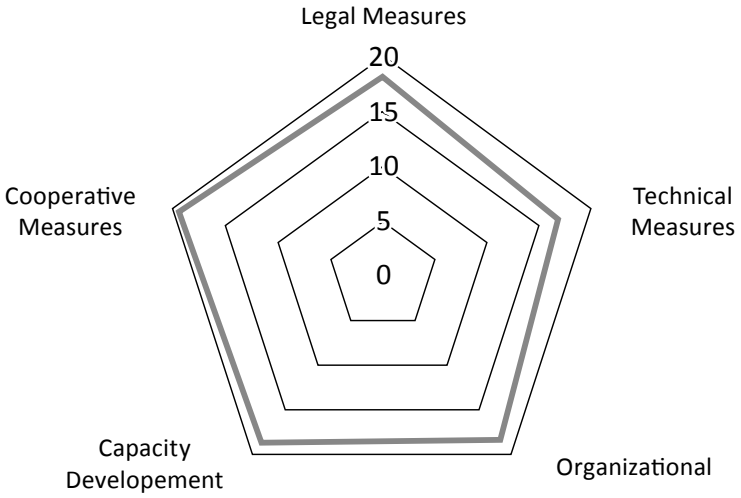
Source: IC-3, 2022

As can be observed, slightly more than a fifth of the victims were 60 or older, which is somewhat lower than their ratio in the total population, however, the damage value was the highest in their case. The age of victims reporting damage and the size of the loss are similarly distributed in most countries, including Hungary. The main reason may be older people's lower degree of skills in applying modern financial techniques. That, in turn, should warn the authorities involved, that they must pay more than average attention to protect older people. Another telling feature is that less than 4% of youth under 20 submitted complaints, which is much lower than their ratio in the total population, while the value of damage incurred for them was twice as high as that of the age group 20-29. It indicates that underage youth lacking the proper skills and experience enter deals mindlessly, resulting in severe damages. To prevent this, more attention is needed to be devoted to improve financial education at schools.

Concerning financial crime risks, it has to be pointed out that the preparedness of individual countries to protect cybersecurity is considerably different. Initiated by the International Telecommunication Union, a Global Cybersecurity Index (GCI) has been drawn up. It is an indicator measuring the readiness grade in 160 member states globally along five dimensions. According to the survey published for the year 2020, the US and Great Britain are the frontrunner. while Estonia and Spain are the only EU Member States among the first ten. Hungary has been

ranked 35, which is in the upper part of the middle range. *Figure 3* illustrates the rating of Hungary (ITU, 2023).

Figure 3
Hungary's cybersecurity index



Source: ITU (2020)

3 TYPOLOGY OF VICTIMS

The victims of "white-collar„ financial crime can be categorised into two large groups (Ganzini et al., 1990):

(1) Innocent victims who are deceived by criminals in usual commercial transactions. They can be creditors, competitors, employees or customers.

(2) "Voluntary" victims who are lulled to enter a scheme by criminals in the hope of temptingly fat profits promised (Dunn, 2007; Croall, 2009; Walklate, 2017.)

The victims' and the perpetrators' relationship is usually similar to different types of white-collar crime: it is non-violent, indirect and impersonal; the victim's person is usually totally unknown and indifferent to the perpetrator (von Henting, 1948; Dunn, 2007). Since the perpetrator will not meet directly/get to know their victim on the digital channels they use, they have no remorse for holding them back from the crime (Walklate, 2017). The subculture of the business world is another factor reducing informal control over white-collar crime. Businessmen regard efforts made to obtain a profit and manipulating the customer as a natural

part of business activities. In addition, they are willing to accept higher-than-average risks to reach higher yields (Lyng, 2005). Their mindset, therefore, leaves no room for the potential threat of being victimised; their attention is completely fixed on the envisioned enormous profit (Davies et al., 2003). Because of the „amorality" of the business world, authorities should constantly look after the market to prevent citizens from becoming easy victims of white-collar crime because of their greed (Ganzini et al., 1990). It includes drawing up the necessary regulations, setting out effective strategies for surveillance, consistent law enforcement and applying proper sanctions (Shicor et al., 2001). In addition, people can be helped to become crime victims if consumers are regularly informed about fraudulent business practices and offered advice on how to avoid them (Croall, 2009).

The socio-demographic profile of the group of „voluntary" victims differs from that in other parts of society. Based on the statistical analysis of the data collected about the victims of investment fraud cases, the Financial Industry Regulatory Authority[6] have found several characteristic features in investors' personality traits and behaviour that increased the probability of them becoming fraud victims (FINRA 2016; Goucher, 2010)

- **Failure to check the investment agent and/or advisor** Over 80% of investors, as a rule, do not check whether their advisor, broker, mediator or agent holds the relevant licence to operate as such (Harvey et al., 2014).
- **Investment into unlicensed high-risk finance products:** nearly three-fourth of known victims of investment fraud cases made investments into high-risk finance products promising high profits, while only half of those who had not become victims did so. Statistical analysis has proved victims of investment fraud decide twice as often in favour of investments promising higher than average yield than the control group (FCA, 2016).
- **Inability to recognise manipulative techniques such as persuasion and framing:** Every fifth investor is incapable to realise if different manipulative methods are used to influence their investment decision (Langenderfer-Shimp, 2001; Petty-Vacioppo, 1981).
- **Overconfidence / hubris as investment decisions are made and/or investment advisors are selected:** Comparing the investment structures of known victims of investment fraud to those not fallen prey to fraud proves fraud vic-

6 The Financial Industry Regulatory Authority (FINRA) is a self-controlling, non-governmental organisation in the US that aims to "protect the investor community from fraud and bad practices". FINRA was established in July 2007. It has significant supervisory rights over its member companies' everyday activities, employees, and the investors they serve. It is not responsible for industry supervision; at the same time, its broad sphere of competence is not subject to the accountability rules relevant to governmental regulatory bodies.

tims have made more than twice as many investments into products of their own selection following friends' or workmates' recommendations compared to the control group (Fattah, 1991). Investment fraud victims, as a rule, are overconfident about their judgement; their decisions are driven by intuition and instinct and they rely on them much more than others (Harvey et al., 2014).

4 TYPES OF FINANCIAL CRIME

Financial criminal acts can be categorised into two groups: so-called "regulated" financial crime and "non-regulated" criminal acts. Regulated crime means the deliberate, intentional violation of financial provisions, including the rules of financial and banking activities. So termed non-regulated criminal acts mainly include fraud and other kinds of deception (Alexander-Seymour, 1998).

4.1 Regulated financial crime

It includes insider trading, (banned) market-making, money laundering, bribery, misappropriation, cybercrime, tax dodging, counterfeiting, etc. (NZZ, 2022). They are deemed intentional violations of legal provisions and regulations to protect money markets and institutions. Acts of regulated financial crime are usually committed by people in leading or decision-making positions or who have access to insider information. According to Lajtár (2019), they are typically the following:

- **Bribery:** payment of a certain amount of money or offering some other advantage to influence the decision of a person or organisation.
- **Insider trading:** using confidential or insider information to buy or sell securities and finance products for the own or a third party's benefit.
- **Misappropriation:** unlawful appropriation of somebody's liquid assets or possessions entrusted in their care or disposal thereof as of their own.
- **Tax dodging:** An act that enables one to avoid the payment of taxes by hiding incomes, wealth and relevant information.
- **Cybercrime:** crime committed with computers / other IT devices or the internet causing harm to data access, the integrity and confidentiality of data including the instalment of malware, or any other criminal act related to the content of information technology data and the violation of copyright or related rights.

- **Forgery:** alteration or imitation of an original public document, banknote or security; modifying or deleting the data thereon and using such altered or imitation documents to achieve material advantage.
- **Money laundering:** covers any and all activities and financial transactions that are aimed at hiding the real source of moneys originating from the commitment of crimes and at transforming them to those of lawful origin.

As regards money laundering, the spread of virtual financial institutions, so-called neobanks[7], having no physical branches but offering digital banking increases, should be noted because albeit unintentionally, they increase the risk of committing financial fraud and money laundering (Pásztor, 2018). Recently, digital payments have been detected to be used for money laundering during investigations of different types of fraud in several member states. Using virtual IBAN account numbers (vIBAN) applied by neobanks undoubtedly allows for fast international payments, which customers appreciate. However, they hide the account holder's country of residence and make detecting suspicious transactions more difficult necessitating further efforts in tracking suspicious transactions.

4.2 Non-regulated financial crime

Non-regulated financial crimes include, first of all, identity theft, fraud, financial fraud, and other forms of deceit. They typically represent making use of misleading data or abuse of information for the purpose of financial gain. Non-regulated financial crimes usually include the following offences (Langenderfer-Shimp, 2001):

- **Identity theft:** obtaining somebody's personal or sensitive data and using them for unlawful material gain.
- **Fraud:** inducing a person to hold or continue to hold a false belief through false claims or false data for unlawful material gain. Its typical forms are:
  - **Financial fraud:** efforts to deceive individuals or enterprises by offering false reasons, investments or services.
  - **Credit card fraud:** using stolen credit card data to purchase goods or services
  - **Investment fraud:** applying deceitful tactics to persuade individuals or enterprises to invest into fraudulent arrangements.

7 IBAN (International Bank Account Number) is an international bank account number of uniform structure implemented in the European Union and other countries.

  - **Banking fraud:** using forged or misleading documents to obtain money from banks or other financial institutions.
  - **Online fraud:** using forged or misleading documents to obtain goods or services.
- **Phishing:** attempt to obtain confidential information, for instance, usernames, passwords or credit card data so that the fraudster pretends to be the officer of an authority or well-known service provider.

Criminals try to commit those types of fraud by applying the most diverse methods. Some typical methods are the following:

- **The "caisson" method:** fraudsters try to make their chosen victim invest in non-existent, low-value or high-risk shares or bonds or to transfer their funds to "secure" accounts provided by them using psychological (excess) pressure. For this purpose, the criminals often use forged documents and expert opinions and sometimes exert time pressure on their victims. (NZZ. 2022).
- **Ponzi schemes:** fraudsters lure investors by promising much higher yields than the market rate within a short time. To maximise profit, initial investors are paid the high gains promised from the funds obtained from later investors, so – because of their initial satisfaction – they will unintentionally "promote" investment into the scheme among their friends. Those who invest after the system has reached its peak will receive nothing, as the fraudsters will disappear by then with the funds transferred abroad via money laundering (FCA, 2016).
- **Pyramid game:** or network marketing, which is similar to the Ponzi scheme in many respects. However, initial investors become active players there, because they must recruit new investors to get the high commission promised. Under the scheme, again, those will lose the most who invest after the scheme has reached its peak.

Criminals use the most diverse communication channels for their schemes, for instance, telephone calls, internet, social media, mass mailing, TV or radio advertisements to reach as many potential victims as possible (Shichor et al., 2001). They can get many potential victims quickly, simply and cheaply using the channels mentioned. A specific example of fraud is when the members of a criminal gang pretend to be police officers or bank employees, contacting the selected victims over the phone under the pretext they want to warn them about threats to their accounts, investments or even their bank. They encourage their victims to transfer their savings to deposit funds claimed to be safe, which they will then withdraw (USDJ, 2015).

In the case of investment fraud cases, it usually turns out later the securities sold to the victim are garbage or non-existent in reality. Although the deceived buyers

could have ascertained without any special efforts whether the securities offered were real, most of them – dazzled by the profit envisaged – did not do so (Alexander–Seymour, 1998).

Cybercrime has recently appeared in the field of "Buy now pay later" (BNPL) financing, also termed instalment payment at point-of-sale. The criminals exploit the current weaknesses of the approval process of BNPL transactions. As no actual loan assessment takes place for BNPL services, criminals often pass inspection relying on algorithms only and order goods they want using accounts obtained through.

The latest risk factors in the field of frauds are the use of artificial intelligence (AI) and deepfake[8] technology to commit diverse acts of financial crime. AI-based chatbots[9], e.g., ChatGPT[10], can be quite easily used in schemes of online fraud. The so termed Deepfake technology can be useful in circumventing remote defense.

5 MOTIVES OF FINANCIAL CRIME

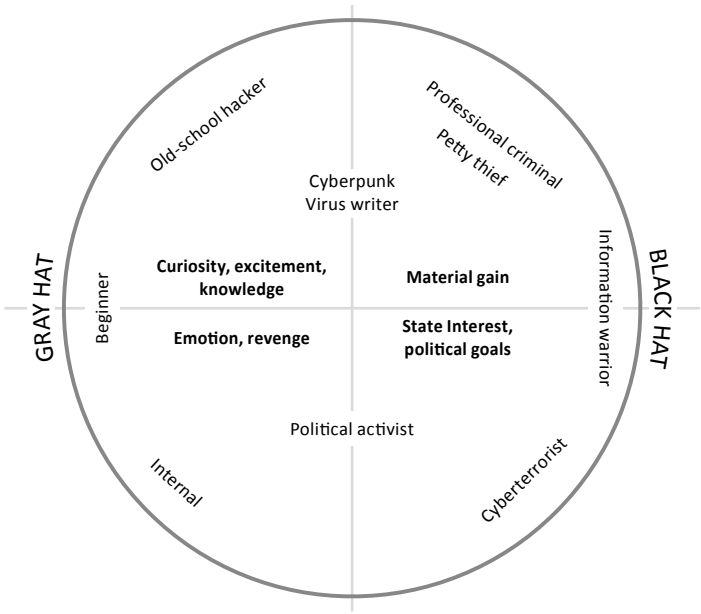
Although it may seem evident that material gain is the driving force behind financial crimes, it is not the only motive. It has turned out that in some cases, some perpetrators were motivated by professional curiosity or thirst for adventure rather than material gain, or else they wanted to retaliate for some grievance or were driven by personal revenge in committing their acts. In addition, some countries may launch cyberattacks out of state interest while terrorist organisations and criminal gangs attack protected infrastructure, including financial assets. *Figure 4* illustrates potential motives for the violation of IT systems.

8 Deepfakes are authentic looking videoclips, which use the faces of real people to display the images of non-existent people with the help of AI or visualise real people as actors in events that have not occurred in reality.

9 Chatbots are software applications that can communicate with customers without human involvement. Chatbot systems have been designed so as to convincingly imitate human behaviour in a dialogue. Although they cannot be considered artificial intelligence in the classical meaning of the term, at today's technological level they can solve tasks such as taking online orders without human intervention.

10 ChatGPT (GPT = Generative Pre-Trained Transformer) is a linguistic model that is capable of real-time communication with people, because it allows processing a natural language and can generate logically suitable answers to users' questions or requests.

Figure 4
Motivational network of IT crime



Source: Varga Á., 2022

The term "hacker" initially meant an IT professional having a comprehensive view of the operation of IT systems, who could cross the borders of a system so as to make it do more than what its developers originally envisaged. However, criminal groups also have attracted people with IT knowledge who can "break" into a system (use it unauthorised) and can obtain information from it for themselves or others, so – step by step – the term "hacker" received a negative meaning. The hacker culture initially regarded as something positive has diverged into subcultures existing side by side. One of them is the group of "crackers": they are people who use their professional skills for malevolent actions or causing damage. More respectable hackers, however, still remain. For instance, grey-hat crackers are people who – although they violate ethical norms or principles – but they do not act out of malevolent initiative as black-hat crackers. Grey-hat crackers are the middle road between white-hat crackers (or ethical hackers) and black-hat crackers who exploit people's weaknesses and the vulnerability of systems for material gain (Varga Á., 2022).

6 SANCTIONS AGAINST FINANCIAL CRIME

Financial crimes are deemed grave for apparent reasons, and severe punishment can be meted out for them. Subject to their severity, imprisonment, confiscation of property and/or fines can be ordered. In addition, the personal and professional reputation of people found guilty of committing financial crimes may be impaired, and they can also be banned from filling positions in the field of finance or other jobs based on trust forever or for a definite period (US DoJ, 2015).

Perpetrators of criminal crimes also bear civil in addition to criminal liability. Under it, they can be punished by the deprivation of profit unlawfully gained, liability obligation or orders of termination and stoppage. The latter sanctions are usually ordered to prevent individuals and organizations from committing financial crimes in future.

As can be observed, cybercrime exerts significant social impact, whether speaking about phishing or fraud, causing harm to people's material security and property. As uninterrupted technological development brings about new emergencies one after the other, as new methods and areas appear, both criminal and civil law must respond to them. However, most legal experts in this country agree that the relevant provisions of the Criminal Code (Hungarian acronym Btk) in effect including Section 315 on information system fraud, Section 422 on illicit access to data, Section 423 on breach of information system data and Section 424 on compromising or defrauding the integrity of the computer protection system or device are satisfactory for the time being to cover crimes committed online, i.e., expanding them would only be justified if markedly new forms of cybercrime appeared (Grund, 2021).

Criminal and civil law instruments are just a part of the measures applied to create a proper defence for cyberspace and maintain its security. The state is responsible for protecting against cybercrime in addition to jurisdiction and law enforcement. It means a series of tasks beginning from establishing proper technical standards and requirements, licensing the distribution of IT products and services, ensuring the protection of government IT structures, preparation for intelligence and law enforcement to information to and education of the citizens.

The set of tools creating cybersecurity must have the preparedness and proper approach of individuals wanting and expecting security. The careful use of the internet and efforts to maintain cybersecurity are satisfactory, in addition to protecting passwords and IT devices; if attempted or carried out, attacks are always reported. Reports by individual users contribute significantly to a higher degree of consciousness of society and allow more effective defence.

The international dimension must be addressed to establish cybersecurity. Most countries have different rules to penalize cybercrimes. Due to cultural differences and traditions, not all crimes trigger the same response. Therefore, if the regulations referring to international wrongful acts differ in various countries, managing the issues of jurisdiction and sharing investigation competence becomes more complex, which results in the slowdown of the exchange of information. As cybercrime is global by nature, the countries affected must establish a high standard of collaboration among their relevant agencies; they must harmonize regulations and share research findings all the more so as the majority of the countries of the world have to face very similar challenges despite their differences in the areas of law or the institutional system. They often have to fight the same perpetrators, thus legal agreements and regular exchange of information between countries and their relevant agencies can be helpful in all countries taking part in the collaboration.

7 FREQUENT QUESTIONS AND ANSWERS ABOUT FINANCIAL CRIME

As already explained above, financial crimes are usually complex and the legal and regulatory environment relating to them is not always clear partly because circumstances can quickly change (FINRA, 2016). Because of such uncertainties, participants in education aimed to increase the standards of financial literacy often raise many questions requiring clarification. Therefore, to support educators, the authors offer short answers to some questions often arising in connection with financial crime.

Q1 What to do to protect myself from financial crime?

Experience has shown *users are the weakest link in the* defence against cybercrime and fraud. If you want to be capable to protect yourself from damages caused by cybercrime, you must be aware of potential risks and you must take all possible measures for protection. It includes recognising attempts for phishing and avoiding investment into schemes the conditions of which are too nice to be true. You must be careful and wary about sharing your personal data in any form.

Here are some features probably indicating investment fraud or deception, so you must be careful about them:

- **Promise of guaranteed high profit reached quickly:** in real life, high profit always goes hand in hand with high risk, which means the investor may lose all their investment. The con

- scious assumption of high risk differentiates investments from savings as the yield of the latter is known and guaranteed in advance, but it is usually low (FCA, 2016; FINRA, 2016).
- **Complex (sophisticated) financial products:** The complexity of a financial product or a complex investment strategy are never the prerequisite or guarantee of reaching a higher-than-average profit. If the operation of the scheme offered is not clear or transparent, particularly if exchange rates or interests change significantly, you had better refrain from the investment, even if the deal does not violate any provision. Typical products promising high profit include leverage and derivative instruments, such as financial agreements on FX (forex) and CFD (contract for difference) managed on online trading platforms. Those deal types are not banned, but they are only suitable for people who are able to incur a high loss without any problem. High leverage means deals can be made using an amount defined by the service provider (margin) where the transaction value can be ten times or even a hundred times of that amount deposited. Increasing the leverage promises high profit, but all leverage transactions carry the risk of multiplied losses, which, unfortunately, investors only face too late.
- **Making an investment without drawing up a contract or other documents:** If an advisor / agent tries to convince their client to make an investment through verbal information and promises only, the wonderful promises and lovely words probably hide a fraud. In every country legal provisions require that investors must be given detailed written information, so termed prospectus, about the technical, economic and legal features and the related risks of the investment option offered, as well as about the organisation and people preparing and managing the investment.
- **romise of guaranteed profit at all times:** Any investment offer must be suspicious if it promises the growth of the invested amount but will not lose its value even in a crisis situation. In reality, impairment may occur even with the most conservative investments.
- **Time pressure and time limit on the investment:** A typical sales technique of investment fraudsters is to say you can only make use of the promising investment option for a short time. By pressurising the victim to make a quick decision they can prevent him/her from careful consideration and obtaining more information.

Q2 How to avoid becoming the victim of cybercrime?

- First of all, take care of the protection of the passwords on your computer, cell phone and the applications used for managing financial transactions. The passwords must be regularly changed. It is the only way to prevent unauthorised entry to your system using passwords obtained from database hacking or abuse passwords potentially obtained. You should devise the passwords you select so that they are difficult to hack. It is reasonable if your passwords include at least eight digits including numbers, lowercase and uppercase letters and special characters randomly generated. Your date of birth, surname or their combinations or the use of simple numeric sequences should be avoided as they can be hacked relatively easily and fast.
- The core software of your computer and cell phone including the firewall and antivirus programmes of the operating system must be regularly updated making unauthorised entry into the system more difficult. Avoid using a financial application or entering your bank account when you use a public Wi-Fi network (used by others too) to access the internet, because in such cases confidential data might be accessed easily by strangers.
- Request a separate bank card for internet shopping and only deposit as much on it that you need for your shopping. Revealing the data of your bank carrying all your savings to web shops is extremely dangerous.
- Be careful if a stranger tries to contact you over the phone or in e-mail. Financial service providers and professional or serious websites only ask for your password in their entry application but never in person; so, you should never give them under any pretext even if the caller asks for it referring to the prevention of some damage. Do not install software recommended or sent by an unknown person without a preliminary security check. It can install a Trojan horse in the software on the computer or cell phone that allows the theft of your passwords or makes the data and programmes stored on the computer or cell phone inaccessible. You should also be wary of sharing information on social media or which web shop you order from. Use cash on delivery if you shop from and unknown web shop.
- Any e-mails or text messages informing you about an unexpected high-amount win or inheritance from an unknown person which require you to transfer some money to cover costs in advance or to reveal your banking data are mostly fraud attempts. Do not reply to them. Phishing emails – even if they are in Hungarian – are usually sent by criminals who do not speak Hungarian, so they use some compiler to translate the text into Hungarian. So, pay attention to the language of the mail received as unusual terms or spelling mistakes can mark the fraud.

Q3 Where to turn if you become victim of digital abuse?

In Hungary, Act L of 2013 on the electronic information security of state and local government bodies has appointed the National Cybersecurity Institute (NKI) within the National Security Service (NBSZ).

When can NKI help?

- Virus infection on home electronic devices.
- Phishing messages or detection of phishing website.
- Detection of damage of government site.

Q4 What to do if I have become victim of cybercrime?

If criminals have caused damage despite preventive measures, the crime should be reported the police as soon as possible and – if the personal bank account or security account has been involved – then with the account managing bank as well.

Tthe crime should be reported to the closest police station without any delay after perceiving the damage. Time is very important from the aspect of catching the perpetrator(s) and to recover the damage.

Q5 Under what conditions needs a bank to compensate the account holder in case of internet fraud?

- If the payments service provider is responsible for carrying out/initiating an unauthorised payments transaction, the payments service provider managing the current account shall, on request, immediately compensate the customer for the damage and loss of funds including the amount of the unauthorised payment transaction. In such a case, the payments service provider initiating the payment shall prove that – within its sphere of competence – the payment transaction has been authorised and accurately recorded and its delivery was not prevented due to a technical fault or breakdown of the payments service it provides.
- Further compensation can be ordered in observance of the provisions applicable to the contract between the paying party and the payments service provider, or the paying party and the service provider initiating the payment.

Q6 Can you expect compensation by the perpetrators of the crime committed against you?

Subject to the severity of the crime, the consequences may be severe. They may include a long term in prison, a large fine or confiscation of property. On the other hand, it is far from certain the perpetrator is caught, or you can receive compensation for the damage even under a successful criminal procedure. In such a case you can consider launching civil proceedings to obligate the perpetrator to

compensate for damages and to pay grievance fee provided the perpetrator does have some property or assets to be used for compensation. Given the uncertainties mentioned, taking out insurance for damages caused by cybercrime is worth considering. Cyber insurance works similarly to casco insurance.

If a cyber incident occurs and the IT system breaks down or is destroyed, the assets of an enterprise may be damaged, the business may lose revenues, may have to face high amounts of unexpected expenses or fines or – last but not least – it will be liable for the damage caused to others. For instance, a ransomware infiltrates the IT system, causing valuable customer data to be obtained by unauthorised persons. Because of GDPR, it is clear the problem is not so much of an IT but an economic nature.

Cyber insurance or cyber-liability insurance is an insurance contract purchased by sole traders or enterprises to protect themselves from monetary damage caused by cyber-attacks. It helps reduce the impact of business breakdown resulting from a cyber-attack focusing on the financial aspects of recovery. Cyber-liability insurance, in addition, can help cover the different expenses incurred by the organisation because of a cyber-attack, related for instance to data recovery or reattracting its customers (Sebők, 2022).

8 SUMMARY AND CONCLUSIONS

The objective of this paper is educational. It intends to inform readers about cybercrime's principal risks and typical features. It reviews the primary reasons for the spread of cybercrime and the critical statistical data. It has introduced the types of personality that are the most exposed to financial risk/fraud appearing in cyberspace, while it has also categorised the main types of financial crimes. Next, it intends to help people recognise the threat of financial fraud. The key objective of the review and categorisation has been to provide educators dealing with the development of financial literacy with in-depth knowledge about cybercrime. The authors hope this paper can contribute to better identifying the threats lurking in the online space, taking necessary protection measures, and calling attention to the new threats appearing as financial matters get increasingly digitised. Active user participation in the fight against cybercrime cannot remain of an ad hoc nature, as it requires uninterrupted participation. The main reason is that the regulatory environment is lagging behind the changes in the field of digital finances, while the criminals are often ahead of the regulatory environment and the authorities. Therefore, it cannot be emphasised enough that strong cybersecurity can only be achieved if users take a proactive part, for which they need to be increasingly prepared, be financially literate and possess the necessary skills.

REFERENCES

AAG (2023): The Latest 2023 Cyber Crime Statistics (updated December 2023), https://aag-it.com/the-latest-cyber-crime-statistics/ (downloaded: 06.12.2023).

Alexander, E. – Seymour, A. (1998): *Roles, Rights, and Responsibilities: A Handbook for Fraud Victims Participating in the Federal Criminal Justice System*. Washington: Police Executive Forum.

Croall, H. (2009): White collar crime, consumers and victimisation. *Crime, Law and Social Change*, 51(1), 127–146.

Davies, P. – Francis, P. – Jupp, V. (eds.) (2003): *Victimology: Theory, Research and Policy*. New York: Palgrave Macmillan.

Katona, Cs. (2021): Kiberbűnözés Magyarországon, avagy hová forduljon digitális bűncselekmény esetén? [Cybercrime in Hungary, or where to turn in the case of cyber crimes?] *Arsboni*, 2021.11.02., https://arsboni.hu/kiberbunozes-magyarorszagon-avagy-hova-forduljon-digitalis-buncselekmeny-eseten/ (downloaded: 09.12.2023).

van Dijk, J. J. M. (1999): Introducing victimology. In: van Dijk, J. J. M. – van Kaam, R. G. H. – Wemmers, J. (eds.) (1999): *Caring for crime victims*. Monsey: Criminal Justice Press, 1–12.

Dunn, P. (2007): Matching service delivery to need. In: Walklate, S. (ed.): *Handbook of Victims and Victimology*. Abingdon, UK: Routledge, 255–281.

Fattah, E. A. (1991): *Understanding criminal victimisation*. Scarborough: Prentice Hall Canada.

Financial Conduct Authority (FCA) (2016): Over 55s at heightened risk of fraud, says FCA. Press Release, https://www.fca.org.uk/news/press-releases/over-55s-heightened-risk-fraud-says-fca (downloaded:2023.12.04.).

Financial Industry Regulatory Authority (FINRA) (2016): FINRA risk meter. https://www.finra.org/investors/tools-and-calculators (downloaded:2023.09.14.).

Ganzini, L. – McFarland, B. – Bloom, J. (1990): Victims of fraud: Comparing victims of white collar and violent crime. *Bull Am. Acad. Psychiatry Law*, 18(1), 55–63.

Goucher, W. (2010): Becoming a cybercrime victim. *Computer Fraud and Security*, 10, 16–18.

Grund, B. (2021): A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról [On crimes in cyberspace and Hungarian practice thereof]. *MTA Law Working Papers*, 21, https://docplayer.hu/235743259-A-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol.html.

Harvey, S. – Kerr, J. – Keeble, J. – McNaughton Nicholls, C. (2014): Understanding victims of financial crime: A qualitative study with people affected by investment fraud. NatCen, Financial Conduct Authority. http://www.fca.org.uk/static/documents/research/qual-study-understanding-victims-investment-fraud.pdf (downloaded: 16.10.2023.10).

von Hentig, H. (1948): *The criminal and his victim*. New Haven: Yale University Press.

ITU (2023): Global Cybersecurity Index 2020, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Krasznay, Cs. (2021): Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése [Twenty years against cybercrime – evaluation of the Budapest Treaty]. *Külügyi Szemle*, 1, https://www.academia.edu/49598305/H%C3%BAsz_%C3%A9v_a_glob%C3%A1lis_kiberb%C5%B1n%C3%B6z%C3%A9s_elleni_k%C3%BCzdelemben_A_Budapesti_Egyezm%C3%A9ny_%C3%A9rt%C3%A9kel%C3%A9se.

Lajtár, I. (2019): A kiberbűnözésről [About cybercrime]. *Ügyészek Lapja,* 1, https://ugyeszeklapja.hu/?p=774.

Langenderfer, J. – Shimp, T. A. (2001): Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, 18(7), 763–783. https://doi.org/10.1002/mar.1029

Lyng, S. (2005): Edgework and the risk-taking experience. In: Lyng, S. (ed.) (2005): *Edgework: The sociology of risk-taking* New York and London: Routledge,17–49.

Neue Zürcher Zeitung (NZZ) (2022): Interpol sieht Finanz-Straftaten und Cyberkriminalität als weltweit grösste Bedrohungen an. https://www.nzz.ch/panorama/interpol-sieht-finanz-straftaten-und-cyberkriminalitaet-als-weltweit-groesste-bedrohungen-an-ld.1708027 (downloaded: 04.09.2023).

Orbán, A. (2023) Közszolgálati Online Lexikon [Public Service Lexicon]. Budapest: Nemzeti Közszolgálati Egyetem, https://lexikon.uni-nke.hu/szocikk/szamitogepes-bunozes/ (downloaded: 20.10.2023).

Poletaeva, V. – Perepelitsa, D. – Arhangelskaya, Tatyana – Zaripov, Ilyas – Pásztor, Sz. (2019): The research task of banks and authorized government institution interests in manufacturing companies' investment projects congruence. *International Journal of Mechanical Engineering and Technology*, 10(2), 1603–1609.

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

Pásztor, Sz. – Szijártó, N. (2016): Internal Devaluation and its Macroeconomic Consequences in the EU Periphery. *International Trade and Trade Policy*, 4(8), 6–23.

Petty, R. E. – Cacioppo, J. T. (1981): *Attitudes and Persuasion: classic and Contemporary Approaches*. W.C. Brown Company Publishers.

Sebők A. (2022): Kiberbiztosítás: Ezért van rá szüksége [Cyber insurance: that is why you need it]. MWT Solutions, 22.10.08., https://mwtsolutions.eu/hu/cikk/kiberbiztositas-ezert-van-ra-szuksege/.

Shichor, D. – Shechrest, D. K. – Doocy, J. (2001): Victims of investment fraud. In: Pontell, H. N. – Shichor, D. (eds.) (2001): *Contemporary issues in crime and criminal justice: Essay in honour of Gilbert Geis*. Upper Saddle River: Prentice Hall, 81–96.

Shivaraj, S. (2023): Financial-crime: Understanding its Growth, Threat and Effects. *The Dope*, 2023.03.03., https://thedope.news/financial-crime-understanding-its-growth-threat-and-effects (downloaded: 01.12.2023).

Statista (2023): Estimated cost of cybercrime worldwide 2017-2028 (in trillion U.S. dollars) https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwid.

Surfshark (2023): Cybercrime statistics. https://surfshark.com/research/data-breach-impact/statistics (downloaded: 06.12.2023).

Szóka, K. (2021): A pénzügyi kultúra és tudatosság meghatározása és magyarországi helyzete [Definition of financial literacy and its position in Hungary]. *Economica*, 12(3-4), https://doi.org/10.47282/economica/2021/12/3-4/10417.

Terták, E. – Kovács, L. (2023): Financial security on cyberspace – PÉNZ7 thematic week, *Economy and Finance*, 10(1), 5–19, https://bankszovetseg.hu/Public/gep/2023/005-019%20E%20Tertak%20Kovacs.pdf.

United States Department of Justice (US DoJ) (2015): Financial fraud crime victims. https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud (downloaded: 11.11.2023).

Varga, Á. (2022): Az információs rendszerek megsértésének esetei, motivációi és szabályozási perspektívái [Cases, motivations and regulatory perspectives of information systems breaches], https://www.hte.hu/documents/10180/4737479/Az_informacios_rendszerek_megsertesenek_esetei_motivacioi_es_szabalyozasi_perspektivai.pdf.

Walklate, S. (2017): *Handbook of Victims and Victimology.* 2nd Edition, New York, London: Routledge.

Weisburd, D. – Wheeler, S. – Waring, E. – Bode, N. (1994): *Crimes of the Middle Classes: White Collar Offenders in the Federal Courts* (Yale Studies on White-Collar Crime Series): New Haven: Yale University Press.