ECONOMY AND FINANCE • VOL. 11. ISS. 4 • DEC 2024 • DOI: 10.33908/EF.2024.4.2

# PHISHING AND SOME POSSIBILITIES OF ITS PREVENTION

*Gabriella Biró – Milán Kiss*[1]

**ABSTRACT**

In parallel with the advance of digitalisation, cybercrime has grown into one of the most prominent issues in recent years, especially in the financial sector. Instead of slowing it down, developments in the last few years, including COVID-19, have given a boost to this process. Phishing, one of the most common types of cyberattacks, is worthy of study, also by reason of its prevalence. This paper aims to provide an overview of the phenomenon of phishing and the possibilities of anti-phishing protection, with special regard to the financial sectors' exposure and the legal context. First, we analyse the most frequent types of phishing, together with their technical and technological background. For the legal context, since the issue is regulated at multiple levels (international, EU and national legislation), we separately discuss the regulation of phishing in private and public law, in particular the directive on payment services in the internal market (PSD2) as well as the payment services act transposing it into Hungarian legislation. The directive imposes a form of strict liability on payment service providers and is also unfavourable for them in terms of the rules of evidence vis-à-vis consumers and microenterprises as clients. The paper also investigates criminal law implications, or more precisely, which offence the respective forms of phishing correspond to under criminal law. Finally, we present relevant developments in law enforcement and IT security. By doing so, we explore the possibilities of payment service providers for preventing phishing attacks on both the provider's and the client's side, and if the incident has occurred, what options they have for mitigating consequences.

*JEL classification:* K24, G21

*Keywords:* cybercrime, phishing, payments

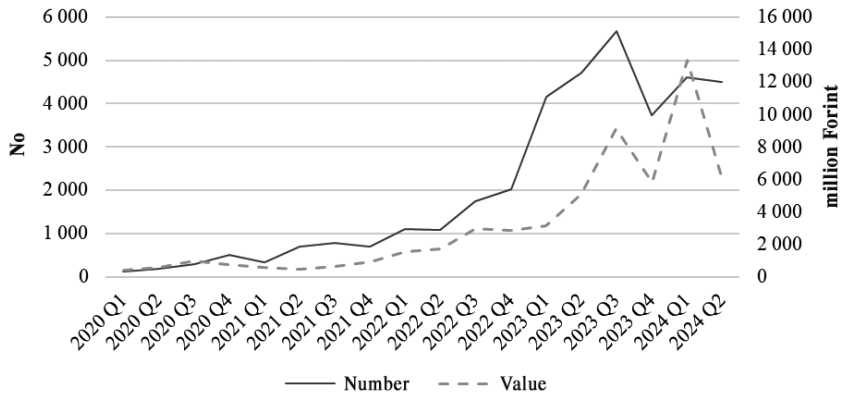
1 *Gabriella Biró*, IT security expert, PhD student, Ludovika University of Public Service, corresponding author. E-mail: biro.gabriella@uni-nke.hu.
*Milán Kiss,* Head of Department, BinX Zrt., PhD student, University of Miskolc. E-mail: milan.kiss@student.uni-miskolc.hu.

## 1 INTRODUCTION

Today, cybercriminal activity is becoming more and more prevalent all around the world and is now a considerable economic factor (VISA, 2023). According to the report of the Word Economic Forum, the scale of cybersecurity is so large that if it were taken as a state, it would be the third largest economy in the world after China and the United States of America (World Economic Forum, 2024). This is presumably because the digitalisation process accompanying technological progress – apart from its legal uses – opens up whole new possibilities to criminals as well. Cybercrime is a general problem, but breaches and abuses are most often committed within financial infrastructures and in cash, of which we can study only the former (Anderson et al., 2019). Therefore, it is reasonable to approach the phenomenon in general through the financial sector's exposure to cybercrime. However, it should be noted that the financial sector and in particular payments are developing and evolving at a fast pace (Kovács, 2010), which makes research in this field more challenging. Furthermore, the authors are also aware that while the object of our study, cybercrime, is digital by definition, cybercriminal activity has a manifest effect in physical space and payments by physical money (cash transactions). Nevertheless, quantifying and analysing these effects statistically is a quite complex task. Accordingly, the focus of this paper is limited to types of abuses identified through to electronic payments, and especially to data from Hungary.

The legal framework applicable to financial services is a determining factor in the behaviour of both users of these services and those abusing them. The procedure of law enforcement authorities, minimum measures and procedures for the prudent operation of payment service providers, and also their contractual relationships with clients and other service providers are regulated within this framework, which should therefore be analysed more closely. It should be noted that it is a quite intricate regulatory framework due to its international nature. Yet, as Hungary is subject to obligations of legal harmonisation as a member state of the European Union (EU), Hungarian national legislation, including the directly applicable legislative acts of the EU, can be considered representative for our purposes. In line with this, we seek to present the legislation applicable to phishing through the Hungarian regulatory framework. Magyar Nemzeti Bank (the Central Bank of Hungary, MNB) publishes statistics on the scale of fraudulent activities observed in payments. These data provide a picture of the scale and dynamics of the problem.

**Figure 1**
**Number and value of successful fraud attempts in electronic payments**




*Source:* MNB, 2024b

As the MNB data clearly show, there has been a considerable increase in both the value and number of successful fraud attempts in the last five years. At the same time, the value of payment fraud is still insignificant over all electronic payments. MNB reports that '[i]n terms of the methods applied in fraud cases, phishing had the highest share in 2023, accounting for 71% of all successful card fraud cases' (MNB, 2024a). Another important finding from a representative survey by CIB Bank Zrt. is that there is no correlation between individuals' social or demographic status and their likelihood of falling victim to fraud (CIB Bank, 2024).

As the observations of MNB also indicate, phishing is a prominent form of cyberattacks. Based on the 2023 IOCTA report[2] of Europol[3], phishing may be a first step in, or an enabler of virtually any type of cybercrime. The 2024 report continues to identify phishing as the most commonly used attack vector. Phishing is a key facilitator of most types of online fraud schemes and malware-based attacks, aiming to penetrate systems to steal the data stored in them or for financial gain (Europol 2023; 2024c).

Our comprehensive inquiry into the phenomenon of phishing seeks to identify possible countermeasures and means of protection against its different forms, and against the regulatory, technological and law enforcement background, as

2 Internet Organized Crime Threat Assessment (IOCTA).

3 European Union Agency for Law Enforcement Cooperation (Europol).

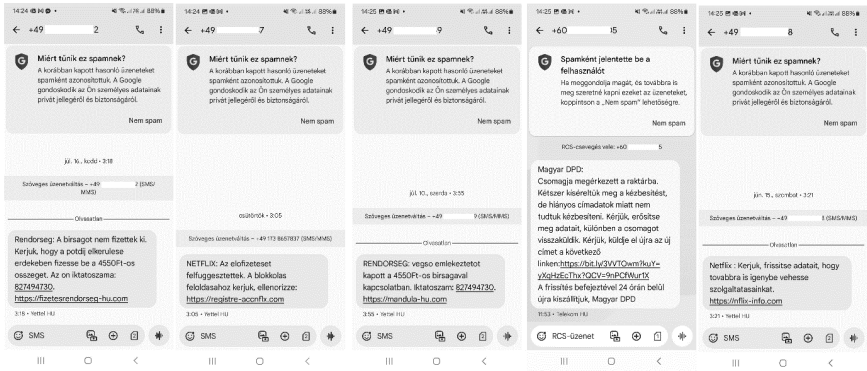
well as how these can be jointly used to reinforce the secure operation of the payment system.

## 2 THE DEFINITION AND FORMS OF PHISHING

The term 'phishing' refers to attempts by attackers to obtain data and information from the target in order to use them afterwards to elicit financial gain or for further attacks. Phishing is a technique involving psychological manipulation (social engineering) to lure the target with a bait, e.g. a potentially interesting (e-mail or text) message, into giving away their data voluntarily, or downloading harmful content or installing applications that steal their data by technological means (Oroszi, 2020).

Phishing attacks may be categorised by the channel of communication (e-mail, text message, WhatsApp, etc.), reach (mass or targeted) and the method used for deception. Phishing primarily refers to fraud by electronic mail, but according to the 2024 IOCTA report of Europol, phishing via text messages, or 'smishing', is the most common type of phishing today, followed by 'vishing', or voice phishing, carried out via fraudulent phone calls. The 2024 IOCTA report also finds an emerging trend for QR code phishing, or 'quishing', where the victim is prompted to interact with a QR code message, e.g. visit a website (Europol 2024c). In phishing attacks via telephone networks (smishing, vishing), fraudsters often manipulate the telephone number (spoofing) to make the recipient believe that the message or call is coming from an entity that they are actually in contact with, e.g. their payment service provider or the police.

**Figure 2**
**Examples of smishing messages**




*Source:* collected by the authors

In everyday life, we mostly encounter mass phishing, where the aim is to reach as many recipients as possible so that at least some of the thousands of messages sent out should succeed. In most cases, the criminals avoid the cost of these messages by using hacked mailing servers or the compromised telephone subscriptions of victims of previous phishing attacks (György, 2021). Such mass messages tend not to be very sophisticated, often containing typos, grammatical errors and inconsistencies. That is because the Hungarian version is usually prepared by automatic translation. However, the rise of artificial intelligence in recent years has brought considerable 'improvement' in their linguistic quality. Targeted phishing or 'spear phishing', by contrast, is concentrated on high-value recipients, utilizing personalised messages directly addressed to the targeted person by name and content that is tailored to look relevant to the target. A subcategory of these attempts aimed at corporate executives is called 'whaling'.

The target and the channel of communication are defining factors in the modus operandi of phishing, but it is a common feature of all types of phishing that the perpetrator impersonates somebody else in the message sent. Phone calls are often initiated by alleged employees of service providers, e.g. credit institutions, and text messages are usually sent in the name of courier services or the police. Fraudulent e-mails often notify of public utility arrears, or are sent in the name of service providers, sometimes credit institutions. Fraud schemes of greater sophistication are carried out through other communications channels, such as social media or chat applications, e.g. fraudsters pretending to be prospective customers on online marketplaces to obtain sellers' data (e.g. for the authorisation of credit institutions' services).

Phishing communications typically state that the data should be provided in the interest of the potential victim, for instance, to secure a financial gain, or to avoid or prevent losses. They tend to urge or even threaten the victim to act promptly so that they do not have time to deliberate if it is justified or reasonable to comply with the request. As pointed out earlier, nowadays, phishing communications are not so easily recognisable by the grammatical and stylistic errors that were so characteristic of Hungarian-language attacks a few years ago. Criminals can now effortlessly produce high-quality content in any language with AI-assisted tools.

Apart from generating persuasive text using large language models, criminals can now put AI at their service in other dimensions of communication. With the so-called deepfake technology, existing images and audio can be used for creating convincing video and audio recordings that are very hard to distinguish from authentic content (Szabó 2023). With these resources, criminals may even initiate real-time phone or conference calls to more credibly impersonate stakeholders whom the victims willingly oblige or provide sensitive data. The press has reported several cases where unsuspecting employees were instructed in a video

conference call to transfer large amounts of money by whom they thought was the company's chief executive or chief financial officer (Magramo, 2024). According to the 2024 report of Europol, this is only one example of the potential of artificial intelligence to facilitate criminal activities, and it is expected that criminals will make increasing use of such methods in the coming years (Europol 2024a).

MITRE ATT&CK®, a widely used knowledge base for modelling and analysing threats, places phishing attacks into the reconnaissance and initial access phase, which is in line with the Europol observation that phishing is a precursor to other criminal acts (mitre.org. 2024). Although the two sources cited above have fundamentally different approaches to phishing, they clearly show that it is always an introductory step to acts defined by law enforcement bodies as a crime punishable under criminal law, or by cybersecurity experts as a cyberattack (Krasznay, 2023).

## 3 PHISHING IN A LEGAL CONTEXT

After providing a definition of phishing, it should be examined whether there are applicable provisions in the legislation, and if yes, what does this legislative framework for phishing and possible means of defence look like. Unsurprisingly, phishing is not directly mentioned in the legislation, but many provisions apply to such forms of fraudulent activity.

Since Ulpian, a distinction is made between public and private law. These two parts of the law are subdivided into further branches (Lábady, 2014). Accordingly, it seems logical to analyse the relevant legislation along this classic structure, having regard also to its embeddedness in international and EU law. The latter has shifted markedly to directly applicable legislative acts in recent years. As a result, more and more regulations of the European Parliament and the Council are applicable in Hungary as well.

### 3.1 Phishing in private law and the rules of liability for damages

Causing damage unlawfully is, of course, prohibited as a general rule in the Civil Code of Hungary[4] [Sections 6:518 to 6:520]. The codified rules of liability and the associated legal dogmatics and jurisprudence have been covered in depth by legal scholars and economists, for instance in (Szalai, 2024). However, these general cases are less relevant for phishing, where the party causing the damage is very rarely called to account before the courts. Therefore, it is more informative to

4 Act V of 2013 on the Civil Code.

study claims for damages arising out of payment services. After all, the funds obtained from cybercriminal activity will eventually be processed by payment service providers. The legislative basis is the EU Directive on payment services in the internal market, or PSD2[5], as well as the Hungarian Payment Services Act (PSA)[6] transposing it – besides other pieces of national legislation – into Hungarian law.

In the context of payment services, compensation, and in particular refund of the transaction amount, occurs in two main areas. The first case of liability for payment orders iswhen the payer provides incorrect payee data for the payment order. For these situations, Section 48(1) of the PSA provides that if a payment transaction is executed based on a unique identifier, it is deemed to have been executed with regard to the payee specified by that unique identifier. According to Section 48(3) of the PSA, the payment service provider is not liable for non-execution or defective execution of the payment transaction due to an incorrectly provided unique identifier. In other words, payment service providers specify the payee based exclusively on a unique identifier, such as account number, IBAN and secondary account identifier details of the account, and are obliged to verify the payee's name only when executing official transfer orders or credit transfers based on remittance summons. Consequently, if the payment service provider records the payment order with an incorrect unique identifier, e.g. a wrong account number provided by the payment service user, the payment service provider has no liability for a potentially defectively executed payment transaction. On these grounds, the liability of the payment service provider in instances of invoice fraud or account switching fraud[7] is far from straightforward. In these cases, the unique identifier for which the payment transaction is deemed executed is in fact provided by the payer (i.e. the company).

However, disputes on liability for damages occur the most often in connection with payment instruments (such as payment cards, or mobile and online banking applications), as the rules of liability laid down in the PSA are very different from those in the Civil Code, which are based on fault. The degree of fault is also the starting point in the PSA. The relevant provisions are found in Section 40(1) and (2) of the PSA, which specify that the payment service user is obliged to use the payment instrument in accordance with the terms of the (payment service)

5 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

6 Act LXXXV of 2009 on the Pursuit of the Business of Payment Services.

7 For more information on these types of fraud see https://kiberpajzs.hu/csalastipusok/telefonos/munkahelyi-csalas-hamis-ugyfel-beszallito/ and https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/kozel-90-millios-utalast-kert-egy.

framework contract, and to act with the care that is generally expected under the given circumstances to ensure the security of both the payment instrument and the personalised security elements required for its use, such as the personal identification number (PIN) or similar codes. The payment service user is obliged to notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument. Since the contents of the framework contract are specified in the legislation, acting with the generally expected care under the given circumstances is in effect the basis of reference also in the PSA. If the unauthorised payment transaction is not carried out with a payment instrument, the payment service provider is obliged to bear the loss and, hence pay compensation to the payment service user without delay. That may happen in the event of unauthorised access to or intrusion into the IT systems of the payment service provider [Section 44(1) of the PSA]. The payment service provider has full liability when the damage is caused by a personalised procedure by means of telecom or information technology devices that function as a payment instrument, or the payment instrument was used without personalised security credentials. This is applicable for instance to payments by virtual payment cards. Basically, this provision stipulates the liability of the payment service provider in cases of online payment fraud. Furthermore, the PSA and the Government Decree on complaints mechanisms in payment services[8] jointly specify the deadline by which refund must be paid at the latest. Allowance is made for exemption from liability, which, however, is very limited in line with the intention of EU legislators. The provisions of the PSA above basically impose strict liability on payment service providers, since the fact that damage has occurred renders them liable. In addition, the provider has full liability under quite rigorous procedural rules, with a very limited scope for exemption where the user is a consumer or microenterprise. In its 'Anti-fraud Recommendation'[9], MNB lays out detailed requirements in relation – among others – to Sections 44 and 45 of the PSA, based primarily on existing case law known at the time of publication of the Recommendation and the provisions of PSD2. As a result, the financial losses incurred by payment service users falling victim to phishing attacks are refunded in certain situations by payment service providers.

8 Government Decree No 435/2016 of 16 December 2016 on the detailed rules for the complaints mechanism for investment firms, payment institutions, electronic money institutions, voucher issuing undertakings, financial institutions and independent financial service intermediaries, and for their complaints mechanism policies.

9 Recommendation No 5/2023 of 23 June 2023 of the Magyar Nemzeti Bank on the prevention, detection and management of abuses observed through payment services.

### 3.2 Anti-phishing instruments of public law

In the public law context, we can find relevant provisions mainly in financial and criminal law. As financial law – which regulates primarily the prudent operation of service providers – is quite extensive in scope and has multiple levels, the length of this paper only permits reference to the most important financial law provisions.

While privacy and the protection of personal data are obviously highly relevant in the context of phishing, a discussion of this dimension would provide sufficient material for a separate study, especially because of the extraterritorial nature of data protection law (Molnár, 2021).

#### 3.2.1 IT security requirements in financial law

The security of payments – including the avoidance of losses to users to the extent possible – is regulated in PSD2 (or in Hungary, the legislation transposing it, most importantly the PSA) and the related Commission delegated regulations. These include, among others, provisions for the management of operational and security risks [Sections 55/A and 55/B of the PSA] and requirements for authentication [Section 55/C of the PSA] by payment service providers. From the point of view of IT security, the Government Decree on IT security[10], and two relevant MNB recommendations (the recommendation on the protection of IT systems and the so-called 'Cloud Recommendation')[11] should be mentioned. Although it is not yet applicable at the time of writing this paper, the DORA Regulation[12] also contains highly important measures for IT security, which are to be applied from 17 January 2025. The above-mentioned legislation regulates in great detail, among others, how the IT systems of payment service providers should look like and the (minimally) required tools of defence of those systems against external and internal attacks. While these provisions ensure only a minimum level of IT security, the IT regulations applicable to the Hungarian financial sector can be considered highly advanced and guarantee the sector's cybersecurity resilience (MNB, 2022).

10 Government Decree No 42/2015 of 12 March 2015 on protecting the information system of financial institutions, insurance undertakings, reinsurance undertakings, investment firms and commodity dealers.

11 Recommendation No 4/2019 of 1 April 2019 of the Magyar Nemzeti Bank on the use of social and public cloud services and Recommendation No 8/2020 of 22 June 2020 of the Magyar Nemzeti Bank on the protection of IT systems.

12 Regulation (EU)2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

For the same reason, it is the clients rather than the IT systems of payment service providers that fraudsters tend to target.

Two legislative changes have been introduced recently specifically to support anti-fraud efficiency in the financial sector. One of those changes is Section 37/A of the Anti-Money Laundering Act[13], in force from 1 August 2024, which establishes a chain of alarm for the notification of payment service providers. This means that if a payment service user falls victim to fraud, their account servicing payment service provider notifies the competent authority and other payment service providers involved in the execution of the payment transaction in a secure manner. The second important legislative change is the addition of provisions for the establishment of a central fraud detection system, among others, to the text of the PSA [Section 55/D]. This legislative package will enter into force on 1 July 2025 and ensures data reporting between GIRO Elszámolásforgalmi Zrt., the financial enterprise operating the Hungarian retail payment system and payment service providers participating in the system for more efficient prevention of fraud in HUF payment transactions within Hungary (GIRO, 2024).

### 3.2.2 The criminal law assessment of phishing in current judicial practice

For a discussion of phishing in a legal context, reference to one of the main branches of public law is inescapable. Namely, the branch of criminal law. As it is practical in the case of most regulations connected to digitalisation, anti-cybercrime legislation has been adopted at multiple levels. International treaties are at the highest level, of which the Convention on Cybercrime adopted on 23 November 2001 (the Budapest Convention) has the most subject-specific importance. The Convention facilitates a comprehensive approach to the assessment of certain acts, including phishing, among the acceding countries (Krasznay, 2021). The legislative acts of the European Union are at the next level, of which the most significant are Directive 2013/40/EU[14] and Directive (EU) 2019/713[15]. Finally, at the national level, the Criminal Code of Hungary[16] is naturally the primary legal source in the matter. As technology evolves and changes constantly, so are the methods and solutions used by criminal actors. It is extremely challenging to

13 Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing.

14 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

15 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

16 Act C of 2012 on the Criminal Code.

keep pace on the regulator's side, especially in regard to the numerous legislative developments in the last few decades. Giving an account of the relevant legal history is beyond the scope of this paper, but the significance of the subject is worthy of mention (Mezei, 2018; 2020).

For a criminal law assessment, phishing as a crime may be considered – based on the applicable legislation – in relation to various offences.

A separate chapter is dedicated to cybercriminal acts in the Criminal Code due to the similarities and close connections between the offences under this category. Section 423 of the Criminal Code specifies violating information systems or data, classified as pure cybercrime, in three separate points having different emphasis. Information systems are the object of the crime under all these points. Within the meaning of Section 423(1), a person who logs into an information system without authorisation by violating or circumventing a technical measure safeguarding that information system or stays logged in exceeding or violating the limits of his authorisation to log in is guilty of a misdemeanour and shall be punished by imprisonment for up to two years. In the first case, the offender is not authorized to access the system, while in the second, they do have the required authorisation, but misuse it, for instance, by way of privilege escalation. Perpetrators of such criminal acts are colloquially known as hackers. It should be highlighted that the target of unauthorised entry to the information system may be the computer used for the criminal offence, but could also be a protected computer network accessible through it, e.g. the online financial services infrastructure used by payment service users. It is a criterion of criminal responsibility that the information system had been protected by technical means, which were also active at the time of the incident. In other words, if a system is protected, e.g. by a firewall or biometric authentication, but these functions are inactive, the suspect cannot be pronounced guilty of the misdemeanour (Belovics, 2023). Section 423(1) also specifies the means by which the criminal act should be committed, i.e. logging into an information system by violating or circumventing a technical measure safeguarding that information system, for example, by exploiting the deficiencies of the security system, or by using the credentials of the authorised user. How those credentials were obtained is irrelevant, while it is exactly at this point that phishing may enter the picture. Furthermore, committing the act to make a profit, cause damage or with a similar purpose (criminal intent) is not a criterion of criminal responsibility, i.e. ideologically or politically motivated attacks are also punishable.

Section 423(2) establishes criminal responsibility if the operation of the information system is hindered or by way of violating the user's authorization limit. Since the primary aim of these provisions is to ensure normal use of the information system (including protection against ransomware and denial-of-service attacks), they are not relevant for phishing. At the same time, another criminal offence

specified in Chapter XLIII of the Criminal Code must be mentioned. According to Section 424(1)(a) and (b), any person who – with the intention to commit the criminal offence defined in Section 375 or 423 – makes, hands over, makes accessible, acquires or places on the market a password or computer program that is necessary for or facilitates the commission of a criminal offence or makes available to another person his economic, technical or organisational knowledge regarding the making of a password or computer program that is necessary for or facilitates the commission of a criminal offence is guilty of a misdemeanour punishable by imprisonment of up to two years. Consequently, creating and distributing different types of so-called 'malware' is regarded in itself as a criminal act (Mezei, 2019).

Upon the codification of the Criminal Code, information system fraud (Section 375) was added as a new criminal act. According to the competent minister's commentary on the draft Criminal Code, information system fraud resulting in damage primarily threatens financial interests, and this type of fraudulent activity was classified separately because it lacks the element of deception in the conventional sense. Accordingly, Section 375(1) of the Criminal Code provides that a person who, for illicit gain, introduces data into or alters, deletes or renders inaccessible any data processed in an information system, or interferes with the functioning of an information system by executing any other operation and causes damage by doing so is guilty of a felony and shall be punished by imprisonment for up to three years (Ambrus, 2021). In addition to the foregoing, within financial fraud, prosecuting criminal acts committed by abusing payment instrument is particularly important. Within the meaning of Section 375(5) of the Criminal Code, any person who causes damage by using or accepting as payment any false, falsified or illegally acquired electronic payment instrument is punishable. Setting aside the intricacies of the related legal dogmatics and implementation, we do not wish to discuss the definition of 'damage' in this paper, as in everyday finance these acts may result in the misappropriation of the full balance held on clients' payment and other (e.g. deposit or securities) accounts, and more recently even in unsolicited loans (Herman 2024). Cash-substitute payment instruments are defined in Section 459(1)(19) of the Criminal Code, as 'non-cash means of payment provided for in the Act on Credit Institutions[17], as well as treasury cards, traveller's checks, credit tokens and bills of exchange made out in accordance with the Personal Income Tax Act, provided they contain protective fixtures, such as coding or signature, against duplication, fraudulent making or forgery, and against unauthorized use.' Based on the provisions of the Act on Credit Institutions [Point 55(a) and (c) under Section 6(1)], the payment instruments used the most frequently by clients

17 Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises

and regarded as such by Magyar Nemzeti Bank as supervisor of the system of financial intermediaries based on the provisions of the Act on Credit Institutions are mobile and online banking applications, payment cards and electronic money (Bárdits, 2021).

In light of the above, though questions may therefore arise in the practical application of the law in relation to the delimitation of the various offences, it can be stated that criminal acts against or committed by abusing information systems are in general punishable and forbidden under the law. That also applies to one of the most frequently used methods, i.e. phishing, regardless of whether damage, or the misuse of payment instruments (e.g. unlawful execution of a payment order using a banking application or a payment card) or personal data [Section 219 of the Criminal Code] have effectively occurred. Based on the foregoing, the conditions to prosecute phishing are provided under criminal law.

## 4 LAW ENFORCEMENT APPROACH TO TACKLING PHISHING

Crime prevention plays a central role in countering phishing, mainly through awareness-raising and security-awareness campaigns (Gyaraki, 2022). In addition to the crime prevention subdivisions of the police, experts of financial awareness, companies and other organisations actively take part in preventive communication efforts (Terták–Kovács, 2023; Kovács–Terták, 2024). Besides conventional channels of awareness raising (e.g. personal, written, in the printed press and television), online presence is particularly important in the fight against phishing, including social media posts and ads, short videos or longer podcasts, or the inclusion of influencers to get the message across, since the potential victims of phishing are exactly those active in the world of online finances. An exemplary campaign for raising security awareness in Hungary is the 'KiberPajzs' (CyberShield) program, a cooperation of participants from various fields (NKI, 2023; KiberPajzs, 2024).

The investigation of successful phishing attempts and related crimes, and the potential recovery of the assets lost is especially challenging because these criminal acts are happening at a much greater speed than the investigative steps. Sometimes a few clicks are enough for victims to unwittingly hand over control over their computers, mobile phones or payment accounts, and for their money to vanish using today's instant payment systems. Cybercriminals often choose Friday evenings or public holidays to debit the payment, savings or securities accounts of the victims, so that they are at a disadvantage in alerting their payment service provider or the authorities. Since these criminal acts are committed in cyberspace, even if the perpetrator can be identified, the investigation process is often difficult

because international cooperation is needed. Criminals are often part of cross-border criminal organisations, may use off-the-shelf infrastructures for phishing and fraud provided as a service, and in the case of vishing, operate call centres very similar to genuine ones (those operated by payment service providers).

Fortunately, 2024 was a successful year in law enforcement, with Europol winding up a phishing-as-a-service platform and the criminal organisation operating it as a result of law enforcement cooperation across 19 countries (Europol, 2024b), while the Hungarian authorities and the Ukrainian police teamed efforts to seize a criminal group targeting Hungarian-speakers and operating a call center (police.hu, 2024). However, it is more common that only lower-level actors of highly organised criminal organisations can be tracked down, i.e. only 'little fish' or money mules commissioned with opening payment accounts for the stolen funds or withdrawing the money.

It is also worth mentioning asset recovery, i.e. the return of stolen money to its rightful owner. In practice, there is a reasonable chance to recover the money only if all stakeholders – the user/victim, the payment service provider and the competent authorities such as the police – act without delay. If the payment service user alerts the account servicing payment service provider of any unauthorised payment transaction or any change in the payment order not requested by them (e.g. early withdrawal of a fixed deposit or modification of communications channel settings) immediately after being notified thereof (e.g. in a text or push message), and the payment service providers involved in the payment transaction and the police cooperate closely and without delay around the clock in halting the movement of the funds, they may succeed in seizing the money and transfering it back to the owner (see the hotline mentioned in section 3.2.1 above).

## 5 IT SECURITY TOOLS FOR PREVENTING AND DETECTING PHISHING

IT security offers various means for tackling phishing, from security awareness training and campaigns to technical solutions. Apart from the crime prevention programs of the police and the KiberPajzs initiative mentioned earlier, the detection and prevention of phishing attempts and their notification to the dedicated entity (the corporate IT security team) is generally covered in corporate internal IT trainings, and some companies may also test the security awareness of employees by phishing simulation exercises. In addition, there are plenty of online educational resources such as the saferinternet.hu site run by the Hungarian division of International Children's Safety Service (NGYSZ) or digipedia.hu operated by the National Media and Infocommunications Authority (NMHH), to mention just a few.

Phishing e-mails can be effectively identified with spam filters and antivirus software, if correctly set up. Spam filters – a default function at bigger, often cloud-based mail service providers and also at most internet providers offering mail services – tend to identify phishing e-mails as spam due to their similarity to unsolicited commercial e-mails in terms of technical features (hidden or spoofed sender address, a high number of recipients, suspicious sender, etc.). Most antivirus software can flag suspicious links in electronic correspondence or in the browser used, warning the user not to click on websites with a phishing potential. In addition, antivirus software can also prevent the running of malicious software used for phishing. Content filtering solutions usually in place in corporate environments also provide a degree of protection. Some internet providers also offer similar internet filter services to consumers.

In electronic correspondence, it is a good practice to attach an electronic signature or stamp to outgoing e-mails, this way authenticating the originating server, enabling the recipient to verify the identity of the sending entity and to detect phishing attempts. Using the Domain-based Message Authentication, Reporting & Conformance (DMARC) protocol is also an effective means of verifying the authenticity of the sender (MNB, 2022). Furthermore, the header of electronic messages also contains additional information that helps decide during the technical evaluation and statistical analysis of messages if they originate from a legitimate, safe environment (Kumar Birthriya–Jain, 2022). In the United States, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) issued a shared counter-phishing guidance, highlighting the importance of using proper multi-factor authentication (so that attackers need more than a user name and the matching password to succeed) in addition to security awareness training, and recommending further technical solutions to prevent phishing (CISA, 2023).

Recent mobile phone models offer anti-phish configurations flagging suspicious messages and unsolicited calls to fend off smishing and vishing attempts. While current legislation in Hungary does not allow telecommunications service providers to similarly flag or screen suspicious communications, the Office of Communications of the United Kingdom (Ofcom) already issued recommendations for this purpose and launched a separate program for reviewing providers' practices (Ofcom, 2024). In Poland, an act on combating fraud in electronic communications was adopted in 2023.[18]

18 Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

There are steps to be taken also against phishing e-mails and text messages already received. We can mark these as spam in our phone or mailing system, block the number (also an option against vishing), or report the phishing attempt through one of the two (NMHH and NGYSZ) internet hotlines available in Hungary, or to the police. Phishing e-mails sent to workplace addresses should be handled in line with the company's internal policy, and should usually be reported to the corporate IT security officer or cybersecurity team. When receiving phishing communications containing a link to a fake website – e.g. mimicking a payment service provider's website – it is a good practice for more experienced IT users – to contact the web hosting provider or domain registrar to remove the content. These sites are often located on cracked servers that host websites offering legitimate services, without the owner or operator being aware of what their server is used for. There are solutions available free of charge for screening suspicious messages, URLs, domains or attachments, such as virustotal.com which utilises more than 70 antivirus software solutions for checking the uploaded content.

All this goes to show that in addition to awareness raising and training, companies and IT and telecommunications service providers have a number of IT security tools at hand to prevent their users and clients from falling victim to phishing.

## 6 PREVENTING AND MITIGATING THE DAMAGE CAUSED BY PHISHING

If the targeted user shares data or installs an application, and damage is done, the payment service provider should be contacted without delay to confirm if any authorised payment transactions have been executed and to take the necessary preventive steps against unsolicited transactions. In practice that means disabling and resetting online and mobile banking access credentials, or blocking the affected payment card and requesting a new one. Importantly, after its immediate blocking, access should only be reactivated once the client/user has made sure to remove unauthorised access to their mobile phone or computer. In case the user has multiple accounts with different payment service providers that may be affected (for instance, due to remote access software installed on the user's PC), these precautionary measures should be taken with respect to all accounts. Similarly, if the user manages also other clients' accounts, or several family members are using the same computer, access to all the potentially affected accounts should

be blocked[19]. A user-friendly summary of the necessary steps is available at the KiberPajzs website (link provided above).

The Anti-fraud Recommendation of MNB referred to in Section 3.1 above outlines detailed proposals for the obligations of payment service providers, which therefore will not be discussed further in this paper. In conclusion, it is possible to mitigate the damage caused by phishing attacks. The actors involved in this process (i.e. payment service providers, law enforcement agencies) are aware of the required steps and make efforts to inform also potential victims of fraud. At the same time, damage mitigation, by definition, cannot be as effective as prevention in avoiding the consequences of phishing.

## 7 SUMMARY

Cyberfraud causes growing losses to the economy that materialise within the system of financial intermediaries. Phishing is one of its most prevalent forms, with phishing attacks accounting for a major share (in Hungary, as high as 70%) of all successful and attempted fraud. Phishing attacks aim at obtaining personal data or credentials for financial services by bulk messaging (e-mail or text), phone calls and psychological manipulation, in order to exploit these data afterwards for financial gain or for further attacks. Criminals have various tools at their disposal to implement phishing attacks, which nowadays can even be sourced from providers specialized in phishing (phishing-as-a-service) (McNee, 2024). As phishing attacks are multifarious, protection against them should be as broad as possible to cover all forms.

The legal assessment of phishing is complicated, as it is relevant for various branches of law. Liability for the damages caused by phishing is of primary concern under private law, especially in the context of financial services, but other types of services may also be affected (e.g. credits and loans). In the case of payment services, providers are subject to especially rigorous liability rules. The applicable EU and national legislation, and current judicial practice impose a form of strict liability on payment service providers for payment transactions executed without the client's authorisation. Exemption from that strict liability towards consumers and microenterprises is only possible if the payment service provider manages to provide evidence for gross negligence or acting fraudulently on the payment service user's part. However, in relationships with payment service users

19 MNB executive circular on preventing fraud linked to electronic access by authorised representatives and stipulations for informing clients of related risks.

other than consumers and microenterprises, the parties may agree to derogate from the provisions of the PSA on the burden of proof. As in private law, public law also contains strict regulations for the protection of information systems and for information system fraud. Under financial law, payment service providers must meet a number of prudential and IT security requirements to ensure the smooth operation of payment systems and the maintenance of trust in the system of financial intermediaries. In practice, these requirements are also effective in preventing phishing.

Phishing may be connected to various punishable acts under criminal law, such as unauthorised access to and interfering with the functioning of information systems, or fraud committed by non-cash means of payment (e.g. mobile or online banking applications, payment cards). It can be established that criminal law provides the necessary means to combat phishing. While the privacy law implications of phishing are obvious, these could be mentioned only briefly in this paper. However, this area of law and the related jurisprudence is well documented in the literature.

Crime prevention, implemented through awareness-raising campaigns and the promotion of security awareness, is a key part of anti-phishing efforts. The investigation of phishing-related criminal offences is challenging, as in many cases, perpetrators act fast and across borders, making the task of law enforcement agencies and international cooperation more difficult. Participants of the system of financial intermediaries, such as payment service providers, the Hungarian Banking Association representing sectoral interests, as well as public bodies and authorities (e.g. MNB or the competent ministry and other authorities) play a central role in the education of the public. In recent years, several initiatives have been launched to raise awareness of cybersecurity and personal finances. PÉNZ7 (Money Week)[20] and KiberPajzs are good examples. The effectiveness of these campaigns is hard to quantify, but in regard to the current value of payment fraud, they apparently have a positive, preventive effect.

IT security training and technical solutions are essential means of proven efficiency for the prevention of phishing. Appropriate spam filters, antivirus software and multi-factor authentication are tools that help mitigate the risks. Recognising and properly reporting phishing messages is another important component of anti-phishing defence, in addition to other tools such as the use of electronic signatures between messaging servers to ensure the authenticity of messages. It cannot be stressed enough that victims of phishing should contact their payment service providers without delay and monitor unauthorised payments to prevent

20 See the website https://www.penz7.hu/.

further unwanted transactions to the extent possible. In the context of online and mobile banking, access should be discontinued and credentials reset, while in the case of payment cards, blocking the card and requesting a new one may also be advisable. Importantly, access should be reactivated only if the security of the mobile phone or computer is ensured.

In light of the above, phishing is a highly complex issue which may be addressed at different levels. To be able to understand and effectively prevent it, we should therefore study its different forms and the techniques used. The legal background should also be examined, with special regard to the uniform IT security provisions under the DORA Regulation, which will be applied across the European Union from January 2025 on. As a general conclusion, phishing may be countered at multiple levels and with diverse tools. While a joint application of legal, crime prevention, security awareness, IT security and law enforcement tools is the most effective defence against phishing, prevention – on both (payment) service providers' and (payment) service users' side – is the surest.

## REFERENCES

Ambrus, I. (2021): Mezei Kitti: A kiberbűnözés aktuális kihívásai a büntetőjogban [Current Challenges of Cybercrime in Criminal Law]. 2020, Budapest: TK JTI–L'Harmattan, 284. Állam-és Jogtudomány 62(4): 128–133. https://doi.org/10.51783/ajt.2021.4.06.

Anderson, R. – Barton, C. – Böhme, R. – Clayton, R. – Gañán, C. – Grasso, T. – Levi, M. – Moore, T. – Vasek, M. (2019): Measuring the Changing Cost of Cybercrime. https://www.repository.cam.ac.uk/items/a9e1b7b4-03c6-43b5-ae0c-b5b59e0d4684.

Bárdits, Z. (2021, 27 February): Bankkártya, üzemenyagkártya, Revolut, Bitcoin - Mi számít elektronikus pénznek? [Bank cards, fuel cards, Revolut, Bitcoin – What qualifies as electronic money?] *portfolio.hu*. https://www.portfolio.hu/bank/20210227/bankkartya-uzemenyagkartya-revolut-bitcoin-mi-szamit-elektronikus-penznek-471486.

Belovics, E. (2023): *Büntetőjog II. (k*ülönös *rész*) [Criminal Law Vol. II. – Special Part]. 9th, updated edition (of September 2023). Budapest: ORAC Kiadó.

CIB Bank (2024, 9 May): Telefonon próbálkoznak a leggyakrabban a kibercsalók [Cyberfraud Comes the Most Frequently Over the Phone]. *CIB Bank Zrt.* https://www.cib.hu/Maganszemelyek/rolunk/sajtoszoba/sajtokozlemenyek/240509-kibercsalas.html [retrieved: 16.06.2024].

CISA (2023, 18 October,): Phishing Guidance: Stopping the Attack Cycle at Phase One. https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one [retrieved: 16.06.2024].

Europol (2023): *IOCTA, internet organised crime threat assessment 2023.* European Union Agency for Law Enforcement Cooperation. LU: Publications Office. https://data.europa.eu/doi/10.2813/587536.

Europol (2024a): *Facing reality?: law enforcement and the challenge of deepfakes : an observatory report from the Europol innovation lab.* LU: Publications Office. https://data.europa.eu/doi/10.2813/158794.

Europol (2024b): International investigation disrupts phishing-as-a-service platform LabHost. https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost.

Europol (2024c): *Internet Organised Crime Threat Assessment (IOCTA) 2024*. European Union Agency for Law Enforcement Cooperation. LU: Publications Office. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

GIRO (2024): Összefogással a biztonságos banki tranzakciókért [Working Together for Ensuring Safe Banking Transactions]. https://www.giro.hu/news/biztonsagos-banki-tranzakciok.

Gyaraki, R. (2022): A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról [The Role of Security Awareness, Questions about Cybersecurity]. *Magyar Rendészet* 22(2): 245–261. https://doi.org/10.32577/mr.2022.2.16.

György V. (2021, 30 March): A csomagküldős vírus itthon is tarolt [The Parcel Delivery Scam Has Swept Across Hungary]. https://index.hu/belfold/2021/03/30/csalas_sms_kibervedelem/ [retrieved: 2024.07.24].

Herman, B. (2024, 18 July): Újabb fontos intézkedést vezetnek be az online banki csalások ellen [Another important measure is introduced against online banking fraud]. bank360.hu. https://bank360.hu/blog/ujabb-fontos-intezkedest-vezetnek-be-az-online-banki-csalasok-ellen.

KiberPajzs (2024): https://kiberpajzs.hu/ [retrieved: 2024.07.25].

Kovács, L. (2010): *Az európai pénz- és elszámolásforgalom jövője* [The Future of the European Payment and Clearing System]. Miskolc: ME GTK.

Kovács L. – Terták E. (2024): Financial Literacy is the Best Protection from Cybercrime. *Economy & Finance* 11(1), 7–28. https://bankszovetseg.hu/Public/gep/007-028%20E%20Kovacs_Tertak.pdf.

Krasznay C. (2021): Húsz év a globális kiberbűnözés elleni küzdelemben: A Budapesti Egyezmény értékelése [Twenty Years of Fighting International Cybercrime – An Assessment of the Budapest Convention]. *Külügyi Szemle*, 20 (Special issue): 191–214. https://doi.org/10.47707/Kulugyi_Szemle.2021.2.09.

Krasznay, C. (ed.). (2023): *Taktikák és stratégiák a kiberhadviselésben* [Cyber Warfare Techniques and Strategies]. Budapest: Ludovika Egyetemi Kiadó.

Kumar Birthriya, S. – Jain, A. K. (2022): A Comprehensive Survey of Phishing Email Detection and Protection Techniques. *Information Security Journal: A Global Perspective* 31(4): 411–440. https://doi.org/10.1080/19393555.2021.1959678.

Lábady, T. (2014): *A magánjog általános tana* [General Private Law]. 2nd ed. Budapest: Szent István Társulat.

Magramo, H. C., Kathleen (2024, 4 February): Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. CNN, https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html [retrieved: 2024.10.17].

McNee, S. M. (2024): How Cybercrime Empires Are Built. *darkreading.com*. https://www.darkreading.com/vulnerabilities-threats/how-cybercrime-empires-are-built [retrieved: 2024.06.16].

Mezei, K. (2018): Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására [International Action Against Cybercrime – Regulation in the European Union and the United States in the Focus]. *JURA*, 24(1): 349–360.

Mezei, K. (2019): A kiberbűnözés szabályozási kihívásai a büntetőjogban [Challenges of the Criminal Law Regulation of Cybercrime]. Ügyészek Lapja, 26(4–5): 21–33.

Mezei K. (2020): A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre [Challenges of Modern Technologies in Criminal Law – Cybercrime in the Focus]. *Állam- és Jogtudomány*, LXI(4), 65–81.

mitre.org (2024): MITRE ATT&CK®. https://attack.mitre.org/ [retrieved: 2024.07.24].

MNB (2022, December): Cyber threat landscape report of the Hungarian financial sector 2022. Magyar Nemzeti Bank. https://www.mnb.hu/letoltes/cyberthreat-landscape-report-2022.pdf.

MNB (2024a, June): Payment Systems Report 2024. Magyar Nemzeti Bank. https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2024-angol-v2.pdf.

MNB (2024b, 17 September): Payment frauds. https://statisztika.mnb.hu/timeseries/data-8827.

Molnár, P. (2021): Comparison of the new Chinese Personal Data Protection Law (PIPL) with GDPR and CCPA. *KRE-DIt*, 2. https://www.kre-dit.hu/tanulmanyok/peter-molnar-comparison-of-the-new-chinese-personal-data-protection-law-pipl-with-gdpr-and-ccpa/ [retrieved: 2024.07.14].

NKI (2023): Mi ellen véd a KiberPajzs? [tudatosan] [What the CyberShield Defends Against? [by awareness]. Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet [National Cyber Security Center of Hungary, Special Service for National Security]. https://kibertamadas.simplecast.com/episodes/mi-ellen-ved-a-kiberpajzs.

Ofcom (2024): Enforcement programme into phone and text scams. *www.ofcom.org.uk*. https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/enforcement-programme-phone-and-text-scams/ [retrieved: 2024.07.26].

Oroszi, E. D. (2020): Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük [Social Engineering in the Context of the COVID-19 Pandemic, or Attack Mechanisms Exploiting the State of Public Emergency and their Prevention]. *Dunakavics*, VIII(V): 5–20.

police.hu (2024): Kozel 90 milliós utalást kart egy álpartnercég [Fake partner company requests a nearly 90 million HUF transfer]. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/kozel-90-millios-utalast-kert-egy.

Szabó, H. (2023): A mistresses intelligencia biztonsági kockázatai eggy új korszak kezdetén [Security Risks of Artificial Intelligence at the Beginning of a New Era]. *Nemzetbiztonsági Szemle,* 11(4), 35–46. https://doi.org/10.32561/nsz.2023.4.3.

Szalai, Á. (2024): *A delectables felelősség joggazdaságtana* [Non-Contractual Liability in the Economics of Law]. ORAC Kiadó. https://doi.org/10.21862/ELTEJKT69.

Terták, E. – Kovács, L. (2023): Financial Security in Cyberspace – PÉNZ7 Thematic Week]. *Economy & Finance* 10(1), 5–19. https://doi.org/10.33908/EF.2023.1.1.

VISA (2023): Visa Payment Fraud Disruption Biannual Threats Report December 2023. Visa. https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/pfd-biannual-threats-report-december-2023.pdf.

World Economic Forum (2024): Global Cybersecurity Outlook 2024. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.