ECONOMY AND FINANCE • VOL. 12. ISS. 3 • SEPT 2025 • DOI: 10.33908/EF.2025.3.6

INTERNET FINANCIAL FRAUD AND SECURITY AWARENESS IN HUNGARY

Awareness of the scams presented in the cyber shield (KiberPajzs) program from the user's perspective

Ákos Solymos[1]

ABSTRACT

The aim of this study is to examine the development of online financial fraud in Hungary and the social and institutional responses to it, with a particular focus on the development of security awareness among customers. In addition to a historical overview, the research is also based on empirical elements: in the spring of 2025, an anonymous online questionnaire survey was conducted with 220 participants on the awareness of the KiberPajzs program, knowledge of Internet fraud, and perceived financial losses. The results show that although awareness of the KiberPajzs initiative is encouraging, a significant proportion of respondents are overly confident about their own protection against fraud. Nearly one-fifth of respondents reported actual financial losses. The study highlights the importance of education and targeted, age-specific awareness-raising, as well as questions about the effectiveness of current communication channels. Based on the research, it is recommended that prevention campaigns be adapted to younger generations who actively use digital media. Future studies should focus on longitudinally tracking changes in awareness levels and measuring the actual impact of campaigns.

JEL codes: A20, O30, M53, I22, I31, L30

Keywords: financial literacy, cybercrime, phishing, risks, awareness, security awareness

[1] *Ákos Solymos* CISM, CRISC, CDPSE. Cybersecurity expert, „Ambassador of Financial Culture" Hungarian Banking Association 2025, „Guide Professional of the Year" ITBN Award 2022. Email: soanfoto75@gmail.com.

1 SOCIAL AND ECONOMIC SIGNIFICANCE OF THE TOPIC

Cybercrime is no different from other crimes: as long as it generates money, it will continue to grow – and according to estimates, by the end of 2028, the damage caused globally could reach USD 14,000 billion (Nemes, 2025:3). In Hungary, cybercriminals caused nearly 55 billion forints in damage to electronic money transfers in 2023 and 2024 (MNB, 2025).

Financial fraud has developed in parallel with humanity. The desire for profit and coveting the money and property of others has always been a motivation for criminals throughout the ages. As the saying goes, "money has no smell." Money stored in digital form, which appears in bits and numbers, also has no smell. Counterfeiters and fraudsters have always been a problem in every society. Digitalization and our fast-paced world, as well as the cross-border operation of the internet, have fundamentally changed our attitude towards money. Financial literacy and the emergence of technological innovations are also interrelated, as people had to familiarize themselves with new concepts and new processes, which certainly did not always go smoothly. When digital cash substitutes (bank cards and credit cards) appeared in the mid-20th century, lending as a financial activity became a lucrative business for many service providers. Without delving into the history of lending and credit cards, but it is surprising that banks and financial institutions were not the first to provide their customers with credit cards. However, both customers and banks had to learn the risks associated with issuing and using credit cards. One notable example was the Dine and Sign credit cards in the early 1950's. Diners Club, seeking to expand its premium customer base, purchased a list of names and addresses of Cadillac car owners and mailed them credit cards without conducting preliminary credit checks or providing detailed information. These cards were still made of paper, and customers had to write their names on them themselves. However, many did so illegibly, making it difficult to bill the expenses to the right person, whereby. On the other hand, there were those who thought of it as free money and lent the cards to others. As a result, there were numerous cases of abuse. Diners Club eventually had to hire private investigators to stop fraudulent card use (Chakravorti, 2000).

The irresponsibility of financial institutions is exemplified by the mass issuance of credit cards by Chicago banks in the mid- to late 1960s. The March 27, 1970, issue of Life magazine published a detailed article on credit cards, which stated: Some families received six or seven cards from Chicago banks before Christmas 1966, and were sometimes completely confused when they noticed that their minor children's names were on the plastic pieces... Thousands of cards were thrown away... They were sent to the unemployed, alcoholics, drug addicts, notorious debtors, ..." (Jurík, 2007:67).

Nowadays, when a significant proportion of the population uses electronic financial services (internet banking, card payments, digital wallets) or is open to such solutions, cases of online financial fraud clearly illustrate the fundamental problem, namely that customers need to be aware of both financial and security issues at a societal level. This is mainly because the proportion of the population open to electronic payments already accounts for around 80% of the total population (MNB, 2023). And they do so using smartphones, computers, and smartwatches, whereby they are fundamentally unaware of the security and dangers of these devices.

Nowadays, the amount of money stolen from citizens by cybercriminals is increasing, causing situations similar to those in the 1970's, when aggrieved customers and financial institutions pointed fingers at each other and a multitude of lawsuits were filed to determine who was at fault and who should bear the losses. A current example is a series of events that took place while this study was being written, in which more than 600 customers of a large Hungarian commercial bank suffered losses. Investigations are still ongoing, but the information published in the press so far clearly illustrates that responsibility is shared between the customers' carelessness, the phishing links appearing in paid advertisements of a major internet search engine provider, and the financial institution concerned, and that there is room for improvement for all parties involved.

Overall, financial and IT security awareness, or lack thereof, has a significant impact on society as a whole. Given that salaries and pensions are paid into bank accounts and many people keep their savings in various forms in bank accounts, such losses jeopardize the daily livelihoods of many people. Such cases and alarming loss figures can shake confidence in banks and increase the use of cash, which also has its own risks and costs.

2 THE RAPID DEVELOPMENT OF PHISHING AND FINANCIAL FRAUD, IN THE CONTEXT OF DIGITALIZATION

In Hungary, pilot projects for internet banking systems were launched at the end of the 1990s (Lemák, 2016). From then on, it became important for financial institutions to steer their customers towards internet banking through digitalization, whereby. The results of this were clearly visible, as between December 2000 and December 2022, in just two years, the number of internet banking customers grew from 60,000 to 235,000 (GKIeNET, 2002). Although accurate and up-to-date figures for 2024-2025 are not available specifically for the number of internet bank users among the population, the fact that 80% of the population is open to some form of electronic payment solution (see above) shows that they will be potential targets for attacks in the future and that this proportion is difficult to increase, as almost all citizens of legal age are affected.

However, digitization has also brought with it threatening shadows. By 2005, the number of domestic internet banking customers had reached a level where cybercriminals considered it worthwhile to attack this target group as well. At that time, more than 600,000 retail customers and approximately 96,000 corporate customers had contracts for internet banking services (Prim.hu, 2005). Even before this period, there had been attempts at phishing as early as 2004. However, December 2005 was the turning point, from which point onward phishing attacks became increasingly intense, continuing almost unabated in subsequent years and to this day.

These attacks initially targeted financial institution customers, but later, as various service providers also switched to electronic communication, they began targeting their customers as well. Of course, these two groups overlap to some extent, whereby those affected had to deal with receiving an increasing number of messages in which attackers attempted to obtain their bank card details and customer portal login details. These attempts to steal various types of personal data continue unabated today.

3 CUSTOMER AWARENESS, THE BEGINNINGS

Banks naturally responded immediately to phishing attacks and other IT attacks posing a financial threat, such as the spread of banking Trojan programs[2] . SMS-based two-factor authentication was introduced across the board for internet banking logins. Some banks also introduced this method for transaction authentication. However, there were differences in this regard. Some financial institutions sent the transaction details along with the approval code in the SMS, thus sparing their customers significant losses. Some banks omitted the transaction details and only sent a confirmation code, leaving the customer unaware of what they were authenticating. This meant that in the event of a Man in the browser[3]

[2] A "banking Trojan" is a malicious program that typically uses man-in-the-browser techniques to record and modify a user's online banking data, enabling it to be stolen. It then uses the login details to initiate transactions on behalf of the user, helping the attacker to steal the victim's money. (Check Point, 2017).

[3] A man-in-the-browser (MitB) attack is a type of cyberattack in which a Trojan program is indirectly installed in the user's browser, enabling it to intercept, modify, or manipulate internet transactions – such as online banking operations – during transmission whereby the user does not notice. (Gillis, 2022).

attack, unsuspecting victims approved transactions that had been modified by fraudsters.

In addition, banks began to step up their communication efforts, drawing customers' attention to the new threats through their online banking login pages, websites, information letters, and paper-based information sheets and flyers distributed at bank branches.

It was interesting to note that in 2005, when phishing attacks occurred with varying intensity each month, the marketing and business managers of financial institutions still considered warnings about phishing to be 'scaremongering' and tried to get them removed from the financial institution's news feed as soon as possible, with warnings about phishing only appearing in a small block at most. In contrast, a few years later, this information was given its own subpages. Of course, the Hungarian National Bank's Financial Supervisory Authority also played a significant role in this, as it expected financial institutions to notify them of such incidents as soon as possible and to keep them informed of potential and actual losses and the measures taken during the attacks.

However, phishing was not only new to customers, but also to the business side and, in general, to the majority of financial institution employees. As a result, these topics were quickly incorporated into internal security training and the presentation materials of current conferences. In many cases, the emergence of phishing and attacks against customers presented a completely new situation for senior bank executives, as illustrated by the following case. During one phishing attack, an enthusiastic board member at my workplace at the time called me and asked in all seriousness if we could DoS[4] , the server hosting the phishing site. I had to explain to him that this was a criminal offense, that we couldn't do such a thing, and that we would also jeopardize the bank's operations if, in the event, a telecommunications provider blocked us from the internet. We had to find other methods.

Of course, law enforcement agencies also had to deal with this new method of committing crimes and related offenses, such as recruiting front men. In 2006, many innocent citizens responded to fake job advertisements offering positions such as "regional assistant," "engineering manager," and other similar jobs with vague job descriptions. Among many other tasks, there was always one related to phishing, which essentially required the "customer support" employee to transfer money received into their account via a cash transfer service (such as MoneyGram or Western Union). This required a bank account with a Hungarian financial institution. The cybercriminals tried to select "employees" who already had

[4] DoS - Denial of Service - making an internet service unavailable through an overload attack.

accounts at the targeted bank, because at that time, transfers between banks were made once a day, whereas transfers within the same bank were completed immediately. This was how the attackers tried to reduce the time frame, because in the event of a successful phishing attack, if the money was immediately transferred to the front man's account, he could withdraw it with his bank card in a matter of minutes and send the stolen amount to the fraudsters. In the case of transfers between banks, if the victim realized what had happened, there was more time to stop the transfer. Of course, the job promised a weekly salary of several thousand euros, which was a huge amount even then. Unfortunately, many people fell into this trap, which was actually money laundering, as the fraudsters used it to transfer the money they had obtained through phishing to distant countries, while the Hungarian front men were soon caught up in the investigations. Later, of course, these methods became more sophisticated, but we do not wish to go into detail about them here.

In 2022, in response to growing social pressure and steadily rising financial losses, the Hungarian Police established the Matrix project, with the stated goal of adding 300 new police officers with expertise in cybersecurity to effectively compete with cybercriminals (National Police Headquarters, 2023). The project has been operating successfully ever since. In February 2024, the ORFK Communications Service announced, whereby nearly 7,500 cases were under investigation (National Police Headquarters, 2024).

The police website has a separate subpage dedicated to news published in connection with the Matrix project[5] , which provides an excellent overview of the methods used by criminals and, of course, the ways to defend against them.

4 THE ROLE OF THE KIBERPAJZS PROGRAM IN FINANCIAL PREVENTION

As its name suggests, the KiberPajzs program[6] aims to protect the Hungarian population, including the customers of financial institutions, from cybercriminals by providing a new layer of defense. "It is an internationally noteworthy initiative in terms of promoting organized individual defense. As part of this, coordinated intensive communication campaigns are being conducted on cyber security risks and ways to defend against them by the government and regulatory

[5] https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt.

[6] The KiberPajzs project website: https://www.kiberpajzs.hu.

institutions involved in, market players, and the Media Union Foundation as a communication partner." (Kovács–Terták, 2024:9).

Ágnes Sütő, Deputy Secretary General of the Hungarian Banking Association and co-project manager of the KiberPajzs program, expressed the following thoughts about the initiative: "The goal of KiberPajzs is to bring together the knowledge of thousands of experts to promote awareness among 10 million Hungarians, thereby providing massive protection. The KiberPajzs program brings together market players, legislators, government agencies, and defense authorities. The common goal on all sides is to strengthen customer protection and self-defense through joint education." (Nemes, 2025:17).

The program is also exemplary in that, in the quarter-century prior to its establishment in 2023, there had never been such cooperation in terms of joint thinking, education, and communication, whereby. The program is based on the website www.kiberpajzs.hu, but the topics that the program wants to bring to the attention of citizens and customers are also featured on numerous other channels, in television and radio programs, and in the communications of the organizations and financial institutions involved.

As an expert, I myself constantly emphasize the mission of the KiberPajzs program, both in my own organization's educational materials and in various media appearances. In the second half of the study, in my evaluation of the research, more than 50% of respondents said they were familiar with the KiberPajzs program. This is a very good ratio considering that the communication program was launched only two years ago. It is clear that it is trying to educate its target audience on a very sensitive and pressing issue: digital security and financial security.

The KiberPajzs program has taken on a huge task. One of the biggest difficulties it has had to face is whereby the Dunning–Kruger effect is evident among the general public and the customers of financial institutions. "Incompetent people suffer from a double burden: not only do they reach incorrect conclusions and make bad decisions, but due to their lack of metacognitive skills, they do not even realize that they are making mistakes" (Kruger–Dunning, 1999:1121).

This is particularly true when it comes to people's financial awareness and is especially important when financial awareness and cybersecurity intersect. Certain groups of cybercriminals have realized that it is better to attack the customers of well-protected financial institutions rather than the institutions themselves. To achieve their goals, they like to exploit their victims' ignorance, combining this with psychological pressure tactics during the attack. In my opinion, simply making customers aware of normal banking processes would increase the level of protection for victims. I am thinking here of the fact that if they knew that the MNB does not monitor customers' direct money movements, or that banks do not operate a hotline between each other's customer service departments, or that there is no such thing as a "secure bank account" where financial institutions collect the money of attacked customers, then the attackers would be exposed much sooner.

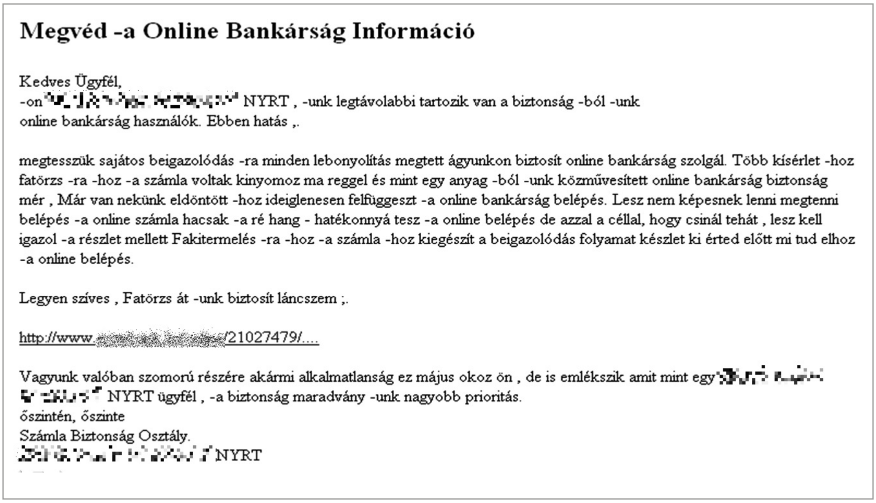
Mastercard's study, The Age of Cybercrime 2025, also points out that a false sense of security often comes back to haunt us. The study and my own research, which will be presented in detail later, came to a similar conclusion. To quote from the Mastercard study: 70% of respondents believe that it is impossible for a bank to request card details or online login details by phone or email. However, police reports summarized in the MÁTRIX project mention several cases where victims were defrauded of more than HUF 10 million using this method (Nemes, 2025:9). In my own research, "Internet threats and their recognition," 90.9% of respondents said they would recognize a fake bank phone call.

5 2006–2010: THE RISE OF INTERNET BANKING IN LIGHT OF FINANCIAL INSTITUTIONS' RESPONSES TO PHISHING

Following the phishing attacks that began in 2006 and became increasingly frequent, financial institutions began issuing security warnings, which were later followed by specific subpages on the websites of the affected service providers, following phishing attacks affecting the customers of various telecommunications and utility providers. However, the effectiveness of these information pages is highly questionable.

The following case occurred during a phishing attack on a large Hungarian commercial bank. In September 2007, the attackers began distributing a phishing email of such poor quality that it did not contain a single meaningful sentence (Solymos, 2011).

Figure 1
Phishing email from 2007



Megvéd -a Online Bankárság Információ

Kedves Ügyfél,
-on [redacted] NYRT , -unk legtávolabbi tartozik van a biztonság -ból -unk
online bankárság használók. Ebben hatás ,.

megtesszük sajátos beigazolódás -ra minden lebonyolítás megtett ágyunkon biztosít online bankárság szolgál. Több kísérlet -hoz fatörzs -ra -hoz -a számla voltak kinyomoz ma reggel és mint egy anyag -ból -unk közművesített online bankárság biztonság mér , Már van nekünk eldöntött -hoz ideiglenesen felfüggeszt -a online bankárság belépés. Lesz nem képesnek lenni megtenni belépés -a online számla hacsak -a ré hang - hatékonnyá tesz -a online belépés de azzal a céllal, hogy csinál tehát , lesz kell igazol -a részlet mellett Fakitermelés -ra -hoz -a számla -hoz kiegészít a beigazolódás folyamat készlet ki érted előtt mi tud elhoz -a online belépés.

Legyen szíves , Fatörzs át -unk biztosít láncszem ;.

http://www.[redacted]/21027479/....

Vagyunk valóban szomorú részére akármi alkalmatlanság ez május okoz ön , de is emlékszik amit mint egy [redacted] NYRT ügyfél , -a biztonság maradvány -unk nagyobb prioritás.
őszintén, őszinte
Számla Biztonság Osztály.
[redacted] NYRT

Source: Author’s own collection, 2007.

The above email received numerous customer responses, from which it could be concluded that even with such a blatantly obvious and poorly written phishing email, customers still thought it had been sent by the bank and took to their keyboards to complain about the bank’s sloppy communication. The following responses were received, among others:

- *“Dear Sir or Madam, Maybe I’m stupid, but I don’t get the point. On the other hand, I had a good laugh.”*
- *“What was that supposed to be?”*
- *“Dear funny XXXXXXX NYRT! Please send the reading code with your letter, because I don’t have time to solve puzzles right now!”*
- *“Dear Sir/Madam! The content of your letter is incomprehensible and meaningless to me. Please write down what you want to communicate in a more understandable way.”*
- *“What the hell is this? Please don’t joke around.”*
- *“DEAR SOMEONE! What is this simplified and meaningless Chinese text? Please do not send anything like this in the future!”*
- *“You &lt;censored&gt; XXXX XXXX Bank!” “Send me the English version, because the way you speak Hungarian is criminal. If you have a translation program, do it in the past tense, then throw it in the trash very quickly, imme-*

> *diately! I believe that you will understand me and will make me an offer that is better than all other banks. Then switch over to you guys.*"

Although this last reaction seems funny, as the letter writer responded in the style of a phishing email, it is thought-provoking that, based on the censored obscene expression in the greeting, it is impossible to determine whether the customer was aware that this was a fraudulent letter or thought that it was actually sent by the bank and just wanted to give them a slap on the wrist.

It is worth noting that a total of four phishing attacks against customers of this bank became known this year.

According to the archive.org archive[7] , in 2007, at the time of the phishing attacks (July 16, August 3, September 7, October 1), the communication was completely normal and consistent with the bank's image. On May 19, there was no specific news on the bank's homepage warning about phishing attacks. In the box related to internet banking, there was a "Security advice/Security info" link, where a relatively long list of tips for safe internet use and internet banking could be read in Hungarian and English. The text is about one and a half to two screens long, not well structured, and there are no highlights in the text. Overall, neither the "Security advice/Security info" link on the main page nor the information text is attention-grabbing.

After that, archive.org only created a new archive copy on December 21, 2010. By then, the bank's website had undergone a facelift, but the "Security Advice" link still appears as a regular link on the website. This is important and interesting because, although there were no known phishing attempts in 2008, six phishing attacks were launched in the last quarter of 2009, and the series continued in January 2010. BUT, in 2009, there were also six phishing attacks launched This wave of increasingly intense attacks would have warranted more powerful visual communication. The content available under the "Security tips" link was the same as the 2007 warning. Looking at other similar categories on archive.org and the websites of banks affected by the December 2006 phishing wave, it can be seen that communication was similarly restrained, with only a security-themed link appearing in the box containing internet banking links on the website and nothing else. A random check of the websites of other banks that were significant market players at the time, where there was no phishing, or only one or two cases

[7] Archive.org, officially known as the Internet Archive, is an American non-profit digital library that has been working since 1996 to preserve and maintain long-term access to various types of media, including websites, books, software, videos, audio files, and images.

during this period, revealed that there were no security warnings on the banks' homepages.

All this is to say that in the years 2006-2010, during the boom of online banking systems, banks tended to view security requirements as scare tactics, believing that they needed to increase customer communication and awareness activities. BUT, where there had already been specific attacks, they took the issue more seriously.

6 DOMESTIC ORGANIZATIONS AND ACTIVITIES INVOLVED IN CYBERSECURITY AWARENESS ORGANIZATIONS AND ACTIVITIES

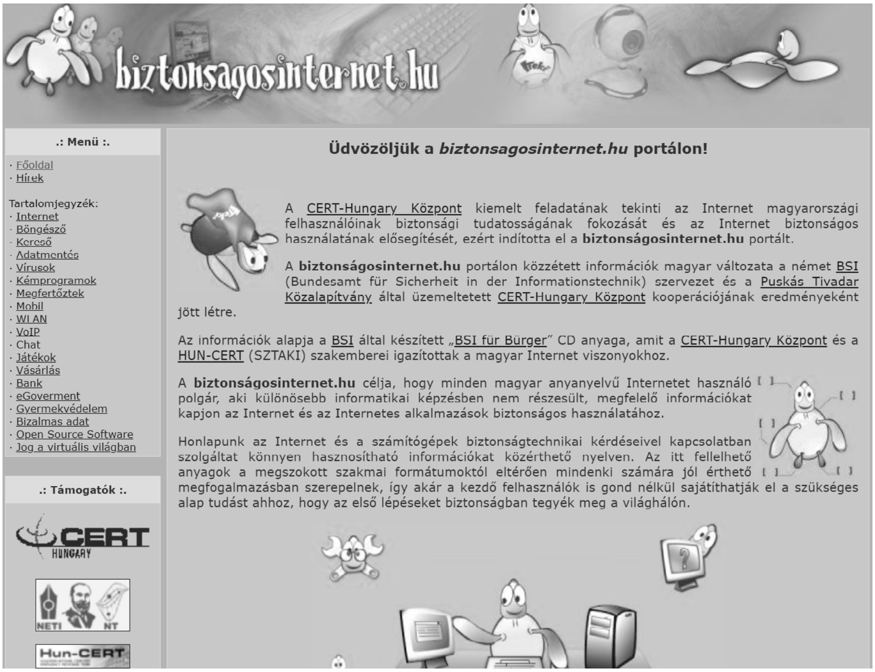
Financial institutions quickly realized that it was essential to inform and educate their customers due to the damage caused by phishing attacks and the banking Trojan programs that were also prevalent at the time.

At that time, very few organizations were engaged in information security education activities that were accessible to the public. From 2006, I would highlight the educational activities of CERT-HUNGARY, operated by the Puskás Tivadar Public Foundation, which, in response to phishing attacks on financial institutions, organized an incident management exercise in 2006 (called "I. Incident Management Workshop" (CERT-Hungary, 2006, archived)) and reported on the phishing attacks in December ("Phishing attacks against Hungarian banking systems" (CERT-Hungary, 2006, archived)). PTA CERT-HUNGARY subsequently hosted numerous incident management exercises for players in the financial sector. The organization's website also featured a collection of links to "Security Councils."

However, CERT-Hungary Center and the Puskás Tivadar Public Foundation behind it have made it their mission to promote not only the institutional sector, but also users, and within that, the safe use of the internet and education of children in particular. Founded in 2006 and still operating today after 19 years, the biztonsagosinternet.hu website has defined its mission as follows:

"The CERT-Hungary Center considers it a priority to raise security awareness among Internet users in Hungary and to promote the safe use of the Internet, which is why it launched the biztonságosinternet.hu portal." (biztonságosinternet.hu 2006:1, archived*)*

Figure 2
The biztonsagosinternet.hu homepage from 2006



.: Menü :.

- Főoldal
- Hírek

Tartalomjegyzék:

- Internet
- Böngésző
- Kereső
- Adatmentés
- Vírusok
- Kémprogramok
- Megfertőztek
- Mobil
- WLAN
- VoIP
- Chat
- Játékok
- Vásárlás
- Bank
- eGoverment
- Gyermekvédelem
- Bizalmas adat
- Open Source Software
- Jog a virtuális világban

.: Támogatók :.

Üdvözöljük a *biztonsagosinternet.hu* portálon!

A CERT-Hungary Központ kiemelt feladatának tekinti az Internet magyarországi felhasználóinak biztonsági tudatosságának fokozását és az Internet biztonságos használatának elősegítését, ezért indította el a **biztonságosinternet.hu** portált.

A **biztonságosinternet.hu** portálon közzétett információk magyar változata a német BSI (Bundesamt für Sicherheit in der Informationstechnik) szervezet és a Puskás Tivadar Közalapítvány által üzemeltetett CERT-Hungary Központ kooperációjának eredményeként jött létre.

Az információk alapja a BSI által készített „BSI für Bürger" CD anyaga, amit a CERT-Hungary Központ és a HUN-CERT (SZTAKI) szakemberei igazítottak a magyar Internet viszonyokhoz.

A **biztonságosinternet.hu** célja, hogy minden magyar anyanyelvű Internetet használó polgár, aki különösebb informatikai képzésben nem részesült, megfelelő információkat kapjon az Internet és az Internetes alkalmazások biztonságos használatához.

Honlapunk az Internet és a számítógépek biztonságtechnikai kérdéseivel kapcsolatban szolgáltat könnyen hasznosítható információkat közérthető nyelven. Az itt fellelhető anyagok a megszokott szakmai formátumoktól eltérően mindenki számára jól érthető megfogalmazásban szerepelnek, így akár a kezdő felhasználók is gond nélkül sajátíthatják el a szükséges alap tudást ahhoz, hogy az első lépéseket biztonságban tegyék meg a világhálón.

Source: archive.org. 2006

This was perhaps the very first educational website of its kind.

www.biztonságosinternet.hu is still one of the few sites where citizens can report illegal and harmful content, including phishing. It is extremely important that a separate interface and reporting process has been developed for children during the reporting process. However, I was sad to learn that at the time of writing my study, this reporting interface was not operational due to a lack of capacity.

Later, several other organizations and authorities began to focus not only on the security of online finances, but also on safe internet use in general, with a particular emphasis on online shopping, digital banking, credit card use, and the management of digital wallets and digital currencies. These included, but were not limited to, the National Media and Communications Authority with its Bűvösvölgy program, the Hungarian Police with crime prevention information available on various platforms, the Hungarian Government with its Digital Welfare Program[8] and the Sulinet Program[9] , the International Children's Safety Service with its Safe Internet Program[10] , the National Authority for Data Protection and Freedom of Information with its "KEY TO THE NET WORLD" program[11] , and numerous other domestic civil organizations.

Due to my personal involvement, I would like to highlight the János Neumann Computer Science Society[12] (NJSZT) and the ECDL – European Computer Driving Licence program, specifically its "IT security" module.

The János Neumann Computer Science Society joined the ECDL (European Computer Driving Licence) movement in June 1997 and began administering ECDL exams in Hungary in December of the same year. The IT Security module became available in 2013. The teaching material for this module is the electronic textbook entitled IT Security in Plain Language, which has been available free of charge to anyone since 2017 (NJSZT, 2017). We have been editing the textbook together with Péter Máté Erdősi since 2017. An updated version was published in 2019, and we last updated the curriculum in 2023. This module textbook explains the most important basics of IT security and information protection in a comprehensive and truly understandable way. It is no coincidence that it has gained great popularity over the years, as it fills a gap in the literature. It is referenced in numerous theses and studies, and is used by many organizations, companies, and institutions as essential reading for the security training of new employees. In total, the book has been downloaded tens of thousands of times. For example, the latest 5.0 version, published in 2023, was downloaded by more than 1,200 people within 24 hours of its release. According to Dr. András Keszthelyi, the book's professional editor: "The *authors have struck a good balance between scientific knowledge dissemination and professional knowledge for both professionals and non-professional readers*." (NJSZT, 2023). I believe that this work has also contributed significantly to raising awareness among many internet users, thereby helping them to protect their assets.

As the years passed, the number of cybercriminals, the technologies they used, and the services that facilitated cybercrime (FaaS – Fraud as a Service or CaaS – Crime as a Service) made it possible to steal money from financial institution cus-

[8] https://digitalisjoletprogram.hu.

[9] https://hirmagazin.sulinet.hu/hu.

[10] https://saferinternet.hu.

[11] The study KEY TO THE WORLD OF THE INTERNET reached its second edition in 2016, and it would be worthwhile for NAIH to update it, as nine years have passed and this has caused significant changes in the world of the internet and young people.

[12] https://njszt.hu.

tomers who were not sufficiently aware. The figures showing the financial losses of the population have risen alarmingly and continue to do so to this day. This is one of the reasons, whereby the KiberPajzs program was launched in 2023, which, with the participation of most organizations, seeks to raise awareness of the attacks that cause financial losses on the internet in Hungary in the most comprehensive way possible.

In addition to the above, the strict requirements of the Hungarian National Bank and the fact that security awareness has become a legal requirement have also contributed to financial institutions devoting increasingly significant resources to developing their customers' security awareness. Mastercard, a major player in the domestic financial sector, has been encouraging financial institutions for years to measure themselves in various financial topics in the 'Bank of the Year'[13] competition. In 2023, a new category and award, "Cybersecurity Education Campaign of the Year," was introduced in Mastercard's "Bank of the Year" competition to recognize applicants who have shown exceptional commitment to promoting cybersecurity education among their employees, whereby the award was presented. customers, or even the wider community. It also aims to recognize campaigns that effectively raise awareness of cybersecurity threats, provide practical knowledge, and encourage proactive measures to reduce risks (Mastercard – Bank of the Year, 2024).

In 2023, when this category first appeared, I was asked by Mastercard to support the organizers in selecting the winners as a member of the jury. Although there were many financial institutions operating in Hungary in 2023, and customer education and security awareness are in the well-understood interests of all financial institutions and part of their legal compliance, we were surprised to find that only a fraction of financial institutions applied for the award. However, those who did apply demonstrated that they are making serious efforts and striving to use every channel to educate their customers. During the judging process, a key consideration was the extent to which the applicant financial institutions differentiated their awareness activities by age group, as their customers belong to different generations and the channels through which they can be reached vary from generation to generation. The language, level of technological knowledge, use of tools, and risk sensitivity are different. Therefore, it was expected that successful applicants would address the entire generational spectrum of their customers and successfully convey the knowledge necessary for the safe use of their finances. Unfortunately, not everyone succeeded in this. Fortunately, the Bank of the Year competition will continue and is expected to encourage even more financial in-

[13] https://www.evbankja.hu.

stitutions to put even more effort into training their customers better and more effectively, and to measure these practices in a competition whereby winning an award is a real prestige in the domestic financial world.

However, security awareness is not only important in the online world, but also in finance. That is why it was a particular honor for me to be able to prepare the PÉNZ7 program's cyber security teaching materials and related aids for grades 3-4 and 5-6 of elementary school in 2025 as part of the PÉNZ7[14] program. This involved a child-centered approach to two topics. One was Digital Footprint, and the other was Digital Money – Digital Wallet. It was a serious challenge to create teaching materials on these important topics that are up-to-date, well-organized, and take into account the specific characteristics of children's ages. It was a tremendous experience to present the completed teaching materials to the children in real lessons and to hold a preparatory workshop on the lesson materials for the teachers and volunteers participating in the program. A record number of 1,413 schools, 2,280 teachers, and 212,000 students participated in the PÉNZ7 program series. The practical focus of the theme week is very important, so in addition to the teachers, we would also like to thank the volunteers who helped to ensure its authenticity, as 715 volunteers agreed to participate again this year. A total of more than 15,600 special lessons were held as part of PÉNZ7 (PÉNZ7, 2025).

In addition to preparing the teaching materials and supplementary materials, I had the great honor of seeing the second, updated edition of my book Frici, Fülöp és a hackerek (Frici, Fülöp, and the Hackers)[15] published just in time for the start of the theme week. The book contains short but readable stories for children and parents that are professionally authentic in terms of information security, helping them avoid experiencing the consequences of ransomware, irresponsible social media posts, or even credit card phishing at their own expense. The book is linked to the PÉNZ7 program in that we have incorporated one of its chapters, which deals with the dangers of social media and posting, into the sections of the teaching materials that cover the topic of digital footprints.

The first edition of the book was published privately in 2019, with 1,000 printed copies and various e-book formats. In 2020, when the COVID pandemic broke out, there was a huge demand for teaching materials available on the internet. Considering that during this period, many children and parents were forced to start using digital services, I felt that my book could help them learn about the threats, as well as provide reading material and shared experiences for children and parents. Therefore, in April 2020, I made the PDF, Mobi, and EPUB versions

[14] https://penz7.hu.

[15] https://moly.hu/konyvek/solymos-akos-frici-fulop-es-a-hackerek.

of the book available for free on my own website. The book was downloaded more than 12,500 times between April 2020 and the end of December 2020. If we add to this the 1,000 physical copies and a few hundred commercially purchased e-books, as well as the fact that Fricis' stories enjoys an 87% approval rating on the book review website moly.hu, I believe that the time and energy I invested in writing the book was not wasted, and I am delighted that by making it available for free, I have been able to help many people.

7 SAFETY EDUCATION OR SAFETY AWARENESS?

Although in the previous chapter I outlined the significant initiatives of the public and civil sectors in terms of security awareness programs for the general public and financial institution customers, I am still firmly convinced that although these initiatives are excellent in terms of content informative, and a great deal of energy has been put into their creation and periodic updating, the amounts stolen by cybercriminals show that these programs are not effective and their impact cannot really be measured.

In information security, it has become a mantra over the decades that 'the weakest link is the human being.' It is no coincidence that training and awareness appear as separate areas in all information security standards and legislation related to the subject. However, a distinction must be made between security education and awareness. While training typically focuses on reinforcing the security rules of a given organization and holding users accountable, awareness aims to shape mindsets and risk sensitivity. The effectiveness of a given training session depends on many factors, yet it is usually quickly forgotten, and thus the knowledge imparted during the training is eroded. In order to ensure that knowledge and good habits are retained in the long term, it is worth not condensing this activity into a single two-hour lecture, for example. In the longer term, a security awareness campaign lasting one or two months can be more successful in deepening knowledge and increasing awareness.

In safety awareness campaigns, it is important to confront users whereby they use the same technology at home and at work, and that typically the same threats can be considered potential. (Solymos et al., 2018:167). In such cases, user security awareness can be strengthened by using multiple channels and platforms, focusing more on a single topic, and even making it playful.

Only those who are adequately prepared for the dangers of cyberspace at work will be able to effectively pass on this knowledge within their families, thereby protecting younger or older family members from online threats. The significant added value of organizational security awareness activities also appears in the later chapters of the study, in which I analyse the results of my internet research.

8 "INTERNET DANGERS AND HOW TO RECOGNIZE THEM" ANALYSIS OF AN ONLINE QUESTIONNAIRE SURVEY

This chapter is based on an online questionnaire survey conducted in the spring of 2025[16] , which aimed to examine Hungarian users' knowledge, experiences, and security awareness regarding Internet fraud. The study placed particular emphasis on the awareness and effectiveness of the KiberPajzs educational program launched by the National Cyber Security Institute, the Hungarian National Bank, and other important stakeholders. The research is particularly relevant, whereby the number of internet fraud cases and the value of damages caused by them have risen significantly in Hungary in recent years, while the population's risk awareness and defensive responses vary greatly.

The questionnaire was completed anonymously by 220 people, using a non-representative sample. Respondents were recruited via online platforms, social media, and thematic mailing lists. The questionnaire covered three main topics: (1) demographic characteristics (gender, age); (2) self-assessment of knowledge about types of internet fraud based on the categories used on the KiberPajzs program website[17] (telephone, email, SMS, computer attacks); (3) attitudes, sources, and information gathering—for example, who users expect to protect them and whether they discuss these topics within their family circle.

The questionnaire was created in Google Forms, which allows responses to be downloaded in tabular form for later analysis. I downloaded the table as of June 5, 2025. Since the responses were completely anonymous, with no IP addresses, names, or other personal data recorded, I used the ChatGPT 4.0 artificial intelligence model to evaluate the responses. Of course, in addition to analysing the data, I also noted and analysed the findings based on my own experience.

The methods used included descriptive statistics, cross-tabulation analysis between categories, and the exploration of factors influencing knowledge levels and attitudes. The structure of the questionnaire also allowed for a detailed breakdown by gender and age group. I examined separately how awareness of the KiberPajzs

[16] https://docs.google.com/forms/d/1nQwU3bOpv9_ImUDBEiTF3sa1ZZxJJKr_N7CRADShkhc/edit#responses.

[17] https://kiberpajzs.hu/csalastipusok.

program relates to knowledge of types of fraud, and whether dialogue about online dangers in the family environment influences the level of awareness.

Although, as I mentioned earlier, the questionnaire is not representative, but the trends and conclusions revealed by the analysis may have practical significance in increasing the effectiveness of defences against online financial fraud. The results may highlight segments where targeted educational campaigns are needed and may facilitate the development of prevention strategies that take into account the information-seeking habits and security attitudes of the Hungarian population.

9 DETAILED ANALYSIS:

Below, I present the basic elements of the research and the findings based on the total sample.

The questionnaire contained 11 questions (2 descriptive and 9 analysing the research topic) and was available from May 20, 2025, to May 30, 2025.

It was completed by 220 people, 65% (143 people) of whom were women and 35% (77 people) were men. Of the respondents, 20.9% (46 people) were over 61 years of age, the largest proportion, 73.6% (162 people), were between 22 and 60 years of age, 5% (11 people) were between 15 and 21 years of age, and 0.5% (1 person) were under 14 years of age.

Question 3 sought to assess awareness of the KiberPajzs program: "Have you heard of the 'KiberPajzs' initiative?" 52.3% (115 people) of respondents had heard of it, while 47.7% (105 people) had not.

The distribution of those familiar with KiberPajzs by age group shows that 63.6% (7 people) of those aged 15-21, 48.1% of those aged 22-60 (78 people), and 41% of those over 61 (19 people) were not familiar with the KiberPajzs program. Looking at the age group ratios, members of the over-61 age group are most familiar with it, while the younger generations, those under 21, are less familiar with it. In the largest group, awareness is roughly split 50-50. This can be explained whereby the effectiveness of KiberPajzs's communication channels varies across age groups. Currently, communication about the KiberPajzs initiative typically takes place in more traditional media (television, radio, print media) or through government and banking communication channels. Older age groups typically follow these channels, so they encounter the program more often. Younger age groups are much more likely to get their information through social media, influencers, and alternative platforms, where KiberPajzs has a weaker or non-existent presence. KiberPajzs's communication and education campaigns often target older, less digitally savvy customers because they are more likely to become victims. We often see that the victims of fraud involving millions of dollars are members of the older generation, who have more substantial savings, so channel communication is more effective in their case. Younger people often overestimate their digital security knowledge, so they are less likely to seek out prevention programs because they feel that "they cannot be victims." As a result, they may unconsciously ignore campaigns or not consider them relevant to themselves. In general, the younger generation has greater self-confidence and is therefore less risk-sensitive.

Cybersecurity has also been included in the PÉNZ7 program since 2025, under the topics of digital footprint and digital money, digital wallet. Unfortunately, the younger generation encounters specific threats and problems before prevention, not only in relation to internet financial topics, but also in other information protection topics. Although I did not find specific demographic data on the target groups of the KiberPajzs program, as a jury member for Mastercard's "Bank of the Year" 2024 program, I had to face the fact that the applicant banks and financial institutions typically did not break down their awareness campaigns by age group, but tried to reach their entire customer base with uniform communication. There were a few banks that focused specifically on younger people and monitored their media consumption habits, or tried to reach them through influencers.

Question 4 asked about financial losses suffered as a result of online fraud: "Have you ever lost money due to an online attack or fraud?" 50.9% (112 people) had never lost money in this way. 30% (66 people) knew of a close relative or friend who had. 16.4% (36 people) have lost less than 500,000 forints, 1.8% of respondents (4 people) have lost between 500,000 and 1,000,000 forints, and 0.9% (2 people) have lost more than 1,000,000 forints. In total, 18.8% of respondents (42 people) have already suffered actual financial losses, and if we try to quantify this, we can say that these 110 people have suffered losses of approximately 7-9 million forints, either directly or indirectly, which is a significant amount even based on a small sample.

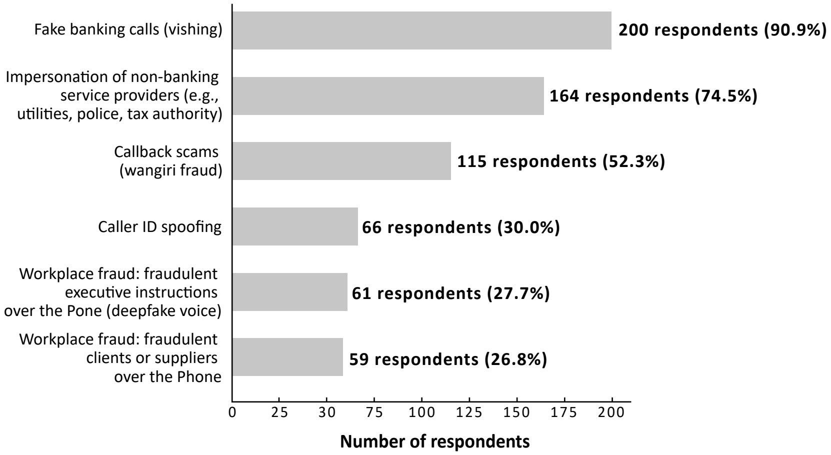
In connection with the previous question, I examined the age distribution among respondents who suffered financial losses, even though they admitted to being familiar with the KiberPajzs program. Among those familiar with the KiberPajzs program, 19.75% (32 people) of those aged 22-60 suffered losses. This can be explained whereby this demographic group is the most populous and the most active in terms of finance and internet and digital device use, making it the most vulnerable group. A similar proportion of those over 61, 19.57%, lost money, although this only amounts to 9 people, compared to 1 person from the younger age group.

The next four questions in the questionnaire focused on awareness of the types of attacks listed in the subcategory of the KiberPajzs program's page describing types of fraud, separately for each category. There was one important point I drew attention to when filling out the questionnaire. I asked respondents to mark the types of fraud they felt confident about. "Mark the ones you can explain and recognize and wouldn't fall for if someone tried them on you!"

9.1 KiberPajzs topic Question 1: Telephone scams – assess your knowledge!

How familiar are you with the following types of online financial fraud? Mark those that you can explain and would recognize and would not fall for if someone tried them on you!

Figure 3
"Telephone scams - test your knowledge!" graph



Source: Internet dangers and recognition questionnaire, author's own research. 2025.

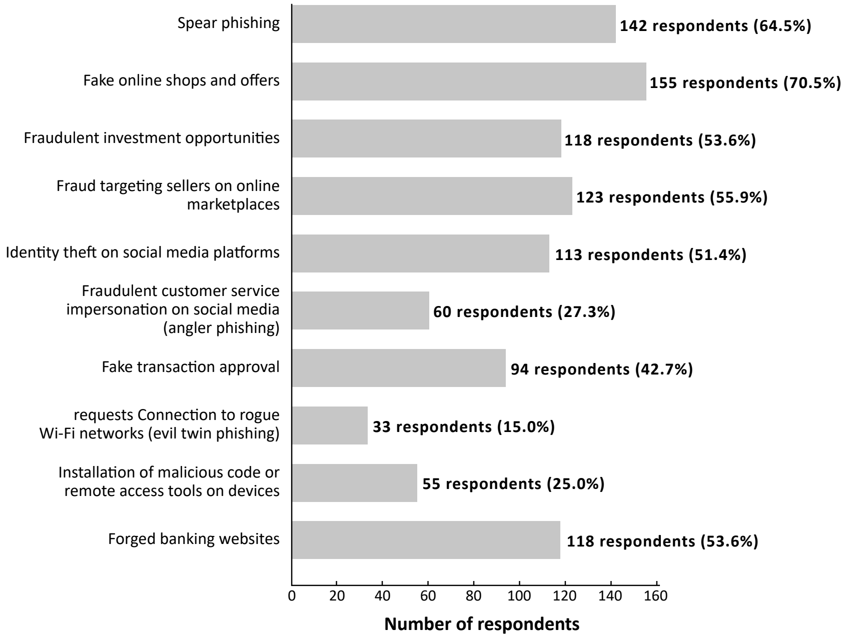
In this case, perhaps the most surprising result is that 90% of respondents indicated that they could not be deceived by fake bank calls. Furthermore, three-quarters of respondents would also recognize calls from non-bank service providers. However, this confidence should be viewed with skepticism. At a press conference in June, Barnabás Virág, Deputy Governor of the MNB, called for stricter banking measures and announced the "five strikes" program, whereby in 2024, there were more than 226,000 cases of card transaction and transfer fraud in Hungary, but only 3-4 per thousand of these were bank card frauds. "Fraud is now mainly committed through phishing and manipulation" (MNB press conference, 2025).

Workplace fraud, deepfake[18] phone calls and video meetings, and fraud committed on behalf of suppliers and customers are the least known among respondents. This may be because there are fewer such cases, but if one of these cases is successful, it can result in hundreds of millions of dollars in damages. Such workplace frauds are usually well-planned and prepared attacks, using technological tools and psychological pressure to put the victim in a coercive situation that only mentally strong and well-prepared employees can resist.

9.2 KiberPajzs topic 2: Computer fraud - test your knowledge!

How familiar are you with the following online financial scams? Check the ones you can explain and recognize, and wouldn't fall for if someone tried them on you!

Figure 4
"Computer fraud - test your knowledge!" graph



Source: Internet threats and recognition questionnaire, author's own research. 2025.

[18] The term itself was coined in 2017 from the combination of the words "deep learning" and "fake." (Erdősi–Solymos, 2023).

Computer fraud is a huge category, perhaps the largest and oldest type of fraud, and although it could be broken down into several subcategories, this was not possible at this time.

Fake online stores and offers were one of the most popular forms of fraud during the COVID period, as almost everyone was shopping online during the period of restricted travel and physical contact. Due to closures and restrictions, the volume of e-commerce purchases increased significantly. According to ACI data, between January and June 2020, the volume of e-commerce purchases increased by 15%, and in May 2020, it increased by 81% compared to May of the previous year. This sudden jump created an ideal environment for fraudsters (ACI Worldwide, 2021).

This meant that many people fell victim to this type of fraud. However, the amount spent on online purchases did not reach the threshold at which victims would have sought help from the authorities. Many blamed themselves and did not report the crime, or learned from their own mistakes and did not make the same mistake again.

An increasing number of websites dealing with online fraud and monitoring potential fraudsters have become available (https://www.scamdoc.com, https://www.scamadviser.com), while KiberPajzs communication, corporate training, and self-organizing groups on social media (such as the Marketplace Scammers Facebook group with approximately 10,000 members) and independent websites (such as https://kamuwebshopok.hu) have also helped. I myself run a Facebook page called Mindennapi biztonságunk blog (Our Everyday Security Blog)[19] , where I try to provide useful security tips to more than 840 followers.

Further analysis of the survey data shows that about a quarter of respondents would only recognize if someone tried to install malicious code or remote management software on their device. If an attacker gets this far, it means that the attackers have managed to maintain the victim's attention and the victim has not recognized that they are a potential victim of an internet attack.

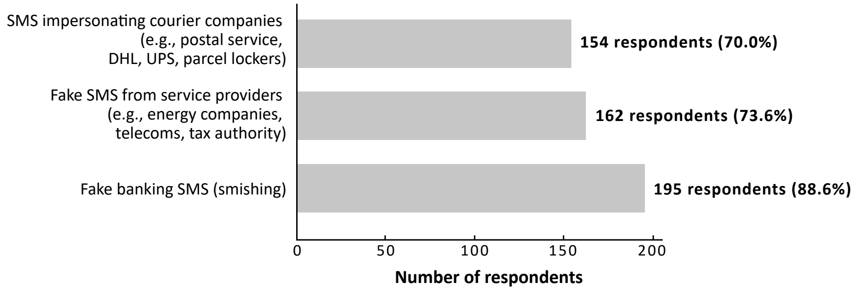
In the survey, the other type of technological fraud—connecting to a fake Wi-Fi network—came in last place. This is simply because people do not understand it and do not really care about it, and the use of personal mobile internet is becoming increasingly widespread.

[19] https://www.facebook.com/mindennapibiztonsagunk.

9.3 KiberPajzs topic 3. Question: SMS scams – test your knowledge!

How familiar are you with the following types of online financial fraud? Check the ones you can explain and recognize, and wouldn't fall for if someone tried them on you!

Figure 5
"SMS scams - test your knowledge!" graph



Source: Internet dangers and recognition questionnaire, author's own research. 2025.

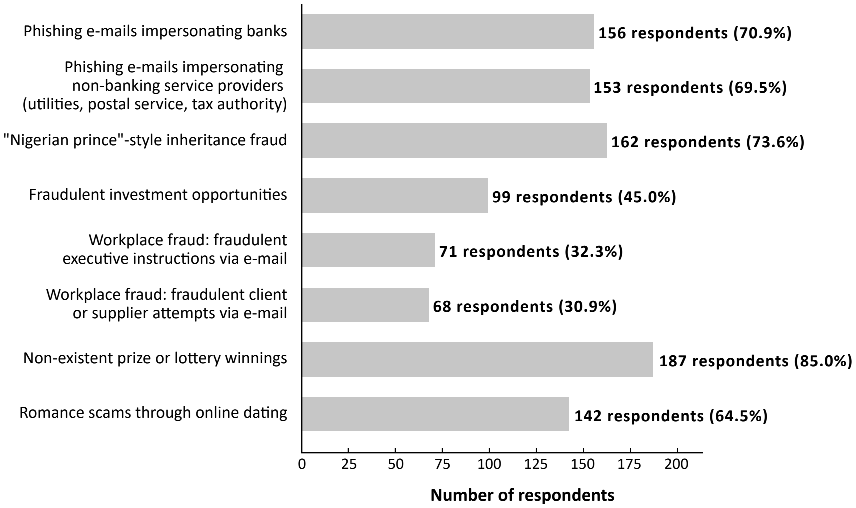
Phishing attacks via SMS have also become increasingly common during the COVID period, with the rise in online shopping, and continue to occur on a daily basis. Overall, the recognition of phishing attacks via this channel is outstanding, as 70% of respondents would recognize fake bank SMS scams, which is a good rate. One reason for this may be that SMS messages are short and concise, and scammers usually use some kind of URL shortening service, for two reasons. One is to hide the real link from the user, and the other is to fit within the required character limit. The channel itself, with its strange links, texts that typically contain grammatical and stylistic errors, and the almost always urgent tone, arouses suspicion in recipients.

The high profile of phishing attacks carried out in the name of courier companies is also due to the fact that articles describing such cases regularly appear in the press, whereby the wave has started, dangerous emails and text messages are spreading in Hungary. ("The wave has started, dangerous emails and text messages are spreading in Hungary" HVG, 2023). Or: "They received text messages from an unknown number on behalf of the DPD courier company, and their bank accounts suffered" (168.hu, 2024). The Hungarian Police also reports such cases on the Matrix project website: " s received phishing SMS messages on behalf of a courier service" (National Police Headquarters, 2024). Just by searching for the term "SMS fraud" on the police.hu website, more than 400 news items of this type can be found.

9.4 KiberPajzs topic 4. Question: Email scams – test your knowledge!

How familiar are you with the following types of online financial fraud? Check the ones you can explain and recognize, and wouldn't fall for if someone tried them on you!

Figure 6
"Email scams – test your knowledge!" graph



Source: Internet threats and recognition questionnaire, author's own research, 2025.

Email scams are perhaps one of the most widespread forms of Internet fraud. Given that correspondence as a form of communication is as old as writing itself, the emergence of scams and manipulation techniques through correspondence is also as old as writing. The only thing that has changed is whereby the speed of message exchange has increased and paper as a medium has been replaced by electronic formats. This statement is confirmed by the fact that, in parallel with the growing popularity of postal services in the United States, the number of letters relating to fake lotteries and fraudulent gifts increased to such an extent that, following a 1868 regulation, Congress in 1872, specifically to protect against postal fraud. The "18 U.S.C. § 1341 – Mail Fraud Statute" is still in force today and is constantly being updated in response to current frauds (18 U.S.C. § 1341, 2023).

Among email scams, apart from the phishing scams discussed earlier, "Nigerian" scams also have a long history, the origins of which are also based on postal correspondence. The ancestor of such scams is the "Spanish Prisoner" scam, which was widespread in Europe in the 16th-19th centuries. The essence of this scam was that fraudsters sent letters to wealthy people, claiming that a rich political prisoner (often a Spanish aristocrat) was being held captive and that his enormous fortune could only be released or transferred with some preliminary financial assistance. Victims were promised a huge reward in exchange for their help. This basic motif remains unchanged to this day.

Since scambaiting[20] is one of my hobbies, I have corresponded with many such scammers using a mailbox reserved specifically for this purpose. In my experience, scammers use a well-structured system with accounts that are used multiple times for each type of scam (for example, an heir suffering in an African refugee camp who will only receive his money if he finds a European partner to invest it, or a famous American soldier who offers a large sum of money in connection with obtaining money found in a safe in the Iraqi desert, or millions left in a Turkish bank by a deceased person with a name similar to that of the potential victim, and a well-meaning banker tries to deliver the money to the real heir). There have been cases whereby the same 'lawyer' was involved in two completely different types of fraudulent correspondence.

Different types of email scams are often mixed with romantic scams and investment scams. Although according to my research, these two forms of email fraud (the "Nigerian" and "out-of-the-blue winnings") are the best known, various forms of fraud continue to claim victims to this day, unfortunately causing losses of up to several million dollars.

The two least known categories, workplace scams (fake executive instructions via email and fake customer service or supplier attempts via email) can be explained by the fact that they presuppose active work experience, which is less relevant to younger age groups (27.3% of the age group, 3 people recognize it), and the oldest age group, those over 60, did not use electronic mail during their active working period.

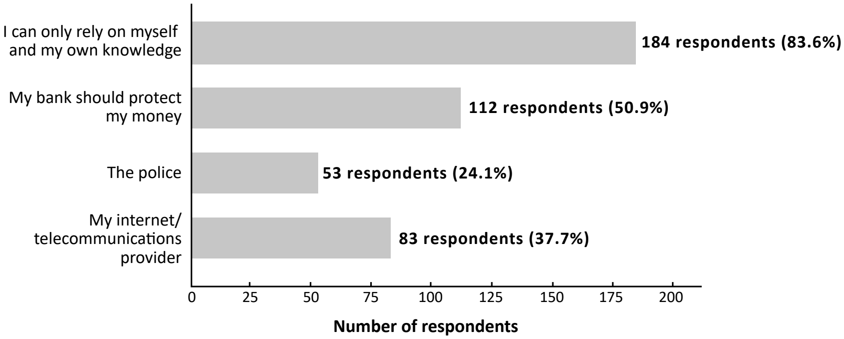
However, the analysis also shows that only 42% (68 people) of the 22-60 age group would recognize such fraud attempts.

[20] Scambaiting is a preventive defense practice in which users deliberately contact online scammers in order to tie up their resources and gather information about their scamming methods and campaigns. (*Charnsethikul–Crotty, 2025).*

9.5 The next three questions focused on the sources of the knowledge assessed above.

Question 1. "Who do you expect to protect you on the Internet?"

Figure 7
"Who do you expect to protect you on the Internet?" graph



Source: Internet dangers and recognition questionnaire, author's own research, 2025.

This question highlights an important topic, namely the basis of people's sense of security. Who protects me on the Internet? Since there were several possible answers, I examined the individual response variations as an analytical criterion. For reasons of space, it is not possible to analyse all combinations, but when it comes to finances, a significant proportion of people are distrustful and rely mainly on their own knowledge and vigilance. It is surprising that only half of the respondents chose the option "My bank protects my money." This is worth thinking about, as banks basically "sell trust." If people do not trust that the money they put in the bank will not be stolen, they will not put it there, or will only put in the bare minimum.

Based on the analysis, 85.7% of those who expect protection exclusively from banks, i.e., who selected only this option, are over the age of 61. The remaining 14.3% are between the ages of 22 and 60. It follows that the actively working and internet banking age group is less likely to believe that protection should be expected solely from banks. Respondents aged 22-60 generally expect joint protection from multiple actors (e.g., banks, police, service providers).

Let us now take a closer look at those who believe that they can only rely on themselves. Among them, let us examine those who did not consider any other option relevant. In terms of numbers, 102 respondents stated this. Analysing their responses, awareness of the KiberPajzs program among this group is distributed as follows. 43.1% (44 people) are familiar with the program, while the remaining

56.9% (58 people) are not. It is worth considering that these 44 people, although familiar with the KiberPajzs program, still only trust themselves. It follows that in their case, the assistance provided by financial institutions or even the police was not convincing. This is also suggested by the following result, according to which 24.5% (25 people) of the 102 respondents have already suffered financial losses, while the majority, 75.5% (77 people), have not. It is conceivable that their experience with the handling of the losses they suffered was poor on the part of the banks and/or the police.

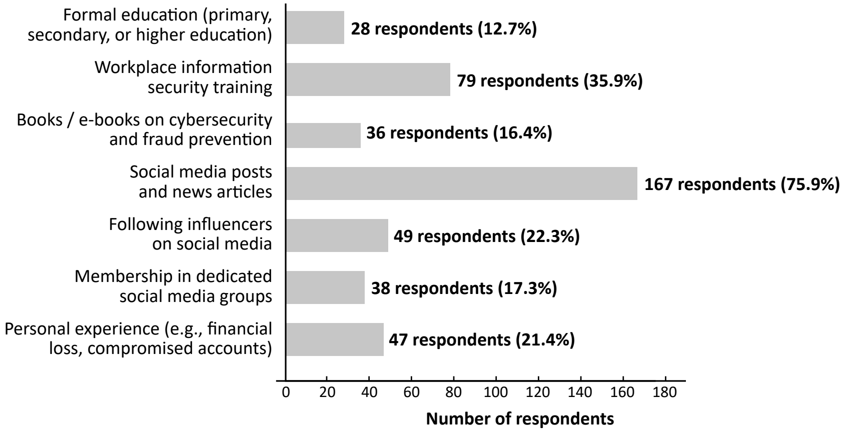
Question 2: "Do you talk about online dangers at home with your family?"

68.8% of respondents (151 people) regularly discuss the topic and warn each other if necessary. 29.5% (65 people) very rarely talk about online financial dangers in their family, as there would be too many things to discuss. 1.8% of respondents (4 people) believe that everyone experiences this at their own expense and do not usually discuss such matters within the family.

Nearly 70% of respondents regularly discuss the topic within their families. I consider this to be a positive thing. This type of knowledge can also be a topic of conversation for all age groups, building internal relationships and transferring useful knowledge.

Question 3 (last question): Where do you get/did you get the most useful information about online fraud?

Figure 8
Where do you get/did you get the most useful information about internet fraud? Graph



Source: Internet dangers and recognition questionnaire, author's own research. 2025.

This question also deals with a very important topic, and it is clear that three-quarters of respondents use social media platforms to learn about information security and financial security issues. Fortunately, in addition to government and civil society actors, there are many experts who regularly post about data and information security, either for the purpose of knowledge transfer or on their own thematic social media pages.

The low proportion of knowledge acquired at school can be explained whereby this topic was not at all relevant at the age when a significant proportion of respondents were attending school. Nevertheless, it is thought-provoking that the lowest percentage of respondents had paid for training themselves (4.5%, 10 people) or had read about security in books (16.4%, 36 people). There may be many reasons why people do not spend money on their own security and training. A wealth of security training is available on major educational platforms (e.g., Udemy, Coursera, Udacity, Thinkfic). Although a significant portion of these are outdated, based on the huge number of community reviews, those who have completed the training still consider it useful. Most of the courses cost a few thousand forints, are the most popular, and can be completed in a few hours. BUT in addition to these, there is a wide range of courses, from free crash courses in the form of e-learning to more serious courses lasting several weeks, some of which even lead to a university degree. The availability of books on reading and information security is minimal compared to the number of books available in Hungary. Most IT and information security books are textbooks or educational in nature. In addition, the Hungarian population, especially the younger generations, are reading less and less and are turning to audio and video-based learning. (Nagy, 2010)

It is important to note that among the methods and channels of knowledge acquisition, workplace information security training ranks second on the imaginary podium (35.9% of 79 people). I myself believe that it is in the best interests of companies and organizations to have security-conscious users. Moreover, they have the resources necessary to either prepare their own training materials or purchase them from companies specializing in information security. I also share the view expressed by that, first of all, users need to be made aware of the importance of information security by reflecting on their own lives and through examples from their own environment, and only then should company and organizational security rules be introduced. I am convinced that if users understand the importance of information protection through examples that affect them or their children, they will find it much easier to understand organizational security rules and will be much less inclined to circumvent or bypass them. This, in turn, significantly reduces the level of risk for organizations. Human error and irresponsibility have been one of the main causes of information security incidents for many years. In a blog post by KnowBe4, one of the leading information security awareness companies, an article backed by Stanford University research states that 88% of security incidents can be traced back to human error (KnowBe4, 2020).

A significant portion of workplace information security training is mandatory, and users are required to complete it, which is perfectly fine. It is good practice for organizations to make available, in addition to the mandatory curriculum, additional courses or training materials that are not strictly related to the workplace but increase user awareness, providing opportunities to learn about, for example, children and the dangers of cyberspace, artificial intelligence, online financial fraud and attacks, or even the dangers of social media.

Looking at the big picture, if we disregard mandatory school and workplace training and focus only on voluntary information gathering, it is clear that social media is the main source of information for users, and this should be built upon in the future.

10 SUMMARY AND CONCLUSIONS

The aim of this study was to provide a comprehensive overview of the development of online financial fraud in Hungary, with a particular focus on the evolution of customer security awareness and the role of the KiberPajzs program. Cybercrime is growing at a rapid pace (Kovács–Terták, 2024), while the security awareness of users of online financial services is unable to keep pace with the ever-evolving methods of attack and fraud. This also increases the risks of digital financial services, especially if customers' security knowledge remains inadequate or is coupled with overconfidence in the future.

In this study, I wanted to remind readers that the primary target of attacks today is no longer the banking system, but the customers themselves. As a cyber security expert with an educational approach, I drew not only on the literature and past events, but also on my own professional experience, including my experiences and memories gained in more than ten years in the field of information security at financial institutions.

While working on this topic, I concluded that although the KiberPajzs program has launched a serious catch-up effort involving a number of relevant organizations in order to raise security awareness in society, it is essential to take further steps in other areas as well. such as putting a central abuse filtering system in place and tightening the requirements on the part of the MNB. Based on the research results, I see a need to strengthen regular awareness campaigns targeted at specific age groups, especially considering the specific media consumption habits of younger generations.

At the same time, I see an opportunity for the government to encourage companies and organizations to strengthen information protection and internet financial awareness for their employees, whereby. Although the GINOP plus workplace training support program[21] was an excellent opportunity for this, I recommend that calls for proposals be launched specifically to support training courses reflecting on these two topics.

In addition, strengthening the presence of social media is another opportunity in which both KiberPajzs and the entire Hungarian expert community need to mobilize greater resources. In this area, I could also imagine supported experts who regularly and credibly try to pass on their knowledge, almost like influencers. Currently, this activity is carried out on a completely voluntary basis, with varying intensity and varying levels of knowledge.

Greater emphasis should also be placed on reaching the oldest age groups, but it should be borne in mind that in ten years' time, the generation in their sixties will already have ample knowledge of the internet and technology, if only through their own experience, and they will be significantly different from the current generation in their sixties and seventies. We need to prepare for this and choose the right communication channels now, taking into account the results of generational research, which is receiving increasing attention these days.

Future research should examine the effectiveness of different forms of education and monitor the changes in the population's attitudes towards information security over the longer term. By implementing these recommendations, supplemented by technological developments and stricter legislation, it would be possible to compete effectively with cybercriminals who are after citizens' money.

REFERENCES

168.hu (August 28, 2024): They received a text message from an unknown number on behalf of the DPD courier company, and their bank account suffered. https://168.hu/itthon/adathalasz-sms-magyar-dpd-280780 (downloaded: May 15, 2025).

ACI Worldwide (2021): Pandemic-Driven Patterns of eCommerce Fraud. https://www.aciworldwide.com/wp-content/uploads/2021/04/pandemic-driven-patterns-of-ecommerce-fraud-article.pdf (downloaded: May 20, 2025).

biztonsagosinternet.hu. (December 19, 2006): [Website archive] biztonsagosinternet.hu (archived by *Wayback Machine*) https://web.archive.org/web/20061012000850/http://www.biztonsagosinternet.hu/ (downloaded: 10.06.2025).

[21] https://www.palyazat.gov.hu/programok/szechenyi-terv-plusz/ginop-plusz/ginop-plusz-321-21/alapadatok.

Chakravorti, S. (2000): Why Has Stored Value Not Caught On? Emerging Issues Series, Supervision and Regulation Department, *Federal Reserve Bank of Chicago.* (S&amp;R-2000-6). https://doi.org/10.2139/ssrn.294516 (downloaded: 10.05.2025).

Charnsethikul, P., Crotty, C. (et al., 2025): *Puppeteer*: Leveraging a Large Language Model for Scambaiting. *University of Hawaii ScholarSpace.* https://doi.org/10.24251/hicss.2025.131 https://scholarspace.manoa.hawaii.edu/items/86d10c9c-236f-425e-ae86-b917f10b3d9b.

CERT-Hungary (November 16, 2006): *I. Incident Management Workshop* [Website archive]. cert-hungary.hu (archived by Wayback Machine). https://web.archive.org/web/20070708044324/http://www.cert-hungary.hu/modules.php?name=News&amp;file=article&amp;sid=29 (downloaded: 14.06.2025).

CERT-Hungary (December 19, 2006): Phishing attacks against Hungarian banking systems [Website archive]. cert-hungary.hu (archived by Wayback Machine) https://web.archive.org/web/20070708044209/http://www.cert-hungary.hu/modules.php?name=News&amp;file=articl e&amp;sid=30 (downloaded: June 14, 2025).

Check Point (19.09.2017): August's Most Wanted Malware: Banking Trojans and Ransomware That Want Your Money. *Check Point Research Blog.* https://blog.checkpoint.com/security/augusts-wanted-malware-banking-trojans-ransomware-want-money (downloaded: 14.06.2025).

Erdősi, P. M. – Solymos, Á. (2023): IT Security Made Easy. *János Neumann Computer Science Society (NJSZT).* https://njszt.hu/letoltheto-it-biztonsag-kozerthtetoen ISBN: 978-615-5036-26-2 (downloaded: May 10, 2025).

HVG (May 23, 2023): The wave has started, dangerous emails and text messages are spreading in Hungary. *HVG Tech.* https://hvg.hu/tudomany/20230523_kamu_email_sms_futarszolgalatok_atveres_adathalasz_levelek_banki_adatok_bankkartyaadatok_csalok (downloaded: 14.06.2025) .

Gillis, A. S. (May 17, 2022). *What is man in the browser (MitB)?* TechTarget. https://www.techtarget.com/searchsecurity/definition/man-in-the-browser (downloaded: 2025.06.14.)

GKIeNET. (2002): E-banking in Hungary 2002. Budapest: *GKI Economic Research.* https://enet.hu/jelentes-az-internet-gazdasagrol-fokuszban-a-penzugyi-szektor-2002-iv-negyedev/ (downloaded: May 30, 2025).

Jurík, P. (2007): Bank Card Encyclopedia – From the Beginning to the Present Day. *HVG Publishing Ltd.* ISBN 978-963-9686-31-1, 67.

Kruger, J. – Dunning, D. (1999): Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, 77(6), 1121–1134. https://doi.org/10.1037/0022-3514.77.6.1121 (letöltve: 2025.06.03.).

KnowBe4. (2020): Stanford Research: 88% of Data Breaches Are Caused by Human Error. *KnowBe4 Blog.* https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error (downloaded: 06.14.2025).

Kovács, L. – Tertàk, E. (2024): The best antidote to cybercrime: financial literacy. *Economy and Finance*, 11(1), 6–29. https://doi.org/10.33926/GP.2024.1.2 https://bankszovetseg.hu/Public/gep/006-029%20Kovacs_Tertak.pdf (downloaded: 10.06.2025).

Lemák, G. (September 15, 2016): A Brief History of Hungarian FinTech (beta). *FinTechZone.* https://fintechzone.hu/a-nagy-magyar-fintech-tortenelem-beta/ (downloaded: June 10, 2025).

Magyar Nemzeti Bank (2023). Money Flow 2030: The MNB's strategic objectives for money flow and the introduction of the Money Flow Development Indicator System. Budapest: *Magyar Nemzeti Bank.* https://www.mnb.hu/letoltes/penzforgalom-2030-strategia.pdf (downloaded: 04.06.2025).

Hungarian National Bank press conference (03.06.2025): "The MNB plans to crack down on bank fraud with five measures" [HVG article]. *HVG*. https://hvg.hu/gazdasag/20250603_Ot-csapassal-szamolna-le-a-banki-csalasokkal-az-MNB (downloaded: 30.05.2025).

Hungarian National Bank (2025): Money transfer fraud (March 17, 2025) Fraud in electronic money transfers (Excel file). https://statisztika.mnb.hu/timeseries/3-visszaelesek.xls (downloaded: 30 May 2025). 8.

Mastercard – Bank of the Year (2024): Cyber security education campaign of the year 2024 – among the categories of Bank of the Year. https://www.evbankja.hu/kategoriak/az-ev-kiberbiztonsagi-edukacios-kampany (downloaded: June 15, 2025).

Nemes, M. (2025): The Age of Cybercrime 2025. *Mastercard* – KiberPajzs. https://kiberpajzs.hu/letoltes/a-kiberbu-no-ze-s-kora-2025-o-sszefoglalo-kiberpajzs-0220fin-mnb.pdf (downloaded: 30.05.2025) 3-9-17.

Neumann János Computer Science Society (June 27, 2017): IT security made easy to understand – NJSZT makes new, free textbook available. https://njszt.hu/hu/news/2017-06-27/it-biztonsag-kozerthetoen-uj-ingyenes-tankonyvet-tesz-hozzaferhetove-az-njszt (downloaded: 30 May 2025).

Neumann János Computer Science Society (December 7, 2023): The Neumann Society's updated IT security textbook is available for free download. https://njszt.hu/hu/news/2023-12-07/ingyenes-en-letoltheto-neumann-tarsasag-frissitett-it-biztonsagi-tankonyve (downloaded: June 14, 2025).

Nagy, J. (2010): Reading culture among 9–14-year-olds in Hungary (Thesis*). University of Debrecen, Faculty of Informatics, Department of Library Informatics*, Debrecen. https://dea.lib.unideb.hu/server/api/core/bitstreams/c83d8ccb-8fef-4cdb-9261-12d57fd33171/content (downloaded: 14 June 2025).

PÉNZ7 (March 3, 2025): *The successes of PÉNZ7 in 2025*. PÉNZ7 – *Finance and Entrepreneurship Theme Week* https://penz7.hu. (downloaded: June 14, 2025).

Prim.hu (November 21, 2005): The number of internet banking customers has grown by more than half. *Prim Online*. https://hirek.prim.hu/cikk/49636/ (downloaded: May 10, 2025).

National Police Headquarters (February 16, 2024). *Matrix Project – we are investigating nearly 7,500 cases*. Police.hu. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/matrix-projekt-kozel-7500-ugyben-nyomozunk (downloaded: June 12, 2025).

National Police Headquarters (November 6, 2023): Matrix Project for cyber security. *Zsaru Magazine* / police.hu. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/matrix-projekt-a-kiberbiztonsagert (downloaded: May 10, 2025).

National Police Headquarters (March 26, 2024): Phishing SMS received on behalf of a courier service. *Police.hu*. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/egy-futarszolgalat-neveben-kapott-adathalasz (downloaded: 10.05.2025).

Solymos, Á. (July 7, 2011): On home turf – Experiences with domestic phishing [Presentation]. *IIR Masterclass Financial Institution Fraud Management* Conference, Budapest. (Presentation slides available in unpublished form from the author.)

Solymos, Á. (2018): In: Berzsenyi D., Gyaraki R., Hámornik B. P., Hirsch G., Kiss A., Marsi T., Orbók Á., Simon B., Solymos Á., Tikos A., Zsíros P. Incident Management – Annual training course for persons responsible for the security of electronic information systems *2017. ISBN 978-615-5764-99-8 (PDF). https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/6848/Incidensmenedzsment.pdf?sequence=1 (*downloaded: 24 May 2025). 167.

United States Postal Inspection Service (2023): History of the Mail Fraud Statute (18 U.S.C. § 1341). https://www.uspis.gov/history-spotlight-2023/history-of-the-mail-fraud-statute (downloaded: 24.05.2025).