Advances in Web Development Journal

vol. 1 no. 2, pp. 13–25

*Submitted: 2023-10-13 | Revised: 2023-10-13 | Accepted: 2023-10-13*

*Keywords: authentication, cyber security, sms, 2fa*

*Albert SZPUNAR [1], Arkadiusz STĘCHŁY [2*]*

# ANALYSIS OF POTENTIAL RISKS OF SMS-BASED AUTHENTICATION

**Abstract**

*The pervasive use of mobile devices and the omnipresence of the Internet have ushered in a transformative era. Nearly everyone, regardless of age, possesses a mobile phone, bridging generational gaps in digital interaction. Mobile phones have become highly personal, with users guarding them zealously. Service providers recognize this intimate relationship, offering an opportunity to enhance security. Traditional password-based security is vulnerable to data breaches, prompting the adoption of mobile phones as a more robust platform for safeguarding digital assets. This shift has also facilitated the development of digital identification applications, reducing reliance on physical identity documents. Additionally, mobile banking applications are replacing physical payment cards, enabling secure transactions. The ascendancy of mobile payment solutions is diminishing the role of physical cash and wallets. In summary, mobile devices have reshaped security and daily activities, becoming the cornerstone of our digital existence, offering higher levels of security, convenience, and efficiency .*

## 1.INTRODUCTION

The popularization of mobile devices and the Internet has dramatically changed the reality around us. Regardless of the age of the members of society, one can assume that they own a mobile phone. Even the elderly today have their own phones and browse Facebook, which can be seen in many a senior center or University of the Third Age. Children also use mobile phones to browse YouTube or TikTok, so much so that YouTube Kids was created [1].

A separate issue is also the matter of how much time people spend on their phones per day [2]. As shown on Fig. 1. 17.3% of surveyed adolescents spend more than 8 hours a day

1. University of Information Technology and Management, Poland
2. Rzeszow University of Technology, Department of Complex Systems, Poland

online. This shows overall attachment to those devices, which is a good foundation for basing peoples security on them.

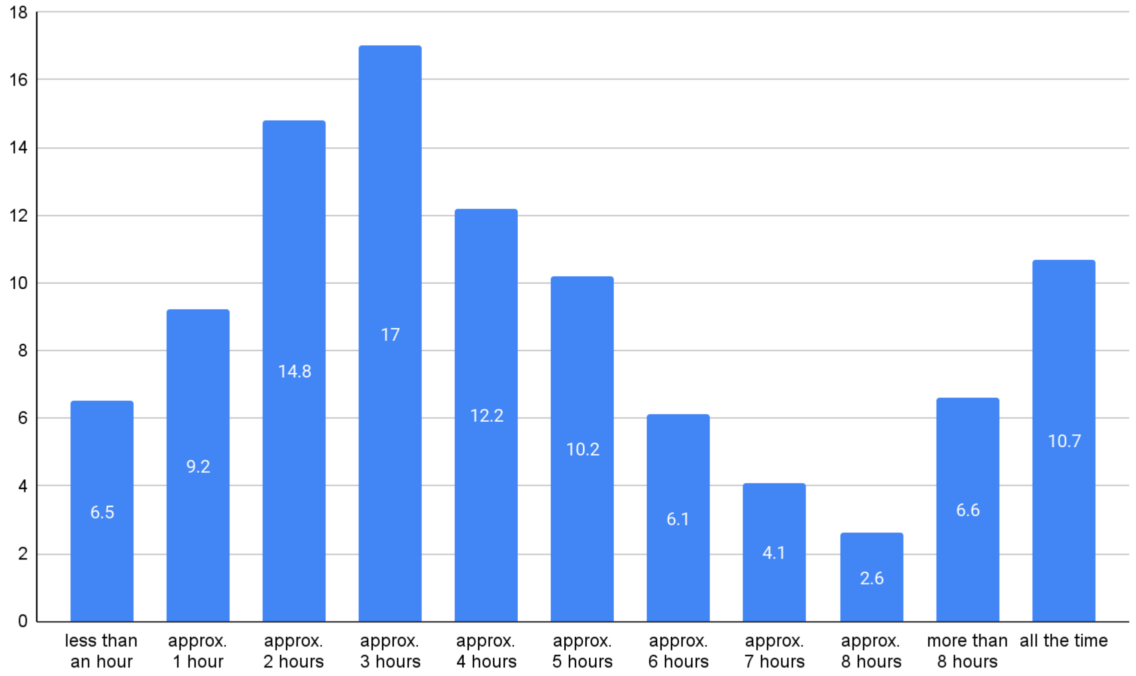


**Fig. 1. Number of hours adolescents spend online [2]**

Another important aspect is the content of the analyzed device and the fact that it is exclusively private. Thus, the owners themselves protect their devices from access by other people, not even handing it over to show a photo. Some people have a fear that the person that received their phone will start looking through the entire gallery violating privacy, which can be an even worse feeling than the content of the photos viewed itself.

This way, service providers have gained a strong component on which to base a new level of security. In addition, this is the ideal time for this type of change, as the old passwords have long been compromised by leaks, and thus accounts have become vulnerable as most people do not change their passwords and don't see the need to do so.

Another point that has arisen from the popularization of mobile devices is the possibility of reducing the amount of things one needs to carry. Instead of an identity card, all someone needs to have is an electronic identification application installed on their phone and confirm one's identity with it. This technology is only just being introduced, but it will allow people to avoid carrying an identity card or driving license. Thanks to this, it will also be possible to avoid the scenario of forgetting one's driving license while being stopped for an inspection and avert the resulting consequences.

Another natural adjustment is abandoning payment cards in favor of a banking application [3] on the phone. Especially since, applications also allow for checking account balance and transfer history. Authentication via SMS is an intermediate state between reusable passwords and the full verification of transactions via applications on mobile phones. However, this solution has one disadvantage in favor of authentication via SMS codes. The application must have constant access to the Internet for full functionality. SMS codes only require the device to be logged into the cellular network. Over time, this difference will naturally be blurred. Another aspect to keep in mind is the internal memory of the device, the applications must be installed on. Additionally a rooted phone completely excludes the operation of banking applications. In these aspects, SMS-based authentication is a better solution.

Using the phone as a payment card is also inadvertently a factor in eliminating physical money. While this is a debatable topic given the potential for abuse, the fact remains that it allows someone to dispense with carrying a wallet.

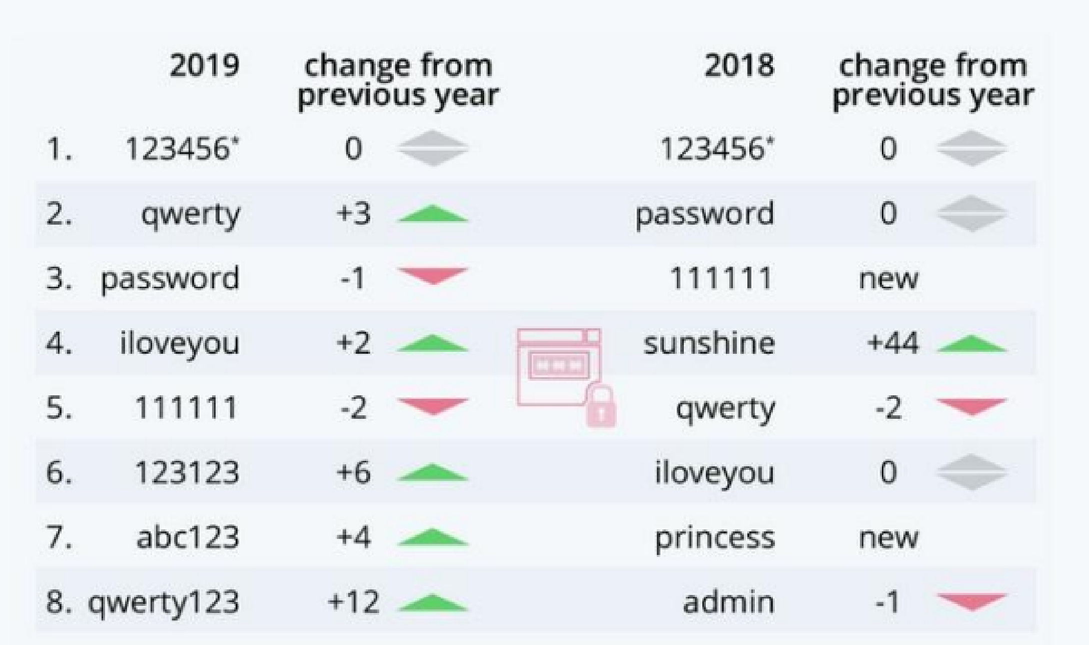
# 2.BASIC TERMS AND CONCEPTS

**2FA** – Two-factor authentication
**U2F** – Two-factor authentication using external usb device
**Phishing** – a method of attack involving the impersonation of another person or institution
**Spear phishing** – a method of attack based on impersonation, targeting a specific person
**One-time password** – authentication code which is valid once and for a certain amount of time
**Mobile phone** – smartphone or ordinary phone operating on GSM
**Mobile network operator** – a provider of wireless communications services
**SIM card** - a card with data assigned to it that allows for a connection to a network
**Electronic identification application** – application for proof of identity of citizens
**SIM SWAP** - a type of attack that involves making a duplicate SIM card

## 3.SMS-BASED 2FA

SMS, which stands for Short Message Service, is a widely accessible feature found on the majority of digital mobile devices. It enables the transmission of text messages, limited to 140 bytes in length, facilitating communication between various applications and individuals [4]. SMS has a wide range of capabilities. Among other things, it is used for security purposes. SMS code authentication is a system called two-factor authentication. The name comes from the fact that, in addition to entering a username and password, the user must also confirm his identity using another factor. It can also be referred to as two-step verification or multi-factor authentication. The abbreviation used for this method is 2FA [11].

The need to strengthen the user verification process arose due to the scale of the digitalisation of everyday life. People use a very large number of services where passwords are required. This naturally leads to an increasing number of logins and passwords, which significantly affects security. Many people set a single password for all services or use one of the common ones shown on Fig. 2. There are cases where the password for a service is identical to the one used for the mailbox. One problem that arises is the complexity of the password. The more complex it is, the more secure it is, but also the more difficult it is to remember. Therefore, a lot of people opt for a small number of simple passwords that are more likely to be cracked. In addition, the password might be too simple or someone might be able to see what characters are entered, either by looking at the keyboard or by using a keylogger.



| | 2019 | change from previous year | | 2018 | change from previous year | |
|---|---|---|---|---|---|---|
| 1. | 123456* | 0 | ◆ | 123456* | 0 | ◆ |
| 2. | qwerty | +3 | ▲ | password | 0 | ◆ |
| 3. | password | -1 | ▼ | 111111 | new | |
| 4. | iloveyou | +2 | ▲ | sunshine | +44 | ▲ |
| 5. | 111111 | -2 | ▼ | qwerty | -2 | ▼ |
| 6. | 123123 | +6 | ▲ | iloveyou | 0 | ◆ |
| 7. | abc123 | +4 | ▲ | princess | new | |
| 8. | qwerty123 | +12 | ▲ | admin | -1 | ▼ |

**Fig. 2. Most popular passwords in 2019 and 2018 [5]**

Another weakness of password-only verification is the problem of storing them with service providers. It is increasingly common for data to be stolen from service providers, in a so-called leak. Additionally most leaks are unintentional, caused mostly by a wrongly entered email [6]. Incidents of such leaks divided by industry are shown on Fig 3. Passwords and logins are then compromised and someone can use them to log into a victim's accounts. Both for profit-making purposes and to compromise someone, especially on social networks. This can be done by anyone who knows both the login and password, because the problem of the verification process is that just knowing these details does not prove the identity of the user.

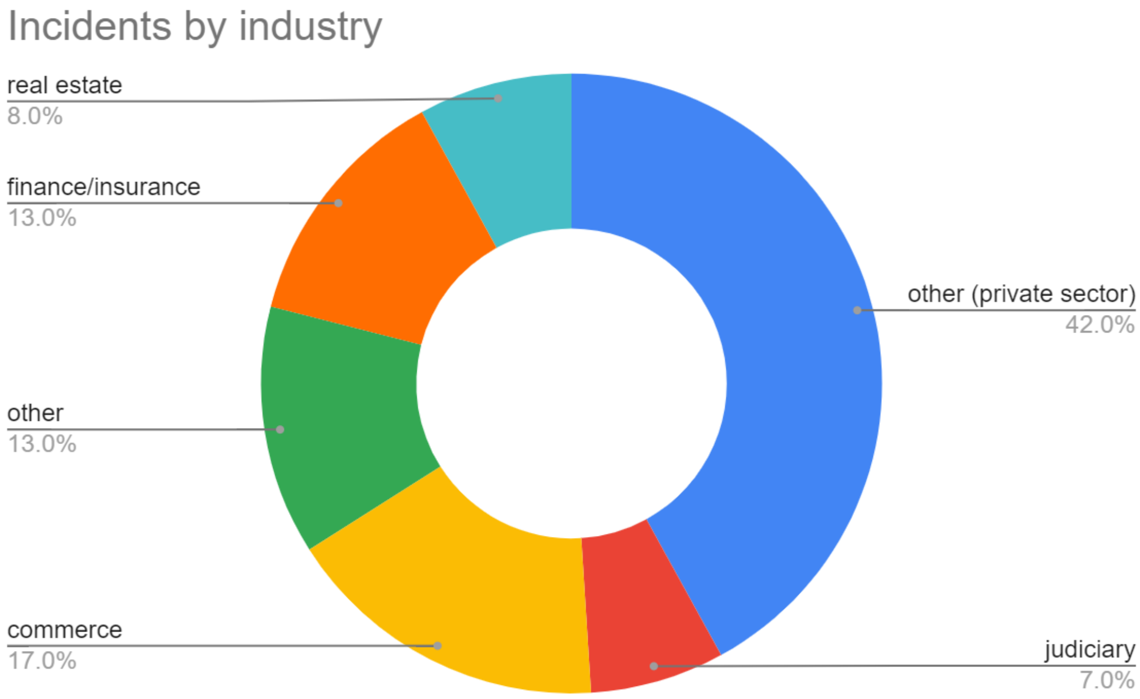


**Fig. 3. Data leaks by industry [6]**

In addition, there is a possibility of falling victim to a social engineering method, a so-called phishing or spear phishing [7] attack. If a target falls prey to such an attack, the attacker acquires their private information, which for example, allows them to gain access to a bank account. Regardless of the details of the attack being carried out. The essence of two-factor authentication is no longer based solely on the component of knowledge, i.e. the username and password, but also on something physically in possession. Which is a significant improvement in the standard of security.

Many shops have introduced loyalty applications for their customers. They offer promotions for card holders, such as “DeliKarta” shown on Fig.4., and display current promotions and coupons. However, neither an app nor the device is required, the phone number alone is sufficient. The authentication during the account creation process itself when issuing the card comes down to an SMS code. This solution has its flaws, for example, someone can use a phone number and take advantage of promotions belonging to someone else. However, the comfort of use favors the use of the phone number by itself.

**Fig. 4. Loyalty Card for Polish supermarket chain "Delikatesy Centrum"**

The SMS code can also only be used to confirm users identity when creating an account. It will not be needed until the user tries to regain access to the account after it has been stolen or in the situation when he has forgotten the password. A separate issue is the database of numbers that can be leaked or sold, which means that the compromised number will then receive fraudulent messages. The more often someone gives out their phone number, the more vulnerable it is to this.

Google has recently made it possible to read SMS in a browser on a computer. The exchange takes place by sending information from the mobile phone to a Google account and then to the computer. This is one of the new options that could potentially pose a threat, especially to less advanced users. It concerns the theft of messages from the mailbox or the constant interception of its contents. Not necessarily by Google, but by a kind of spyware that can be placed on the device beforehand if the attacker had access to the victim's phone, such as the SpyPhone shown on Fig. 5 [8]. In this way, someone could learn verification codes and even modify the contents of a mailbox on the fly. Such an attack could be carried out at night and lead to the victim not even knowing that the authentication message has arrived, as it could be used and deleted while the victim is asleep.

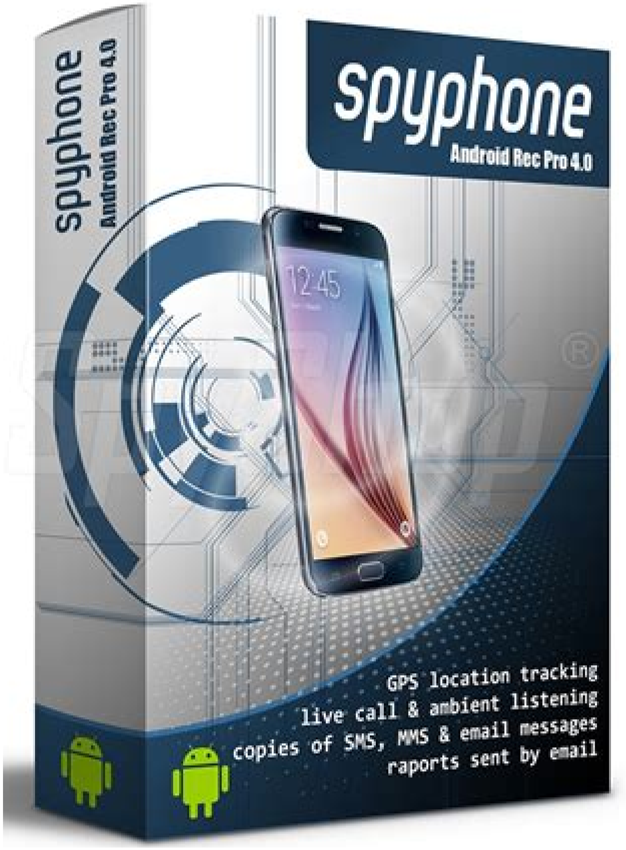
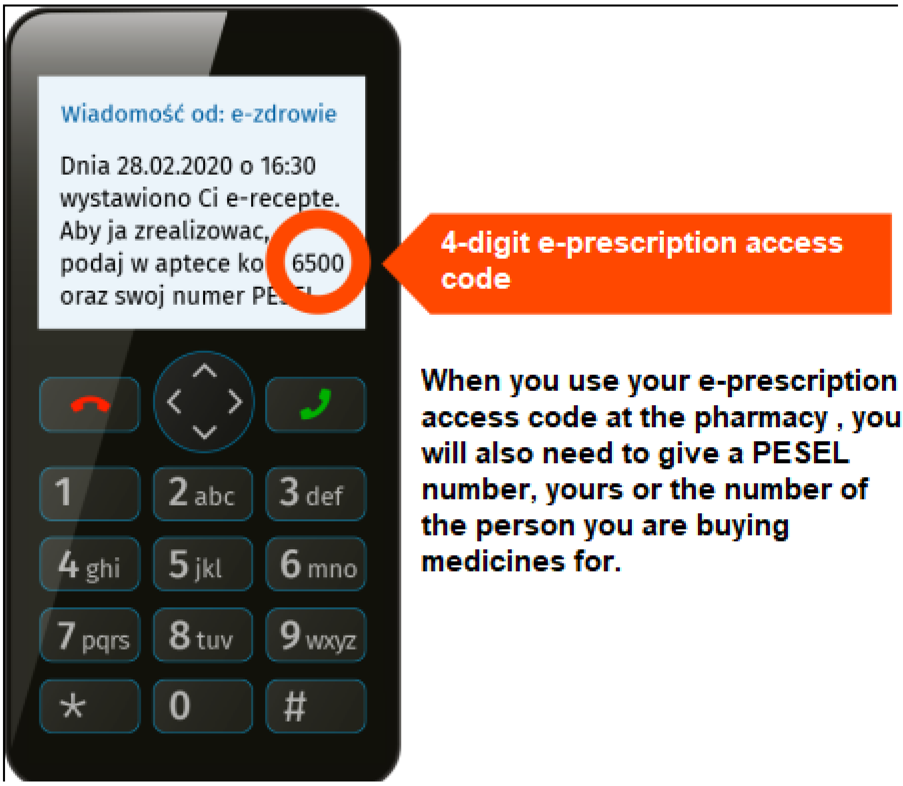


**Fig. 5. Ad for SpyPhone, an app that allows for tracking GPS, contacts and other installed apps.**

The prevalent use of phone numbers is also a problem. Every person with a Facebook account already has a phone number connected with a name. Even without consent, the service provider has access to this type of information as well as the IP addresses from which logins occur. There are also special websites that openly inform the user who the phone number belongs to. Most of this data comes from leaks (eg. facebook leak in Indonesia [12]). The more people use services that require their phone number, the easier it is for their numbers to end up in such a database.

A new technology is also being introduced in Poland [10], allowing for connection between the phone numbers and the trusted profile or e-prescriptions [9] of citizens. This way, phone numbers allow users to check a wide range of data concerning them. More and more service providers accept the use of this type of authentication. An example of an e-prescription text message is shown on Fig. 6.



Wiadomość od: e-zdrowie

Dnia 28.02.2020 o 16:30 wystawiono Ci e-recepte. Aby ja zrealizowac, podaj w aptece ko 6500 oraz swoj numer PE

4-digit e-prescription access code

When you use your e-prescription access code at the pharmacy , you will also need to give a PESEL number, yours or the number of the person you are buying medicines for.

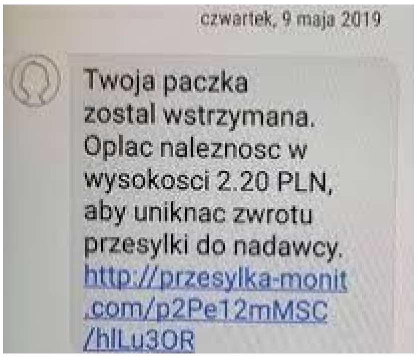
Fig. 6. An example of e-prescription text message

Advantages of the solution:
During bank transfers, verification SMS is sent with information about the transaction. This reduces the possibility of transferring funds to a fraudulently changed target account. It is also not necessary to show the entire account number, the last digits are sufficient.
Furthermore, as part of the text message information about the amount of funds to be transferred is also shown. Which further helps while verifying the transaction. Each one-time password necessary for confirmation of the transaction has an expiry date and can only be used to verify one transfer.
In addition, it is a very low-cost way of verification as a business does not have to specifically maintain a separate application.

Downsides of the solution:
Someone can view the content of the verification SMS on a locked phone if the security configuration is not set up correctly. Another problem could be the direct transfer of the SIM card to another device. If the card does not require a PIN code at start-up, it’s possible to see the entirety of a text message. This is why on some phone models where a banking application is installed it is necessary to set up a screen lock method, even if it’s only a set of the ones.
An attack called SIM swap [13] is also a threat. If someone wants to launch an attack and is in possession of victims data, they can create a false identity card with which they will be able to obtain a duplicate SIM card from the operator. In this case, the current card will be deactivated and the perpetrator will receive a verification SMS code from the bank and then authorize the transaction.

2FA protects against the risks of compromised passwords. However, it does not protect against phishing attacks or other voluntary forwarding of verification code. A better solution to protect against phishing is the U2F dongle. However, this is an impractical solution for most users.

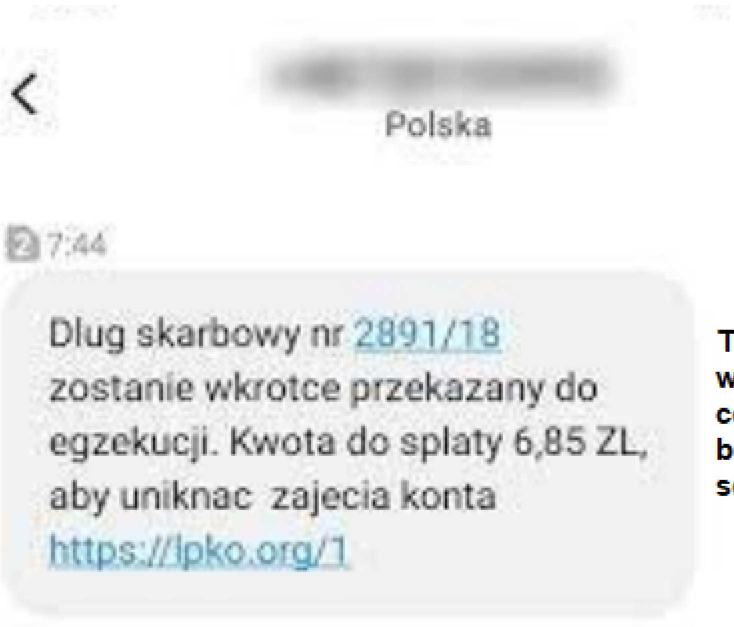
Another type of threat that is connected to a phone number and SIM card is SMS messages from various criminals impersonating service providers [14] that pressure users into clicking on a link or paying for a parcel, for example on the grounds that it has exceeded its weight. The amounts are usually negligible, so as not to raise suspicion. In this way, people expose themselves to further attacks as they are labeled as vulnerable and risk being targeted by a larger amount of fraudulent messages.



czwartek, 9 maja 2019

Twoja paczka zostal wstrzymana. Oplac naleznosc w wysokosci 2.20 PLN, aby uniknac zwrotu przesylki do nadawcy. http://przesylka-monit.com/p2Pe12mMSC/hILu3OR

**Your package has been put on hold. Pay the fee of 2.20 PLN to avoid returning the shipment to the sender.**



[redacted]
Polska

7:44

Dlug skarbowy nr 2891/18 zostanie wkrotce przekazany do egzekucji. Kwota do splaty 6,85 ZL, aby uniknac zajecia konta https://lpko.org/1

**Treasury debt No. 2891/18 will soon be transferred to collections. The amount to be paid 6.85 ZL to avoid seizure of the account**

**Fig. 7. Fraudulent messages**

The fact that it is easy to spoof the SMS sender can add to the criminals credibility. Therefore even SMS alert services can be exploited by fraudsters. Every convenience opens the way to weaknesses in terms of the security of people's data.

# 4.COMPARISON AND ANALYSIS

A separate method at a similar level in both requirements and effectiveness is authentication through special applications. In these, service providers rely on vendor-direct solutions, without imposed standards. Each banking application uses its own proprietary solution. In this case, however, a permanent Internet connection is required. So are requirements for the system to be up-to-date and have sufficient memory. Some applications also offer the use of biometrics as a form of security. In many cases, authentication by SMS alone is sufficient. An example of that kind of application is shown on Fig. 8.

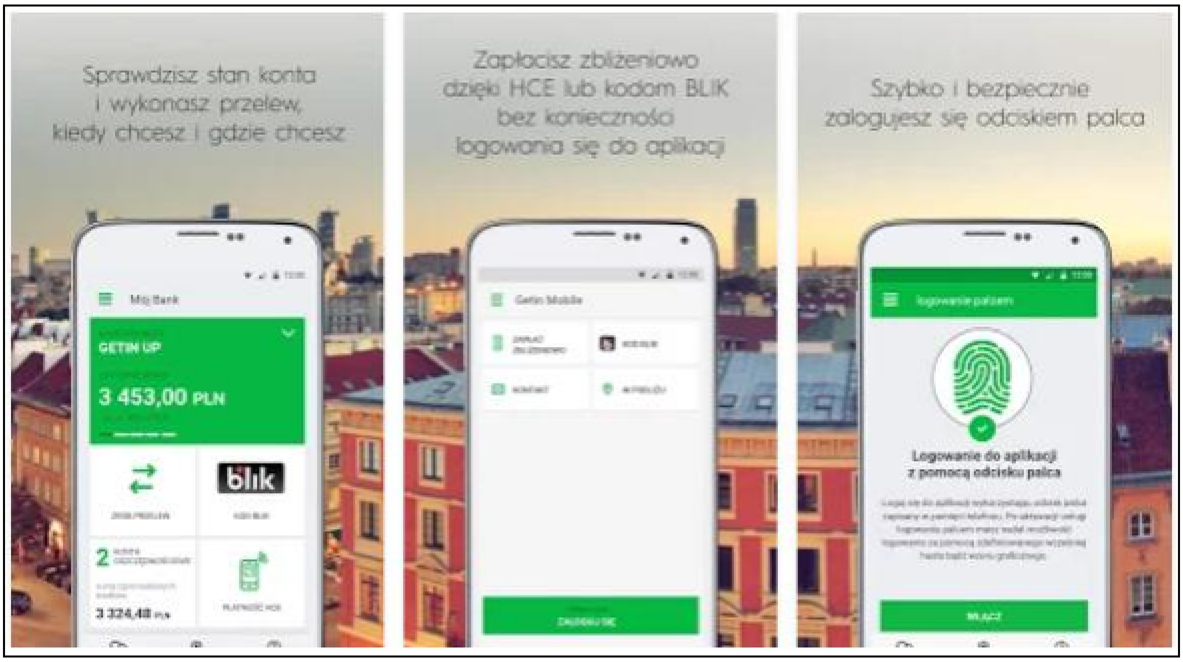


**Fig. 8. Ad for a banking application that uses biometrics**

An even more secure solution for confirming a person's identity is the use of a hardware key, such as YubiKeys [15] shown on Fig. 9. However, this solution requires a computer and is not yet applicable to mobile devices. Without a dongle, it is not possible for a third party to log in.

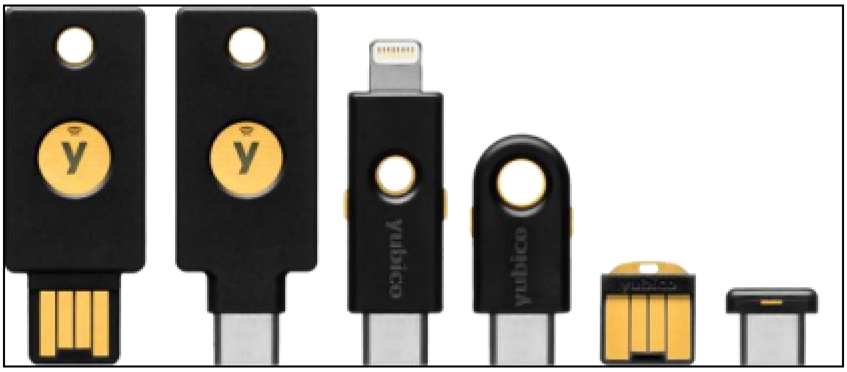


**Fig. 9. YubiKeys, dongle based 2FA**

# 5.SUMMARY

SMS authentication is a welcome advancement in security of accounts, previously protected only by usernames and passwords. It is an intermediate approach between passwords and authentication via special applications based on biometrics, effective enough to suffice in many cases. Especially considering the cost of maintaining additional applications. More secure solutions are unfortunately less practical, which is the reason for their slow adoption. For an average user the level of security that a dongle offers is not enough to counteract its inconvenience. SMS authentication is unlikely to be superseded any time soon and for some operations it has a high chance to remain as a permanent solution.

**Author Contributions**

*All authors declare equal contribution to this research paper.*

**Conflicts of Interest**

☑ *The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.*

☐ *The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:*

……………………………………………………………………………………………

## REFERENCES

[1] Babusabgari., Balakrishna B. (2021). Exposure and use of digital media among under-five children DOI: https://doi.org/10.18203/2349-3291.ijcp20213315
[2] Dębskiego M., Bigaj M. (2019). Ogólnopolskie badanie Młodzi Cyfrowi [Polish national survey “Młodzi Cyfrowi”].
https://dbamomojzasieg.pl/wp-content/uploads/2019/11/Ogolnopolskie-badanie-Mlodzi-Cyfrowi.pdf
[3] Sharma, Akash & Singh, Sunil & Kumar, Sudhakar & Chhabra, Anureet & Gupta, Saksham. (2023). Security of Android Banking Mobile Apps: Challenges and Opportunities. 10.1007/978-3-031-22018-0_39.
[4] Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., & F. Gómez-Skarmeta, A. (2007). A Survey of Electronic Signature Solutions in Mobile Devices. Journal of Theoretical and Applied Electronic Commerce Research, 2(3), 94–109. MDPI AG. Retrieved from http://dx.doi.org/10.3390/jtaer2030024
[5] Katharina Buchholz (2021). The Most Popular Passwords Around the World https://www.statista.com/chart/16922/most-popular-passwords-2017-and-2018/
[6] Aleksandra Grendys (2020). Raport: 89% wycieków danych w firmach to przypadki nieumyślne [Report: 89% of data leaks in companies are unintentional].
https://przemyslprzyszlosci.gov.pl/raport-89-wyciekow-danych-w-polskich-firmach-to-przypadki-nieumyslne/
[7] Shukla, Anjali & Chavan, Sameer & R, Srivaramangai. (2023). Spear Watch: A Thorough Examination to Identify Spear Phishing Attacks. International Journal of Innovative Technology and Exploring Engineering. 12. 46-51. 10.35940/ijitee.H9680.0712823.
[8] Liu, Enze & Rao, Sumanth & Havron, Sam & Ho, Grant & Savage, Stefan & Voelker, Geoffrey & Mccoy, Damon. (2023). No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps. Proceedings on Privacy Enhancing Technologies. 2023. 207-224. 10.56553/popets-2023-0013.
[9] Grabowska B., Seń M., Klisowska I. (2021). E-prescription in Poland - a preliminary report. 151-156. doi:10.15503/emet2020.151.156.
[10] Eysymontt, Małgorzata. (2022). The “mObywatel” application as a sign of the increase of informatisation of the Polish society – critical remarks on the practical applicability of the tool. Acta Iuridica Resoviensia. 38. 57-74. 10.15584/actaires.2022.3.4.
[11] Albesher AS. Reviewing the Usability of Web Authentication Procedures: Comparing the Current Procedures of 20 Websites. Sustainability. 2023; 15(14):11043. https://doi.org/10.3390/su151411043
[12] Natamiharja, Rudi. 2018. “A Case Study on Facebook Data Theft in Indonesia”. Fiat Justisia: Jurnal Ilmu Hukum 12 (3):206-23. https://doi.org/10.25041/fiatjustisia.v12no3.1312.
[13] Snehal Manohar Awale | Dr. Praveen Gupta "Awareness of Sim Swap Attack" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.995-997, URL: https://www.ijtsrd.com/papers/ijtsrd23982.pdf
[14] Novanema D. (2021). Short Message Services (SMS) Fraud Against Mobile Telephone Provider Consumer Review From Law Number 8 Of 1999 Concerning Consumer Protection. Journal of Law Science. 3. 36-43. 10.35335/jls.v3i1.1654.
[15] Reynolds J., Smith T., Reese K., Dickinson L., Ruoti S., Seamons K. (2018). A Tale of Two Studies: The Best and Worst of YubiKey Usability. 872-888. 10.1109/SP.2018.00067.