WYŻSZA SZKOŁA GOSPODARKI EUROREGIONALNEJ IM. ALCIDE DE GASPERI W JÓZEFOWIE

MONIKA NOWIKOWSKA

War Studies University, Warsaw, Poland

monika.nowikowska@gmail.com
ORCID: orcid.org/0000-0001-5166-8375
DOI: doi.org/10.13166/HR/HQNC8939

IDENTITY THEFT. PROTECTION OF PERSONAL DATA IN CYBERSPACE

Abstract

The aim of this article is to review main issues connected with the identity theft. The aim of the article is to review the main issues related to identity theft on the Internet. It points to the issue of scientific discourse within the key concepts: cyberspace and security, cybercrime, digital identity. The rapid development of information and communication technologies has increased impact on our everyday life. From the moment of apperance of the Internet and the smartphone, our identities have been recreated in the virtual world. From online banking to online shopping, there are many places that require personal information from us. Any unjustified use of information about our identity can have consequences for our savings and, in some cases, even for our lives. The extent of identity theft is constantly increasing. The more we use smartphones and the Internet for our daily needs, the more often our personal data is replicated. The number of victims of identity theft reported to the police is constantly increasing. This is an ongoing problem that is worrying and requires decisive action. This article discusses what is known about prevalence and cost of identity theft, describe the institutional framework in which identity thefts take place, and consider some of the main policy issues associated witch the problem.

Keywords: *personal data, cyberspace, cybercrime, identity theft, digital identity, phishing, vishing, smishing*

What is identity theft? Definition

Most people define *identity theft* as the theft of personal identifying information for some kind fraudulent purpose. It is generally recognized that identity theft is the illegal use of someone's personal data or information for individual gain. Also known as identity fraud, this type of theft can cost a victim time and money. Identity thieves target information like: names, dates of birth, drivers licenses, credit cards, bank information. Usually they use the stolen information to gain access to existing accounts and open new accounts. Identity theft can have financial consequences for the victim. The cost to the victim depends on when the crime is reported and how it occurred.

The terms *identity theft* and *identity fraud* describe the theft for farudulent purposes of personal information such as account number and another personal identifiresdsuch as a mother's maiden name[1]. It is possible to distinguish between identity thefts and identity fraud. Identity theft usually means stealing somebody's identity data. Identity fraud means using that data to open accounts. Identity theft covers a range of fraudulent acts. For example identity theft stealing ID data form bank account, passports, social security number, birth certificates, credit cards, driver's licenses. Identity fraud – using the stolen data to open accounts, make passports, use social security number, clone bank card, make fake driver's licenses. An identity thief might open an account in someone's name, file taxes on their behalf to receive the refund, or use their credit card number to make online purchases.

Identity theft is one of the fastest growing crime in cyberspace. Cyberspace has become a domain which pertains to many areas of human life[2]. Although still considered a *novum*, the term was first used in the 1980s by W. Gibson, who described it as follows: A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity (…). Lines of light ranged in the non-space of the mind, clusters and constellations of data[3]. Gibson pointed out some characteristic features of the environment:

[1] J. Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, *Berkeley Technology Law Journal* 2005, vol. 20, no. 1, p. 260, http://www.jstor.org/stable/24117505 (accessed: 17.08.2023).

[2] See more: K. Chałubińska-Jentkiewicz, *Cyberspace as an Area of Legal Regulation*, (in:) *Cybersecurity in Poland. Legal aspects*, K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński (eds.), Springer Cham 2021, p. 28; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, *Cybersecurity and Law* 2021; vol. 5(1), pp. 45-52; A. Mukerji, *The Need for an International Convention on Cyberspace*, *Horizons: Journal of International Relations and Sustainable Development* 2020, no. 16, pp. 198-209; D.R. Johnson, D. Post, *Law and Bodrers: The Rise of law in Cyberspace*, *Stanford Law Review* 1996, vol. 48, no. 5, pp. 1367-1402; G. Brown, K. Poellet, *The Customary International Law of Cyberspace*, *Strategic Studies Quarterly* 2012, vol. 6, no. 3, pp. 126-145.

[3] W. Gibson, *Neuromancer*, Katowice 2009, p. 59.

unlimited time and space, virtuality, complexity, and the collation of all resources in one huge database[4].

D. E. Denning defines cyberspace (its technical aspect) as the space of information created by all computer networks put together[5]. A similar definition is formulated by G. T. Rattray. *A physical domain which is the result of the creation of information systems and networks which enable mutual interactions through electronic communication*[6]. K. Chałubińska-Jentkiewicz idicates, that one of the defining features of cyberspace is its network character. It is very often associated with the information revolution, and is undoubtedly connected with the rapid growth of telecommunications and the popularisation of the Internet[7].

The crime of identity theft is regulated in the Polish legal system in Article 190a § 2 of the Criminal Code[8]. *Anyone who, impersonating another person, uses his image, other personal data or other data by means of which he is publicly identified, in order to cause him material or personal harm – shall be punished with imprisonment from 6 months to 8 years.*

Personal data as an object of identity theft

Object of protection of identity theft is personal data. The principles of personal data protection have been regulated under Polish law in several legal acts. The fundamental act which stipulates the protection of personal data is the Constitution of the Republic of Poland of 2 April 1997[9]. The right to personal data protection is a unique legal construct intended to protect the values

[4] E. Szczepaniuk, *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, Warszawa 2016, p. 69.

[5] D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, p. 24.

[6] G.T. Rattray, Wojna strategiczna w cyberprzestrzeni, Warszawa 2004, p. 30.

[7] K. Chałubińska-Jentkiewicz, *Cyberspace as an Area of Legal Regulation*, (in:) *Cybersecurity in Polan. Legal aspects*, K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński (eds.), Springer Cham 2021, p. 28; see also: K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, p. 60.

[8] The Act of 6 June 1997 the Penal (Journal of Law 2022 consolidated text, item 1138).

[9] (Journal of Law No. 78, item 483).

referred to in Article 47 of the Constitution of the Republic of Poland. The Constitution provides that *everyone is entitled to the legal protection of their private life, family life, honour, and reputation, as well as the right to decide on their personal life*. In the relevant literature, the individual's right to protect their personal data is called *information autonomy*[10].

The right to the protection of personal data is categorically associated with the right to privacy, recognising it as its unique form[11]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (The General Data Protection Regulation) (GDPR)[12], is also of fundamental importance in this regard. The issue of personal data is also governed by the Act of 10 May 2018[13] on personal data protection, which repealed several provisions of the former Act, and introduced new ones, which regulate, inter alia, the status of the President of the Personal Data Protection Office, as well as the procedure for initiating and conducting proceedings in connection with the infringement of personal data in the common courts, and the Act. The group of legislative acts regulating the principles of personal data processing in cyberspace also includes the Act on the National Cybersecurity System[14].

[10] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Artificial Intelligence v. Personal Data*, *Polish Political Science Yearbook*, vol. 51(3) (2022), pp. 185; see also: M. Safjan, *Ochrona danych osobowych – granice autonomii i informacji*, (in:) *Ochrona danych osobowych*, M. Wyrzykowski (ed.), Warsaw 1999, p. 9; M. Nowikowska, *Ochrona danych osobowych w dokumentach kontrolnych*, (in:) *Reforma ochrony danych osobowych. Cel, narzędzia, skutki*, J. Taczkowska-Olszewska, M. Nowikowska, & A. Brzostek (eds.), Poznań 2018, p. 165; M. Nowikowska, *Personal Data Protection in the Context of the Act on the National Cybersecurity System*, (in:) *Cybersecurity in Poland. Legal Aspects*, K. Chałubińska-Jentkiewicz, F. Radoniewicz, & T. Zieliński (eds.), Springer Cham 2022, p. 171; M. Nowikowska, *Protection of personal data in audit documents*, (in:) *Reform of protection of personal data system. Purposes, tools, effects*, J. Taczkowska-Olszewska, A. Brzostek, M. Nowikowska (eds.), Poznań 2018, p. 99.

[11] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Security v. Privacy – Legal Aspects*, Maribor 2021, pp. 7-9.

[12] (OJ L 119, 4.5.2016, pp. 1–88).

[13] The Act of 10 May 2018 on personal data protection (Journal of Law 2019 consolidated text, item 1781).

[14] The Act of 5 July 2018 on the National Cybersecurity System (Journal of Law 2023 consolidated text, item 913).

According to the GDPR, *personal data* refers to any information concerning an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an internet identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person.

It is irrelevant to the principles of personal-data processing (including the determination of the scope and type of obligations incumbent on processors and personal-data controllers) that the processing of the data occurs in cyberspace. In European Union, the GDPR protects personal data regardless of the technology used for processing that data – it is technology neutral and applies to both automated and manual processing, provided the data is organised under pre-defined criteria. It also does not matter how the data is stored – in an IT system, through video surveillance, or on paper. In all cases, personal data is subject to the protection requirements set out in the GDPR[15].

Personal data under GDPR is regarded as any personal information relating to a natural person. Whether private, professional, or part of public life, it is considered personal data[16]. This data includes anything that could be used to identify an individual, either directly or indirectly, even where that data is considered generalised[17]. Some categories are a person's name, identification numbers such as a social insurance number, ID number, age, location, physical, mental, genetic, sexual orientation, medical records, email, social, and more[18].

It should be emphasised that no comprehensive list of categories is given within the GDPR. The broad range of data sources becomes especially relevant

[15] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2021, p. 49.
[16] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Artificial Intelligence*…, s. 186.
[17] A. Gobeo, C. Flower, W.J. Buchanan, *GDPR and Cyber Security for Business Information System*, River Publishers 2018, p. 8.
[18] R. Walters, L. Trakman, B. Zeller, *Data Protection Law. A comparative Analysis of Asia-Pacific and European Approaches*, Springer Cham 2019, p. 55-56.

where profiling of data is used. Personal data covering all these categories can provide comprehensive insight into a given individual[19].

According to Article 1 of the GDPR, the EU legislators, when determining the adoption and application of uniform solutions for the processing of personal data in all EU Member States, pursue two equally important objectives: first, they protect the fundamental rights and freedoms of natural persons, and in particular, the right to the protection of their personal data; and second, they ensure the free transfer of personal data between Member States[20].

Identity theft – causes of the phenomenon

The use of services provided electronically, in addition to many benefits also involves some risks. The availability of technology and the dissemination of network solutions has led to a change in forms of crime. Modern cybernetic criminals often treat breaking the law on the web as another test of their skills or having fun. Identity theft is also known as forgery, embezzlement or seizure of identity[21].

Identity theft is a computer crime that affects more and more people. As many as 300 000 cases related to this problem were recorded in 2023 in US (there are no statistics on this subject in Poland). Statistics indicate: *Almost one third of Americans have been a victim of identity theft. Over 300,000 Americans fall victim to phishing/vishing/smishing attacks yearly. Every year there are more than 50,000 individual personal data breaches in the US. Identity theft victims in the US are most commonly aged between 30-39 years old. Americans are statistically likely to know a victim of identity theft*[22]. According to the Federal Bureau of Investigation's (FBI) 2021 Internet Crime Report, the most common type of cybercrime in the US is phishing/vishing/smishing – all of which involve stealing users' personal data.

[19] P. Voigt, A. Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer Cham 2017, p. 11.
[20] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Artificial Intelligence*…, p. 186.
[21] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Security v. Privacy*…, p. 57.
[22] https://30+ Identity Theft Statistics for 2023 (www.explodingtopics.com) (access: 23.08.2023).

Identity theft generally occurs in three stages: acquisition, use, and discovery. The crime may begin with a lost or stolen wallet, credit card information stolen during a transaction, a data breach, a computer virus, phishing, or a scam.

The crime of identity theft has been expressed in Art. 190 a § 2 of the Penal Code, according to which identity theft is impersonating another person, thereby using his or her image or other personal data to cause him personal or material damage. Identity theft is all actions taken to obtain real data from real people. These data are obtained with the use of various technical and ICT means using social engineering[23]. In 2020, phishing campaigns, i.e. attacks using social engineering, increased significantly.

Social engineering is a tool used by both cybercriminals and the services of other countries. These types of attacks use images of well-known telecommunications operators or Internet providers, as well as other events of current media interest. And so, last year, a popular motive for attacks was the COVID pandemic (impersonation of a page with a map of the spread of the virus, sending messages allegedly containing the official WHO announcement, etc.)[24]. A criminal using computer programs (e.g. Sniffier), which are specialized in analyzing and receiving data, eavesdrops and has the ability to reach all private data. There are two types of information acquisition: one that stores data in files and interactive, which allows you to view the transmitted data on a regular basis[25].

According to the Federal Bureau of Investigation's Internet Crime Report, the most common type of cybercrime in the US is phishing/vishing/smishing – they all involve the theft of users' personal information, it is worth discussing what phishing/vishing/smishing is. What is the difference?

[23] K. Chałubińska-Jentkiewicz, M. Karpiuk, Prawo nowych technologii, Warszawa 2015, p. 245.
[24] *More and more threats in cyberspace. ABW Report* (Internal Security Agency in Poland) http://Coraz więcej zagrożeń w cyberprzestrzeni. Raport ABW – Służby specjalne – Portal Gov.pl (www.gov.pl)) (access: 23.08.2023).
[25] K. Chałubińska-Jentkiewicz, M. Karpiuk, op.cit., p. 248.

Phishing/vishing/smishing

Phishing describes *a sheme when a cybercriminal sends a fake email message requesting the recipient to click on a link or respond with requested personal information. The email address of the sender often apperas to be legitimate address, such as that of a bank or other organizationwith access to personal information*[26]. The play is simple: you receive a message via email, SMS, or instant, complete with a link you are supposed to click. So it might be for a bank, credit card, or a dating site in the case of instant messaging. Following the link takes you to an actual copy (a spoof) of the related website. You're asked to log in or confirm some details. These are recorded by scammers and used to steal your identity. Perhaps the number one reason behind identity theft is the double-pronged attack of phishing and spoofing websites.

Phishing is generally associated with fraudulent emails, whereby an unsuspecting victim is targeted by an email claiming to be from a trusted source but is actually seeking to acquire sensitive information or inject malware into the victim's systems[27].

Phishing is a type of social engineering attack, a term describing the psychological manipulation of someone into doing or revealing certain things. These attack methods are usually quite popular among hackers, as they can be set up with relative ease and rely on human error. Humans are notoriously easier to trick than breaking through system or network defences. Social engineering and human error, rather than technology, make up 95% of successful cyber attacts[28]. Many social engineering schemes do not necessarily require much technical savvy and, in general, may be successful regardless of how smart technically the scammer is[29]. Phishing attempts are getting more and more

[26] T.S. Reed, *Cybercrime And Technology Losses: Claims And Potential Insurance Coverage For Modern Cyber Risks*, *Tort Trial & Insurance Practice Law Journal* 2019, vol. 54, no. 1, p. 156-157. JSTOR, https://www.jstor.org/stable/27008150 (accessed 24.08.2023).

[27] *Phishing, Vishing and Smishing: What's the Difference?* (www.cybertecsecurity.com) (accessed: 24.08.2023).

[28] A.S. Malish, *Navigating Cyber Coverages for Modern Day Cybercrimes*, *Tort Trial & Insurance Practice Law Journal* 2019, vol. 54, no. 3, p. 916. JSTOR, https://www.jstor.org/stable/27008183 (accessed: 24.08.2023).

[29] Ibidem, p. 917.

sophisticated, and when you consider that the recipient will often be a busy employee trying to handle lots of different things at once, it is understandable that so many manage to get duped by these sneaky emails. Hackers are well versed in convincingly disguising themselves as a company or individual you would normally trust, particularly when they already have certain pieces of information about you[30]. The same technique can also be executed by phone, called *vishing*.

Vishing follows similar schemes to phishing accomplished through phone calls. Just like with phishing emails, phone scammers will often call up claiming to be from a legitimate company. They may claim to be a bank accusing you of fraud and telling you that you need to give them your details to clear it[31]. When it is a phone call, it can be even more stressful for the person on the receiving end, especially if they are being told they have done something wrong. In moments of heightened emotion like that, however, we are even more likely to make mistakes – this is what the scammer is hoping for. Typical vishing scams will involve a hacker claiming to be from somewhere like your bank. This person usually telling you there is an issue with your account . They might need you to prove your account by providing login credentials, but this should always be the first red flag. Some may even offer some information they already have on you to show they are legit. How do vishing hackers get our numbers? Well, hackers can find phone numbers in a variety of ways but the best place to hunt for data is the Dark Web. An absolute treasure trove of data, hackers can grab all kinds of personal information, including phone numbers.

Smishing follows the same *modus operandi* as phishing and vishing[32]. When a text message, or SMS, is sent to someone requesting personal or financial information this is known as smishing. This is a popular entry point for hackers and scammers. It's often easier for a hacker to find phone numbers than emails too which is why smishing attacks are rising. It should be emphasized that while most people are aware of the dangers of phishing emails and usually know what to look out for, it does not tend to be expected as much

[30] *Phishing, Vishing…*, (accessed: 24.08.2023).
[31] Ibidem.
[32] A.S. Malish, op.cit., p. 916.

on your phone, so it can be easier to miss the signs. If we consider how many mobile phone users are often on the go and in a rush, we can see how easy it must be for someone to click on a fraudulent text when it comes in before we have even had a chance to think. Just like with phishing, hackers targeting someone's mobile device may be looking to get someone to install malware or stealing personal information by tricking them to input information on a fake website and giving it to the hacker. As more and more business employees use their own mobile devices at work, smishing can be as much a business threat as it is to an individual consumer, so it is important to know how to spot it and what to do about it[33].

Smishing and and *vishing* are similar schemes accomplished through SMS texting and phone calls where the criminals send text messages or call potential victims and pretend to be someone with legitimate access to the victims' personal information. Victims who respond then provide their personal information[34].

Effects of identity theft

Identity theft and identity fraud refer to crimes in which someone wrongfully obtains and uses another individual's personal data in a way that involves fraud or deception, often for economic gain. Identity theft has profound consequences for its victims. They can have their bank accounts wiped out, credit histories ruined, and jobs and valuable possessions taken away. Some victims have even been arrested for crimes they did not commit[35]. It shows that identity theft can have financial consequences for the victim and tThe cost to the victim depends on when the crime is reported and how it occurred.

Identity theft's negative impacts often involve finances, but there can be other consequences, as well, including an emotional, social and physical

[33] *Phishing, Vishing*…, (accessed: 24.08.2023).

[34] T. Scott Reed, op.cit., p. 157.

[35] *U.S. Department of Justice. Office of Justice Programs: Identity Theft*, Octber 2011, https://www.ojp.gov/sites/g/files/xyckuh241/files/archives/factsheets/ojpfs_idtheft.html#:~:text=Identity%20theft%20has%20profound%20consequences,crimes%20they%20did%20not%20commit (accessed: 25.08.2023).

toll. For example, if a thief commits a crime and provides our name to police, something known as *criminal identity theft* and authorities arrest us as a result, we can imagine the resulting stress, as well as disruption to our life until we are able to resolve the situation.

We can distinguish the four different ways victims can be affected by identity theft: (1) financially, (2) emotionally, (3) socially and (4) physically.

Ad 1) Financial tool. The financial hardships that may be caused by identity theft can last for months or years after our personal information is exposed. Through account takeover, identity thieves can also take over investment and other financial accounts, the impacts of which could affect on retirement or mortgage. Thieves may not use information for months or even years, waiting for a time when we may not be as attentive to the risk. Thieves can also sell personal information on the dark web[36].

Ad 2) Emotional tool. The next impact of having our identity stolen is the emotional toll that can accompany it. Identity theft is often a faceless crime that can trigger a host of emotional reactions. The first feeling that victims may experience is anger. But after the initial shock, other challenging and long-term emotions may come into play. A 2016 Identity Theft Resource Center[37] (ITCR) survey of identity theft victims indicated emotional suffering caused by identity theft, such as:

- 74 % of respondents reported feeling stressed;
- 69 percent reported feelings of fear related to personal financial safety;
- 60 percent reported anxiety;
- 42 percent reported fearing for the financial security of family members;
- 8 percent reported feeling suicidal.

Ad 3) Physical toll. Identity theft issues could also manifest as physical symptoms. In its 2016 ITRC survey, 23 percent of ID theft victims surveyed

[36] A.G. Johansen, *4 Lasting Effects of Identity Theft*, in: https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft (accessed: 25.08.2023).

[37] The ITRC is a non-profit organization established to minimize risk and mitigate the impact of identity compromise, established in 1999. The ITRC has conducted surveys and produced publications since 2003 on topics including the emotional and psychological impact of identity theft, the victim aftermath of data breaches, social media habits, impact on foster youth, cyberattack trends, and more. See: www.idtheftcentre.org (accessed: 25.08.2023).

feared for their physical safety, 39 % experienced an inability to focus, 29 % reported new physical illnesses such as body pain, sweating, and heart and stomach issues, 41 % had sleep issues, and 10 % could not go to work due to resulting physical issues. For example, if someone is using your name to commit crimes and law enforcement arrests you, that's a highly stressful event. And before you clear your name, your arrest record may still pop up on background checks, affecting everything from employment to your housing options down the road.

Ad 4) Social toll. Identity theft can also have a social impact. Social media accounts are being hijacked more and more often. Victims who reported being a victim of a social media account takeover: (85%) of victims had an Instagram the account was compromised; (25%) victims reported a Facebook account breach; (48%) of victims clicked on the link they clicked presumed to have come from a friend; (51%) lost personal funds or sales[38].

Protecting against phishing/vishing/ smishing attacks

The majority of cyber attacks are successful because they use social trickery, often playing with emotions, to catch someone out, and phishing, smishing and vishing are perfect examples of this. Spear phishing relies on social engineering to trick individuals into revealing sensitive information or downloading malicious software rather than hacking into a system vulnerability by force[39]. As Michael Bossettanotes: *social media platforms, as high-trust environments typically accessed from a mobile device for personal entertainment or networking, are highly conducive waters for spear phishing. Moreover, the wealth of public information available on social media can be exploited by*

[38] ITRC_2022-Annual-Report_Final-1.pdf (www.idtheftcenter.org) (accessed: 25.08.2023).

[39] M. Bosetta, *The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy*. *Journal of International Affairs* 2018, vol. 71, no. 1.5, p. 97. JSTOR, https://www.jstor.org/stable/26508123 (accessed: 24.08.2023).

threat actors to devise sophisticated (and automated) spear phishing campaigns that target government and military personel[40].

The best way to stay safe is to be aware of these different kinds of attacks, particularly as they evolve, and know how to respond to them properly. The most effective response is to simply ignore anything that does not quite sit right and always avoid handing over any personal information until you have officially confirmed the legitimacy of that contact. Generally, if we do not recognise the sender of a text, we should never be replying to it. Banks should never request information over text or tell us to update account details. If there is a link, it is likely to be fraudulent and we should directly contact our bank to alert them.

We can list the following actions to protect our online identity:

- keep your cards in a secure location;
- use strong passwords and two-factor identification when possible while using online accounts;
- do not use the same password for every account;
- check your credit score and credit reports frequently;
- do not enter your bank information or credit card number on sites that you do not recognize;
- use shredders to destroy personal documents;
- set up *suspicious activity* alerts on your bank accounts

Prevetning identity theft mean *verifying that buyers are who they claim to be*[41]. Sellers and creditors deploy a wide wariety of techniques to perform this task. Authentication techniques can be classified into three categories:

a. *token-based authentication* (based on a phisical obcject in the possession of the user);
b. *knowledge-based authentication* (based on a possession of information that only the individual would be expected to know;

[40] Ibidem, p. 97.

[41] K.B. Anderson, E. Durbin, M.A. Salinger, *Identity Theft*, *The Journal of Economic Perspectives* 2008, vol. 22, no. 2, p. 183. JSTOR, http://www.jstor.org/stable/27648247.P.183 (accessed: 17.08.2023).

c. *biometrics*, based on some physical characteristic of the person himself, such as a way of signing documents[42].

For example a credit card payment system relies on a token-based aproach for in-store transaction, where the token is the card itself. For transactions where the buyer is not physically present merchants rely more hevily on knowledge-based authentication by verifying that the address reported by the cardholder matches an address on filewith the card issuer. One type of token-based authentication used on lin eis that based on the card verification numer, printed on the back of a card, which is meant to confirm that the buyer is at least in possession of the card.

To verify identity when creating a bank account, lenders rely on knowledge based authentication. For accounts that are opened in person, the creditor may require photo identification or other physical proof of identity. For accounts opened online, over the phone, or by email, no token-based method is available. In such cases the lender generally relies on the borrower's knowledge od birth date, personal numer, ID numer, address, Social Security number, and other personal information, comparing information provided by the borrower to that in the data base of a third party *data broker*[43].

How to report identity theft. There are multiple ways to take action if we suspect private information related to our identity has been compromised. First of all, we should document the theft. Register when and where you last used your debit or credit card. We should register and check when and where we last used our debit or credit card. We can document fraudulent charges. If we receive a bill for a credit card we do not own, we do not discard it. We should also contact our bank for financial fraud. It is important to freeze aour accounts as soon as you we believe they have been compromised. A bank may place an alert on our account and send us a new card if ours has been stolen. The second important step is to notify the Police authorities.

[42] Ibidem, p. 183.
[43] Ibidem, p. 184.

Summary

Identity theft happens when someone's personal information is accessed and used for fraudulent purposes, such as financial crime or impersonation. Our identity can be abused in many different ways, and the harm can be lasting and significant. In today's cyber-focused world, the Internet is one of the way identity thieves can gain access to personal information like passwords to email and social media accounts. Whether we rely on social media for our profession or use it to stay in touch with friends and family, hackers could damage our reputation or put our job on the line by using current accounts, and even creating new, fraudulent accounts, in which they post while pretending to be us.

A criminal may access financial data, apply for loans or credit cards in someone else's name, take over bank accounts or credit cards, or sell the information on the dark web. However, there are simple ways to protect your identity from theft and misuse, lowering your risk of long-term damage. Identity theft can have many lasting negative effects on its victims. One of the best things to do is act quickly to limit its impac and seek help. Depending on the type of ID theft, this can involve reaching out to a variety of entities, including banks and law enforcement.

References

Anderson K.B., Durbin E., Salinger M.A., *Identity Theft*, *The Journal of Economic Perspectives* 2008, vol. 22, no. 2

Bosetta M., *The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy*, *Journal of International Affairs* 2018, vol. 71, no. 1.5

Brown G., Poellet K., *The Customary International Law of Cyberspace*, *Strategic Studies Quarterly* 2012, vol. 6, no. 3

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019

Chałubińska-Jentkiewicz K., *Cyberspace as an Area of Legal Regulation*, (in:) *Cybersecurity in Poland. Legal aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Springer Cham 2021

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii*, Warszawa 2015

Chałubińska-Jentkiewicz K., Nowikowska M., *Artificial Intelligence v. Personal Data*, *Polish Political Science Yearbook* 2022, vol. 51(3)

Chałubińska-Jentkiewicz K., Nowikowska M., *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2021
Chałubińska-Jentkiewicz K., Nowikowska M., *Security v. Privacy – Legal Aspects*, Maribor 2021
Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002
Gibson W., *Neuromancer*, Katowice 2009
Gobeo A., Flower C., Buchanan W.J., *GDPR and Cyber Security for Business Information System*, River Publishers 2018
Johnson D.R., Post D., *Law and Bodrers: The Rise of law in Cyberspace*, *Stanford Law Review* 1996, vol. 48, no. 5
Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, *Cybersecurity and Law* 2021, vol. 5(1)
Lynch J., *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, *Berkeley Technology Law Journal* 2005, vol. 20, no. 1
Malish A.S., *Navigating Cyber Coverages for Modern Day Cybercrimes*, *Tort Trial & Insurance Practice Law Journal* 2019, vol. 54, no. 3
Mukerji A., *The Need for an International Convention on Cyberspace*, *Horizons: Journal of International Relations and Sustainable Development* 2020, no. 16
Nowikowska M., *Ochrona danych osobowych w dokumentach kontrolnych*, (in:) *Reforma ochrony danych osobowych. Cel, narzędzia, skutki*, J. Taczkowska-Olszewska, M. Nowikowska, & A. Brzostek (eds.), Poznań 2018
Nowikowska M., *Protection of personal data in audit documents*, (in:) *Reform of protection of personal data system. Purposes, tools, effects*, J. Taczkowska-Olszewska, A. Brzostek, M. Nowikowska (eds.), Poznań 2018
Nowikowska M., *Personal Data Protection in the Context of the Act on the National Cybersecurity System*, (in:) *Cybersecurity in Poland. Legal Aspects*, K. Chałubińska-Jentkiewicz, F. Radoniewicz, & T. Zieliński (eds.), Springer Cham 2022
Rattray G.T., *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004
Reed T.S., *Cybercrime And Technology Losses: Claims And Potential Insurance Coverage For Modern Cyber Risks*, *Tort Trial & Insurance Practice Law Journal* 2019, vol. 54, no. 1
Safjan M., *Ochrona danych osobowych – granice autonomii i informacji*, (in:) *Ochrona danych osobowych*, M. Wyrzykowski (ed.), Warsaw 1999
Szczepaniuk E., *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, Warszawa 2016
Voigt P., Bussche A., *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer Cham 2017
Walters R., Trakman L., Zeller B., *Data Protection Law. A comparative Analysis of Asia-Pacific and European Approaches*, Springer Cham 2019