The change in the technological landscape resulting from the widespread availability of mobile devices and with it the use of social media has largely determined the way many societies live in the 21st century. Social media, as a result of the creation of social interactions, differentiate themselves in significant ways from the dominant forms of mass media of the previous century. They allow people to generate content themselves and make it available to a wide audience. People are no longer condemned to just watch and admire popular people but can create themselves in front of an audience through inexpensive and accessible technologies. In other words, the media user is no longer simply a consumer of content but is also a producer of content. One consequence of this is that they seek to popularise themselves in the digital space through the exposure and promotion of private


content. Undoubtedly, this possibility (of sharing and talking about oneself in front of a ‘global audience’), is one of the main reasons for many users’ presence in cyberspace.

A report compiled by the EU Cyber Security Agency (ENISA) in 2022 shows that the vast majority of Europeans have access to a smartphone and a home computer (95% and 88%, respectively) while 82% reported being online several times a day or almost continuously. The same number of people admitted to constantly using social networks such as Facebook, Instagram, Snapchat, Twitter, Tumblr, and Tinder. An important factor in the dynamics of this phenomenon is the experience of the COVID-19 pandemic. It has contributed to the rise in popularity of dating sites and other social media platforms, among others. It is worth mentioning that the phenomenon is also influenced by the change in social judgement regarding online networking and the emergence of various free or low-cost dating apps. The prevalence of such practices should not come as a surprise, given that popular culture is also increasingly focused on sexual self-expression. Thus, it can be argued that irresponsible participation in social media can entail a number of negative consequences, one of which is vulnerability to a wider range of criminal victimisation.

This is illustrated by certain aspects of Facebook, the world’s most popular social network (with more than 800 million active users), which allows anyone aged 13 or over to create an account. Despite this restriction, there are many children below the indicated age range who are also users of this medium. At the beginning of 2022, 87% of the global population (we are talking about everyone — regardless of age) were regular users of this social network.

Following these figures, there is concern that a large number of young people are engaging in online interactions with unknown people without any parental control. Concerns are therefore raised that social networking sites may provide cybercriminals with an easy way to commit fraud.

### A research approach to the phenomenon of cyber fraud

This paper discusses the logic behind the behaviour of an online fraudster in the context of establishing intimate relationships. The paper presents the manipulation process, based on two different, most commonly used models for committing the crime. In order to identify and describe

---


the relevant factors to help better understand the phenomenon of cyber fraud, a survey was conducted on the forums of the most popular social networks between July 2021 and July 2022. 352 submissions were received from people who, based on their responses, could be classified as victims of cybercriminals. The information obtained in this way provided a better understanding of a rather new and hitherto underdeveloped area of research. This has made it possible to expand the knowledge in the field of cyber threats to include issues related to the harmful actions of cyber criminals.

Manipulation techniques have been developed and identified based on responses to surveys that were posted on popular social networking sites and based on an interview with Internet chat room participants in Poland. As a result, the data includes what individual complainants were able to remember and describe from their experiences. However, this mechanism of mapping cybercrime is subjective in nature and may affect the accuracy and form of interpretation of events. Despite these limitations, the acquired dataset provided a basis for analysing how cybercrimes are carried out. The data collected can provide unique insights into cybercrimes suffered by social media users who chose to share their experience.

The research survey was anonymous and respondents declared that they were at least 18 years old. All survey participants consented to their responses being shared for research purposes. This resulted in an anonymised sheet with detailed data. Each response contains the following information: demographics of the complainant (gender, age), details of the scam (how the content was manipulated and scammed) and any losses suffered (amount, sensitive data lost, reputation). As an aside, it should be noted that the statistical results obtained should be treated with caution, as they are likely to be an underestimate of the actual number of cyber frauds taking place.

The analysis conducted in this paper aims to answer the following research questions:

1. How does the extortion of specific content occur in the context of establishing intimate relationships?
2. Are there patterns of criminal behaviour as to the phishing of private content.
3. What is the profile of those susceptible to cyber fraud?

It was intended that the data obtained would provide a better understanding of the mechanism of digital fraud and how cybercrime may evolve in the future and how it can be countered. The negative social phenomena arising from the dynamic process of digitisation are particularly evident in the area of numerous scientific studies. Cybercrimes are in-

---

creasingly becoming an area of study for researchers interested in online victimisation. They are most often the subject of analyses linked to mental health consequences such as psychosocial maladjustment, mental disorders, antisocial behaviour, suicidal thoughts, self-harm, anxiety, and depression.\(^9\) It can be seen that cases of the mechanism of cyber fraud involving phishing for photos, recordings or other private data or money are reflected in the scientific literature.\(^10\) The present work fits into the thematic scope of both these strands, while at the same time complementing existing research with a description of the manipulation methods used by fraudsters.

**Selected aspects of cyber fraud**

Social media have become an integral part of everyday life. The use of social networks and applications has rapidly become popular, and it is no longer unusual to establish, maintain, share and build social relationships using this medium. It can therefore be said that technology has redefined and transformed the meaning of making friends, thus creating many convenient situations for committing cyber fraud.\(^11\) This threat is illustrated by data from 2019, when 2.19 billion accounts on the Facebook platform were disabled as fake.\(^12\) Many people are unaware of the risks in the face of digital developments.\(^13\) For example, engaging in risky online

---


behaviour can jeopardise personal safety and increase the risk of unwanted contact from criminals.\textsuperscript{14}

The phishing for intimate content most often takes place via social networks (e.g. Facebook, Instagram, Twitter), instant messaging (e.g. Messenger, Snapchat, Whatsapp) and chat rooms including video (e.g. Skype, Google Hangouts). The phenomenon usually culminates in blackmail and demands for sexually explicit online activities, e.g. the creation of pornographic material and/or actual sexual contact, while threatening to publicly disclose intimate photos or videos if the perpetrator does not comply with the demands.\textsuperscript{15}

Fraudsters may create a false profile using images belonging to an attractive person with a high social status in order to deceive victims and thus obtain financial gain.\textsuperscript{16} The image thus presented makes many recipients want to be included in the group of friends of the figure so created.\textsuperscript{17} Some fraudsters make the additional effort of building a digital social environment to make such a profile credible in the public perception.\textsuperscript{18}

The moment of deconfi dence for fraudsters comes when they are about to take part in a videoconference or attend a meeting in person. Most often, in such a situation, they withdraw at the last moment and break off the acquaintance.

Digital fraud based on an insincere relationship can include lying, telling half-truths, exaggerating, withholding information, cheating, stealing or concealing behaviour from a prospective partner. This is due to the nature of cyberspace, which makes it quite easy to create false profiles, allowing, for example, adults to present themselves online as children in order to better engage minors in communication. All these factors


\textsuperscript{17} Lovelock M, Catching a catfish: Constructing the “Good” social media user in reality Television, Television & New Media 2017, No. 18(3), pp. 203–217.

significantly increase the ability of sexual predators to identify and target children on social networks.\(^{19}\) Such manipulation can lead to serious consequences in the real world, including forms of sexual assault or suicide. Such experiences often expose victims to significant emotional and psychological suffering, causing fear and anxiety.

**Manipulation methods used by cyber fraudsters**

The sequence of behaviours is important for understanding the manipulation mechanism of an online fraudster. The pattern of contacting the victim and the subsequent scenario of the conversation may vary. However, from the many observed cases on the Internet, two most typical behaviours and manipulation techniques of such fraudsters can be singled out.

The first type is usually a user who impersonates another person out of curiosity and disapproval of a particular group of users with whom he or she wishes to establish contact. They are also unaware of their apparent anonymity and the legal consequences.

During a conversation, he or she is subject to very violent emotions, ranging from optimism and satisfaction to verbal aggression. Usually, the dialogue does not resemble a normal conversation in terms of the content and number of sentences. In other words, the behaviour resembles a person under the influence of alcohol, emotionally and illogically formulating statements. They are also usually sentences in a harassing and demanding form. Statements are constructed as demands and expectations are to be fulfilled immediately, such as sending a photo, providing an address or the name of a school or workplace. The advantage in terms of the number of articulated messages is on the side of the scammer. He or she very often ends their sentences with so-called emoticons, which are used excessively in the statements, or the ‘emoticons’ themselves are used instead.

Characteristically, the first to take the initiative for a conversation, asking questions that usually relate to the person’s home address, school name, university, place of work, *i.e.* questions that will allow the person to be located and identified. Unlike his or her victim, the scammer does not have an e-mail name referring to the user’s nickname, and often does not have a profile on Facebook or other alternative social networks.

A fraudster using a fake profile to manipulate other users sends image files of small size, usually measured in kilobytes. The names of the images consist of chaotic and random numbers and letters. The person depicted in the images usually presents with an identical hairstyle, clothing and in the same place and circumstances. There is an indiscernible change to seasons, places, or events. It is difficult to see other life situations

---

in which this person would be involved. In summary, the fraudster usually has a limited stock of photographs, down to just a few, and almost identical. Often, the person depicted in the photo looks provocative.

Usually, the scammer also reveals a random background, i.e. the furnishings of the flat and the surroundings of the person in the photo. Inscriptions on objects (cigarettes, bottles, labels, book covers on a shelf) in a foreign language may indicate an attempt at fraud.

The second type of fraudster – the professional one, who usually already has several victims in his or her ‘track record’ – is the exact opposite of the first type of fraudster, characterised above all by discipline and composure. He or she is very well equipped for this purpose, being a combination of a specialist in computer science, computer graphics and psychology.

These skills are put to full use. The fraudster prepares him/herself in almost every detail, creates their profile with great care from the start; their image profile, personality profile and biography are all refined. He or she is also very emotionally stable. At the beginning of an acquaintance, they ‘help’ their victim. They exploit people’s weaknesses, so that, paradoxically, the ‘help’ often consists of acceptance and listening to confidences. The unsuspecting person sees support and understanding in such relationships. He or she gives what the victim lacks on a daily basis, so most often it is acceptance, warmth, and understanding. They are balanced and patient, and through conversations, learn about the weaknesses of their victim. And through daily and constant contact, the conversation with the scammer becomes a regular part of the victim’s life. An emotional dependence is thus born, the person becomes more and more attached to his or her interlocutor and is increasingly anxious to maintain contact. The fraudster, sensing this state of commitment on the part of the victim, begins to articulate demands. A second stage of manipulation takes place, involving blackmailing them into breaking contact. In this situation, the victim, out of fear of losing their only friend, is prepared to make sacrifices.

Such a swindler, although well prepared to manipulate, also has weaknesses. However, detecting them depends above all on the vigilance of the user him/herself and of third parties, i.e. in the case of a child, parents or older siblings.

Great caution and prudence are required in online relationships and in making acquaintances. Above all, attention should be paid to the manner of conversation, language and style, as well as the choice of words. Obviously, a university-educated person claiming to be the president of a corporation will not write with mistakes, and his or her choice of terms will show a broad vocabulary, eloquence and a certain amount of reading.

Of course, specific knowledge is needed to detect an impersonator. A fraudster pretending to be a child, such as a middle school student in second grade, will often make mistakes, such as not knowing the applicable reading material. Similarly, he or she will not use words and terms typical of youth fashion. The language and terms used by minors are very
dynamic. If the term ‘jazzy’ was used a year ago, it is no longer fashionable in a year’s time and is replaced by ‘mega’ or ‘but a firecracker’.

However, the true art lies in posing subtle questions to a person suspected of deception, in such a way that they are seamlessly integrated into the dialogue, stemming from the logic of the conversation and the context of the subject. Such a conversation serves as a kind of credibility test for the interlocutor. For instance, if a parent, who is witnessing their child’s conversation with an unfamiliar user in a chat, asks the child for their opinion on school readings that are not appropriate for a certain age, and the individual on the other side of the screen affirms the false claim about the obligation to read such material, then there is a high probability that this individual is not actually who they claim to be.

It is important at this point to pay attention to the reaction time involved in answering, if the conversation continues smoothly and statements on both sides occur rhythmically every two to three seconds, then if there is a problem with the answer when the ‘test comment’ is entered, there are reasons to interpret this as a typical escape from the subject. If, on the other hand, the response only appears after a few minutes, one may become suspicious that the person was surprised by the comment and was searching for the answer to the question asked online during this time.

The check technique can, of course, be applied to other topics, but it is important to be able to introduce the check question into the dialogue in a natural way so the other party does not become suspicious. A user’s correct response to a photo they receive of a beautiful woman should be based on a comment such as, ‘You came out beautiful in the photo, I think you used an “eyelash curler”’. Of course, the scammer will not know what this is, unlike any adolescent girl or woman. Such a scammer will either give an incorrect or evasive answer, or just take time to find out what the device is and what it is used for.

Some perpetrators manage to evade detection because victims often refrain from reporting or publicising such incidents out of fear of experiencing embarrassment, both personally and within their families, and due to the potential moral consequences. A large number of scammed people are therefore left at the mercy of scammers.

Three groups of people are most vulnerable to fraud. The first is men seeking attractive experiences, sensations, looking for an alternative to everyday life, bored with their current lives, usually on social and dating sites. The second group is adolescents, driven by curiosity and puberty and the strong emotions associated with this. The third group is the LGBT community looking for life partners. Each of these groups remains anonymous and most cases go undetected due to victims’ fear of embarrassment as well as social harassment.

The many forms of cyberbullying leave those who experience it feeling helpless and despairing. This violence is exacerbated when the victim does not find people in the world around them capable of helping them to overcome the difficulties they face. Action is also needed here on the part of public institutions that can minimise cyber threats effectively enough.
Conclusions of the research

A number of factors that co-occurred with the phenomenon of cyber-bullying were noted during the interview process, such as environmental factors (e.g. portrayal of violence in the media, peer pressure), personal factors (e.g. socialisation, family upbringing) and personality traits (e.g. lack of moral commitment, impulsivity, narcissism). 20

Research shows that there is a correlation between age and susceptibility to fraud. The younger the users of social networks, the more likely they are to be manipulated by cybercriminals. For many people, the virtual world is an opportunity for personal revenge against a hated, hostile reality. In addition, marginalised and socially unaccepted individuals are more likely to engage in risky online behaviour, including publishing and sharing personal information, photos and videos, or adding strangers as friends.

It is important to note that every interaction between offender and victim is in some way unique and tailored by the offender to make the most of the victim’s identified weakness or vulnerability and situation. Thus, not every victim will experience every stage, which may not necessarily be linear in the offender’s execution, as presented in the research. What is consistent is that offenders are violent towards victims and will not back down from anything to manipulate them and force them to comply with their demands.

The analysis showed that the profile of victims is an important factor influencing the effectiveness of cyber fraud. Online interactions are usually motivated by the expectation of a face-to-face encounter. Social media is, in a way, responding to these needs. They offer the possibility to use location-based features (since most users look for partners who live no more than 25–30 km away from them) and to identify specific interests or social groups (e.g. sexual minorities) without fear of social ostracism.

Curiosity, boredom, the desire for entertainment, a certain kind of relaxation, as well as a break from reality, and the search for one’s own ideals, which are difficult to find in reality, also play a large role. A certain kind of addiction to cyber-communication cannot be overlooked as well, which significantly influences the presence on such Internet portals.

Observations of the behaviour of adult instant messaging users show that women are more likely to be scammed than men. On the other hand, with regard to age, older Internet users are much more likely to be cautious than younger ones.

Security measures are slowly being strengthened in cyberspace to protect users from falling into the clutches of scammers. But they are the

---

exception rather than the rule. Many social network administrators are reluctant to undertake detailed scrutiny because such measures may discourage potential customers. But pressure on them to take such steps is likely to increase. Other portals, on the other hand, are introducing charges for certain additional services, such as using algorithms to determine compatibility between people per subscription. Sites that require people to pay for their services and complete detailed surveys are more likely to attract those users who are serious about finding love. This is, of course, an effective way to demonstrate seriousness of intent, but is certainly not sufficient protection against online scammers and sex offenders.

Despite all this, users should still approach online contacts with a healthy dose of scepticism. Portals with potential partners are often much smaller than the numbers of registered users show. As it turns out, only a small percentage – even out of several thousand people – are ‘active’, which in practice means that profile owners have logged in at least once in the last three months. What’s more, some services allow people to be contacted on condition of payment, so naturally the number of such users is shrinking.

It seems that one of the reasons for such phenomena is the modern consumer culture dominated by human carnality. With the enormous technological progress, a far-reaching erosion of human values is taking place. Watching pornographic content and live sex chat rooms are wreaking havoc on the minds of not only young people. The infantilisation of adults on the Internet is also noticeable. In order to prevent such harmful activities in cyberspace, it is worth remembering a few rules, the first of which is to choose complex passwords for online accounts. In addition, the password must remain private and confidential. At the end of each use, remember to disconnect from the session, including on mobile phones. The second rule is to set the account as private so no one can access it. The third is to avoid giving out too much personal information (e.g. phone number, religion, relationship). These are all details that potential stalkers can use against the person of their choice. The fourth rule is to refrain from taking or publishing suggestive or intimate photos or videos. It is also imprudent behaviour to talk about one’s joys and sorrows. The author of this type of content is not fully aware of the size of the audience. Some images or information may be misinterpreted or deliberately misused.

In the digital age, manipulation, lies and deception have become even more common and easy. It is one of the fastest-growing problems in life today. This is a very worrying phenomenon, especially as the above content brings with it violence and brutality in human behaviour.

Summary

The cyber threats described in the article are crucial in determining how educational institutions, law enforcement agencies and NGOs can take action as a basis for the process of strengthening the level of cyber
security. Examining the nature of cyber threats can help prevent them and contribute to more effective cyber monitoring efforts. A key area for this topic is the analysis of phishing tactics for specific content (by stealing or creating a false identity). Understanding it can help provide the needed information to assist both users and social network creators and moderators in countering cyber threats.

In conclusion, the research findings presented in the paper may prompt reflection on cyber security and may also encourage pro-social online behaviour and help users to improve their online competence. The content of the paper can also be a resource for school principals, teachers and social workers, who are increasingly implementing a comprehensive programme on online abuse so schoolchildren can be better prepared to identify potential digital risks.\(^{21}\)

The use of false identities to obtain private content will become increasingly important, as will all other cybercrimes, which have huge consequences for every user. One thing is certain: technology has flooded the world and may have overturned many existing practices. A child born today will grow up in a data-driven world. People are and will increasingly be surrounded by powerful digital technologies that can digitally process millions of pieces of data in a matter of seconds. However, it is important that parents and children understand the risks of using the internet, as in any area of life. It is also crucial to build digital education, emphasising the importance of involving relevant institutions and civil society organisations in creating actions to better protect children and young people in the digital environment and contributing to making the internet a place of opportunity, creativity, fulfilment and trust.

References

3. Brenner A, Smith A, 72% of online adults are social networking site users. Electronic source: https://www.pewresearch.org/internet/2013/08/05/72-of-online-adults-are-social-networking-site-users/.

17. Kopecký K, Online blackmail of Czech children focused on so-called “sextortion” (analysis of culprit and victim behaviors), Telematics and Informatics 2017, No. 34(1).
20. Lovelock M, Catching a catfish: Constructing the “Good” social media user in reality Television, Television & New Media 2017, No. 18(3).
34. Ritzer G, Jurgenson N, Production, consumption, prosumption: The nature of capitalism in the age of the digital 'prosumer', *Journal of Consumer Culture* 2010, No. 10(1).

DOI: 10.5604/01.3001.0053.8540
http://dx.doi.org/ 10.5604/01.3001.0053.8540

**Keywords:** cyber security, cyber threats, cyber fraud, cyber manipulation, phishing, social media

**Summary:** In today’s digital environment, users freely use almost all available digital services, from opening and maintaining bank accounts, shopping, working, education, and entertainment to sharing private content (photos, videos) and sending confidential information via email. The evolution of the Internet has also radically changed the nature of communication between individuals and influenced contemporary friendship-making. The increased use of cyberspace to establish social relationships has also resulted in the emergence of new forms of crime, leading to the extortion of information, photos, videos, or money. Consequently, this has increased the ability of criminals to seek out potential victims around the world and exploit ('hopeful') individuals seeking relationships with other users. Criminals use a range of dating websites and apps to contact victims, but are increasingly using social media platforms, including Facebook, WhatsApp, Instagram, and TikTok. More often than not, these types of relationships end in a form of blackmail and the articulation of threats to disseminate intimate images or record-

---

ings if the victim does not comply with certain demands, whether behavioural (sending more sexual images or continuing an intimate relationship) or financial. 24

The phenomenon described above is one of many pieces of evidence supporting the thesis that perceptions of the Internet have long since moved beyond the limits of technology. Analyses of cyberspace are increasingly recognising this unique environment as a set of social practices. Tools for understanding how people use technology to, among other things, interact with other users are therefore gaining importance.

Palabras clave: ciberseguridad, ciberamenazas, ciberfraude, cibermanipulación, phishing, redes sociales

Resumen: En el entorno digital moderno, los usuarios utilizan libremente casi todos los servicios disponibles: abren cuentas bancarias, compran, trabajan, estudian, se entretienen, comparten contenidos privados (fotos, videos) o envían información confidencial por correo electrónico. La evolución de Internet también ha cambiado radicalmente la naturaleza de la comunicación entre individuos y ha influido en la forma de entablar amistades. El mayor uso del ciberespacio para establecer relaciones sociales también ha hecho surgir nuevas formas de delincuencia, que conducen a la extorsión de información, fotos, videos o dinero. En consecuencia, ha aumentado la capacidad de los delincuentes para buscar víctimas potenciales en todo el mundo y explotar a individuos (“esperanzados”) que buscan relaciones con otros usuarios. Los delincuentes no solo utilizan diversos sitios web y aplicaciones de citas para ponerse en contacto con las víctimas, sino que también utilizan cada vez más las plataformas de las redes sociales, como Facebook, WhatsApp, Instagram o TikTok. En la mayoría de los casos, este tipo de relaciones terminan en una forma de chantaje y amenazas de divulgar imágenes o grabaciones íntimas si la víctima no cumple determinadas exigencias, ya sean de comportamiento (envío de más imágenes de contenido sexual o continuación de una relación íntima) o económicas. El fenómeno descrito es una de las numerosas pruebas que apoyan la teoría de que la percepción de Internet traspasó hace mucho tiempo los límites de la tecnología. Los análisis del ciberespacio reconocen cada vez más este entorno único como un conjunto de prácticas sociales. Por lo tanto, los instrumentos que permiten comprender cómo las personas utilizan la tecnología para, entre otras cosas, interactuar con otros usuarios, están cobrando cada vez más importancia.