Miloš Tanasijević[1]

PROFESSIONAL PAPER
UDC 657.632

DOI: 10.46793/Rev26113.169T
Received: 15.03.2026.
Accepted: 30.03.2026.
Published: 30.06.2026.

Identification and Prevention of Financial Fraud in the Digital Environment

Abstract: *With the increase in the number of financial frauds in the digital environment, through new technologies and the use of social engineering methods, understanding, identifying and preventing financial frauds in the digital environment is of particular importance. The most common frauds based on social engineering are elaborated and explained, with a focus on phishing frauds. The most common types of financial fraud in the digital environment are indicated, as well as how to protect yourself from them and what preventive measures to take. This paper aims to explain the most common and most dangerous financial frauds in the digital environment, with a special emphasis on phishing fraud and its forms and types. A simulation of a phishing attack is presented in detail under strictly controlled conditions and under clearly defined rules. The goal of this phishing campaign is to demonstrate how scammers attempt to manipulate the victim and exploit their social status, coupled with ignorance, to obtain financial data for financial gain.*

Keywords: *financial fraud, scam, phishing, security, finance*

[1] University of Belgrade, Faculty of Organizational Sciences, Serbia.
E-mail: mt20233956@student.fon.bg.ac.rs
ORCID iD: https://orcid.org/0009-0009-3323-3509

INTRODUCTION

Today is characterized by a rapid rise in the digitalization of a large number of financial services. Banking services, electronic payments, online trading and financial applications have become an integral part of everyday life. However, in parallel with these processes, new risks are emerging that threaten financial security, among which financial fraud in the digital environment, such as card fraud, cryptocurrency fraud and phishing scams, occupies a special place.

Unlike traditional forms of financial fraud, digital financial fraud takes place in a virtual environment and relies on the misuse of information systems, digital communication channels and user data. They include various forms of illegal activities, such as identity theft, phishing attacks, payment card misuse, unauthorized access to accounts and manipulation of digital transactions. Timely and accurate recognition of such fraud is of utmost importance, as it allows for timely protection and reduction of financial losses of organizations and individuals. The study of financial fraud in the digital environment stems from the fact that, despite their technological aspect, these illegal activities are based on financial transactions and the acquisition of illegal property benefits. Digital technologies in this context represent a means of execution, while the essence of the problem is of a financial nature and insufficient awareness of financial security in the digital environment. Successfully detecting and proving financial fraud in a digital environment requires an integrated approach, which involves close cooperation between financial and computer forensics.

The profound changes brought about by the digitalization of business have affected all segments of the financial system, particularly the methods of detecting and preventing financial fraud. In an era where data represents the most valuable resource, modern technological tools such as artificial intelligence, blockchain, and digital forensics are indispensable in identifying irregularities and reconstructing financial flows (8). Despite the efforts of regulators or management, fraud continues to occur, causing significant financial losses and undermining the reputation of companies. Financial fraud and misconduct share numerous common characteristics, yet each illicit act has its own specific features. They may be committed by different individuals, across various departments, and can occur in companies of different sizes (9).

PHISHING: A SOCIAL ENGINEERING TECHNIQUE IN CYBER FRAUD

Phishing is an attack in which a malicious attacker attempts to steal money or personal information from a user by tricking the user into unknowingly providing them with personal information, passwords, or payment card numbers. *It* is a specific type of financial fraud via electronic mail, or e-mail. By *impersonating or* falsely representing a trusted entity (bank, financial institution, government institution, reputable merchant, etc.) via an electronic communication channel, the victim is tricked into entering personal information.

A type of fraud that aims to collect and misuse confidential user data, such as bank account numbers, social media passwords, or email access, is called phishing (1). Phishing can also be defined as a form of social engineering in which an attacker attempts to fraudulently obtain sensitive information, such as usernames, passwords, and credit card details, by posing as a trusted entity in an electronic communication (2).

Social engineering is a type of psychological manipulation, where a person is lured into taking actions that they would never take under standard circumstances, i.e. revealing personal or sensitive data. It can be said that social engineering is a type of cyber attack, because it uses modern technology, techniques and the Internet as a communication channel. Phishing certainly stands out as the most widespread and dangerous form of social engineering.

We often talk about software vulnerabilities. The human equivalent of software vulnerabilities is emotions. When faced with a frightening scenario, people very often react impulsively, "on the spot", and only think later. It is precisely on this "vulnerability" that hackers base social engineering techniques with which they carry out successful cyber-attacks (3).

Before carrying out a phishing attack, the victim is thoroughly investigated. All information that can be of help to the attacker is collected, so that his attack looks as convincing as possible and is as successful as possible. Almost everything is investigated, where the potential victim works, what accounts he uses, in which banks he has accounts, who he hangs out with, where he shops, what he uploads to social networks, etc. By possessing this information, a message with convincing content is created. This phishing message is mostly disturbing or captivating in nature.

A captivating message is usually based on information about the victim's interests. Based on this information, a message with convincing content is created, with which the victim will be captivated, and an offer that almost anyone would accept in real circumstances, and rarely would anyone refuse. The content of the message, in this case, is that a free trip, mobile phone, plane ticket, car, money from a prize game, etc. has been won. To claim the prize that the victim supposedly won, it is most often necessary to click on a link and enter account credentials or payment card details to supposedly pay out the prize. The link is most often disguised through link shorteners (such as: *bit.ly* , *cutt.ly* , *skr.rs* , *short.io* , *tinyurl.com* ...) and its authenticity cannot be determined at first glance.

A distress message has the same sequence of steps as a charming message. The difference from charming phishing messages is that in this case, the user is frightened and intimidated. This causes a rash and quick reaction in the victim. Such messages instil fear, tension, cause a sense of urgency and create panic. A sense of urgency is often created, and the victim is rushed to enter the data as soon as possible. In this way, the victim is left with very little time to think rationally and carefully review the authenticity of the message. The most common content of such messages is that the user is running out of time to perform an action, and if they do not enter the requested data immediately, someone else will take over their account and will never recover it. Also, tricks are used that their account is compromised, blocked or disabled and if they do not immediately confirm their identity and

enter the data, they will lose all the money in the account, which they will never be able to recover. Unfortunately, out of fear that this will actually happen, many people fall for these phishing messages and enter their personal banking information and passwords. The data is then forwarded to a malicious attacker who misuses it in the same way.

Due to its high efficiency, phishing is the most popular form of cybercrime. Cybercriminals are successful because they research their victims thoroughly beforehand. They usually pretend to be reputable companies, financial institutions, friends or acquaintances, and carry out the attack using email, text messages (SMS), direct messages on social networks or in video games.

CONDUCTING EXPERIMENTAL PHISHING RESEARCH AND ANALYZING THE RESULTS

For the purposes of implementing and conducting experimental phishing research, a platform for training and simulating phishing attacks, called *Gophish, will be used*. The platform is *open-source*, which means that the source code is publicly available and can be used, revised, modified, and shared for free. This refers to software whose source code is available under *the open source* license, which means it is free, and therefore a great opportunity for those who want to further develop this project (4). In this way, you can both contribute to the community and encourage innovation and improvements in this domain.

Gophish The platform is primarily intended for educational phishing simulations, as it allows for testing in a strictly controlled environment and under clearly defined conditions, how resistant individuals or groups in organizations are to so-called "phishing". *Gophish* is written using the *Go programming language* and is designed to be easy to install, use, and administer, with clear and intuitive steps, without complex infrastructure or configuration (5).

DEFINING EXPERIMENT GOALS AND RULES OF ENGAGEMENT (SE-ROE)

Before any research or experiment is started, whether in part or in whole, it is necessary to establish the rules of engagement for social engineering. *Engineering Rules of Engagement* (SE-ROE), which will be presented below.

The goal of the research is to educate and raise awareness among individuals about security in the digital environment, as well as the threats that manifest in various forms every day. Consent to conduct the research was obtained from the registered owner of the domain name, izradawebsajtova.com. Consent was obtained in written and oral form and published on a privileged page at the following address: https://izradawebsajtova.com/saglasnost . The password for opening protected content on the page is: "*admin*" (in lowercase, all connected, in Latin).

The research focuses on simulating the implementation of phishing attacks on participants' financial information, including the simulation of theft of payment card data, the purpose of which is to determine the vulnerability of participants to this type of attack and subsequent education with the aim of preventing bad actions and never repeating them. The research is conducted strictly under controlled conditions with the full written consent of the owner. Strict conditions for conducting phishing research have been defined, with the confirmation of the owner, including a list of email addresses that will be presented in Table 1.

Table 1.

Serial number	Email address to be used for the experiment	Owner approval to participate in the experiment
1	aleksandar@izradawebsajtova.com	APPROVED
2	misa@izradawebsajtova.com	APPROVED
3	marija@izradawebsajtova.com	APPROVED
4	dragana@izradawebsajtova.com	APPROVED
5	tamara@izradawebsajtova.com	APPROVED

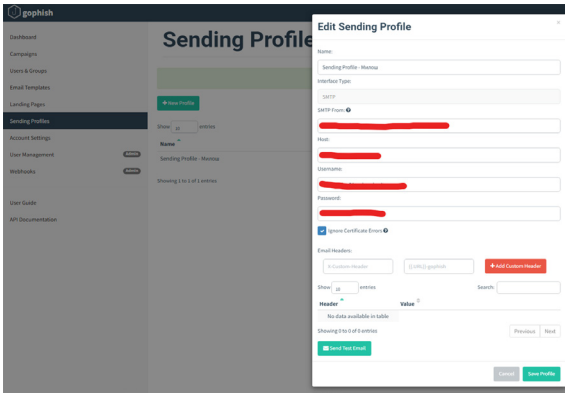
The survey will be conducted exclusively on approved email addresses from the table. The duration of the survey will be exactly three days, and potentially entered data will not be collected, shared or processed. The completion of the survey includes informing participants about the results of the survey, along with the preparation of educational content with the aim of raising awareness about security in the digital environment and providing advice on recognizing threats.

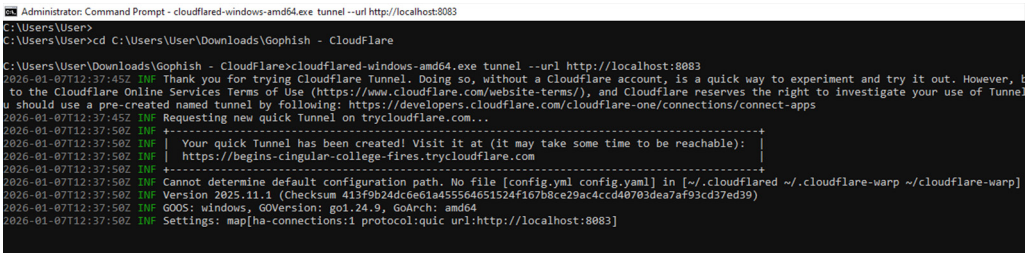
The following activities are permitted within the experiment: simulating phishing emails to approved email addresses, using realistic but fake email message templates, and tracking technical indicators such as email opens and clicks to enter data for statistical and educational purposes. All other activities not explicitly listed as permitted activities are considered prohibited activities.

PHISHING ATTACK SIMULATION IN A CONTROLLED ENVIRONMENT

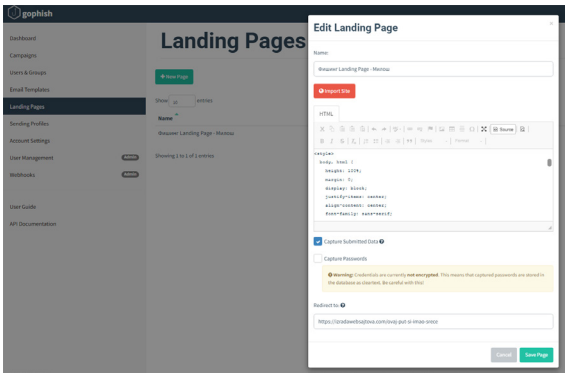
We'll start with the section called *Sending Profiles,* in which we configure the email address that we will use for sending and that will be displayed to recipients.

The GoPhish environment you set up only works on your local network and is not accessible from the internet, which means that the full potential of the tool will not be available to email recipients on another network. To overcome this problem, we will connect *Cloudflare* tunnel and thus avoid restrictions and add a domain for the phishing page.

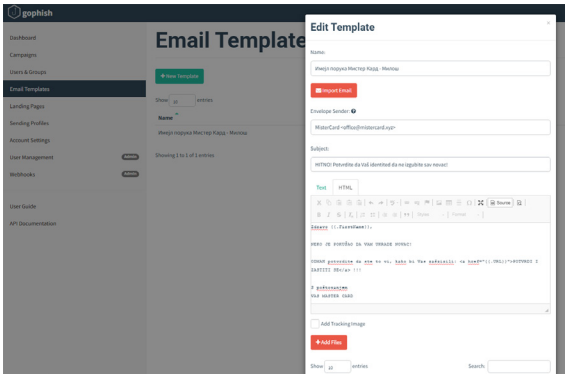




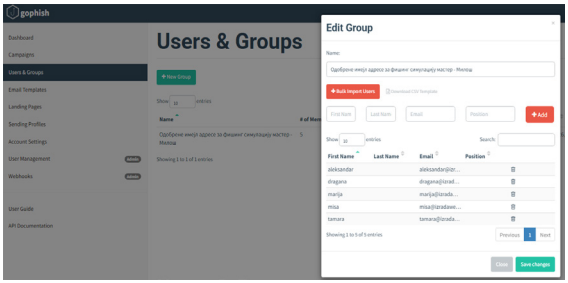
Creating a Phishing *Landing Page* page using *custom* code is the most important part, which defines the appearance of the phishing page. It is also possible to insert a page from a website using *Import Site*, *in which only* the URL to the specific page that will be automatically cloned is specified. In this example, we have chosen our own code that we have added and adapted the structure for the needs of the project. The entered data is used exclusively for statistical purposes. If the research participant clicks on the data entry button, they are redirected to a page that informs them that they were lucky this time, because this is a test.



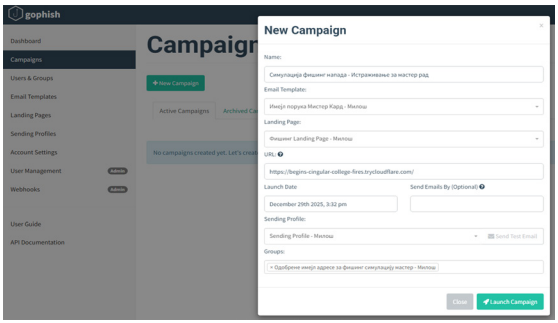
The content of the email message is created using *an Email Template. Here, a distressing message is created that forces urgency and CloudFlare's public* is entered. domain.



The first thing you can notice is that instead of *Master Card* It says *MisterCard* in the sender's name. If you pay closer attention, you can see that the sender's email address is offlce@mistercard.xyz where the name contains the Latin letter "*l*" instead of the letter "*i*" and it comes from the domain *m* ***i*** *stercard.xyz which* resembles *mastercard.com* domain. Handcrafted *Landing The Page* page is only visible when the campaign is launched, and only using *the Go* variable *{{.URL}},* through which each link can be viewed separately.



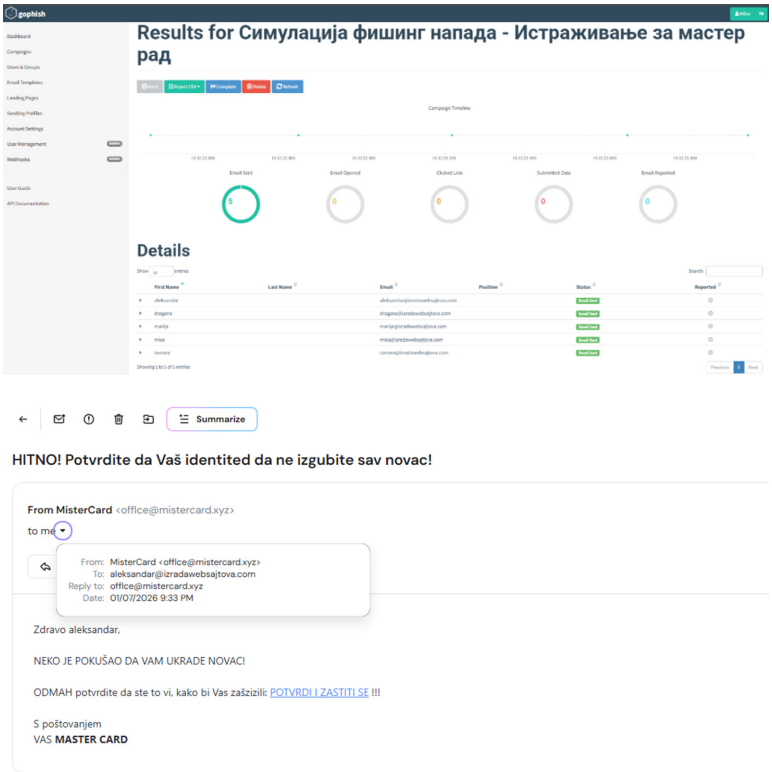
Email addresses that have received consent and approval to participate in the phishing survey have been added to the *Users & Groups section* as a separate group. After the preparation and setup are complete, we begin creating a phishing email campaign.



Phishing messages will be sent according to the specified criteria, and the results will be analyzed after three days.

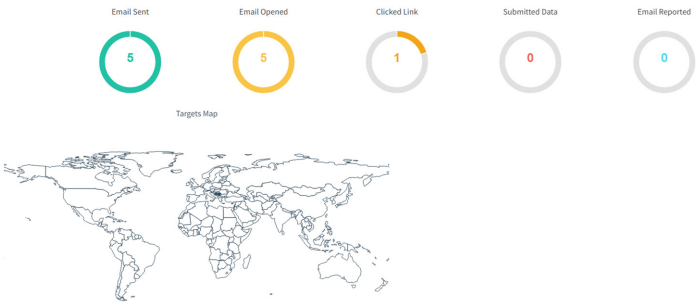
ANALYSIS OF RESULTS

In the following image, we can see that the emails were successfully delivered to all 5 email addresses, but none of the emails has been opened yet. In the image below, we can also see what the email message that the survey participants received looks like.



After a certain period of time, we obtained the results presented in the following figure.

It is clearly visible that all participants in the survey opened the email message and that only one person clicked on the link. In the more detailed survey results, we can also see which person clicked on the link, from which operating system and at what time. On the world map, in the survey results view, we can see the location of participants who opened the email message by country, and that is only Serbia. It is important to note that the person who clicked on the link did not enter any data.



The results of the conducted phishing attack simulation show the real state of the participants' level of awareness of financial security in the digital environment. The goal of this activity is to raise individual awareness of financial fraud in the digital environment and indirectly raise the awareness of the wider social community. The results obtained serve as a basis for further improving the general awareness of society about financial security on the Internet, while indirectly strengthening the culture of safe behavior in the digital environment. Given that only one person clicked on the link and no one entered sensitive data, this research has relatively good indicators.

PROTECTION AND PREVENTION MEASURES

To protect ourselves from a potential fraud or threat, it is necessary to know the threat, because if we do not know what we are defending ourselves against, we will not know in any way or how to protect ourselves from it. In this regard, emphasis is placed on education and training on the types and methods of fraud in the digital environment, which are almost always focused on finances, as the main motive for the attack. Training and education of individuals, along with comprehensive awareness-raising of society about the risks of digital fraud, is one of the key elements of strategic protection in the modern financial environment.

In the case of phishing, it is always recommended to:

- Checking the email address from which the message was sent.
- It is advisable to always double-check, especially if there is a sense of urgency or urgency, which is a basic signal for something suspicious.

- If you suspect the legitimacy of an email message, contact the institution (for example, a bank) and verify it further.
- never send passwords, personal or banking information via a form sent from a suspicious email address.
- Use the usual procedure to update your details, as the bank will never request details of personal/confidential data via email.

In certain situations, it can be difficult to recognize a phishing attack, as the messages are crafted to appear authentic, so the first step in defense is to be aware of the possibility of fraud. To be on the safe side, you should not rush to open attachments in the message, click on links, or send a reply. Characteristics that may indicate a phishing scam are shown in the image below, and they are attachments and links, spelling errors, and unnecessary urgency regarding the verification of the email address or other personal information (1).

Instructions for safe use of ATMs:

- When entering your PIN at an ATM, cover the keypad from view.
- A PIN code is a personal identification number that no one should know.
- Keep the PIN code separate from the card.
- Do not allow an unknown person to assist with a transaction.
- Regularly check your payment card statement and transactions.
- Check for suspicious physical attachments at the ATM.
- Make sure you take your card out of the ATM before you leave.
- If the ATM holds your card, notify the bank immediately.
- Block a lost or stolen payment card immediately and report it to the bank.

The financial institution that has made the most progress in this area and stands out from the rest for investing in education and developing guidelines and methodologies for handling security incidents is *Société Générale Bank*. CERT *Societe Generale,* in collaboration with CERT *aDvens,* developed *Incident Response Methodologies* (IRM) 2022, a collection of practical guidelines for handling security incidents (6). The publicly released documentation contains operational procedures used in various types of security incidents, providing standardized methodologies for CERT teams.

The Financial Institutions ICT Incident Response Team (FIN-CSIRT), as the first sectoral CERT in the country, enables the formalization of cooperation between financial institutions and other relevant stakeholders in the country and abroad, with the aim of creating more efficient cyber resilience of the entire financial sector of our country. FIN-CSIRT leads efforts to create a secure environment for users of financial services in Serbia. Another important goal of the Financial CERT is to raise awareness among users of financial services with the aim of providing better information and creating a safe and reliable digital environment for all categories of users of financial services (7).

CONCLUSION

User education and awareness-raising should not be seen as a one-time activity, but as a dynamic and continuous process that must keep pace with the rapid development of digital technologies and the evolution of fraud methods in the modern environment. The digital transformation of financial services has brought numerous advantages in terms of efficiency and speed of financial transactions, but at the same time has brought and significantly increased the exposure of financial systems to various forms of digital threats.

Financial fraud in the digital environment represents one of the most significant security challenges of the modern financial sector, and it is necessary to view it through the prism of financial security and risk management. It is not enough to simply install a program that will provide a minimum of protection, which in most cases is only apparent protection. No software solution will fully protect us from all types of malicious activities, because they are much more imaginative today than before, so that they provoke our reaction, so that we unconsciously perform an action that we would never do under normal circumstances. The first line of defense is, first of all, a person (user) as a trigger for actions. Therefore, it is necessary to invest in understanding financial fraud in the digital environment, as a step towards further progress of the individual as a user and the community as a whole. What is current today as a method of attack may be modified or replaced by another method in the near future.

The point is not to invest in software that will provide permanent protection, but rather to invest in educating people. Given that digital finance is now an indispensable part of our everyday lives, raising awareness about the security of digital finance is an imperative for a society striving for development. When talking about protection and security risks, it must be remembered that it is a constant struggle between those who try to exploit loopholes and commit abuses by using human emotions, empathy and fears on the one hand, and those who create mechanisms for education, training and defense on the other.

References

1. National CERT of the Republic of Serbia. (2021). *Phishing – Recommendations for the prevention of phishing attacks*. Republic Agency for Electronic Communications and Postal Services (RATEL). Available at: https://www.cert.rs/files/shares/%D0%A4%D0%98%D0%A8%D0%98%D0%9D%D0%93%2021.pdf
2. Jagatic TN, Johnson NA, Jakobsson M. and Menczer F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968. Available at: https://dl.acm.org/doi/pdf/10.1145/1290958.1290968
3. IT Clinic. (2018, June 26). What is social engineering? IT Clinic – Blog. https://it-klinika.rs/sta-je-socijalni-inzenjering/
4. Wright J. (2020). *Gophish open source phishing framework (MIT License)***.** Available at: https://docs.getgophish.com/user-guide/license

5. Gophish Project. (n.d.). Gophish user guide: Software documentation. Available at: https://docs.getgophish.com/user-guide/documentation
6. CERT Society General. (2022). IRM - Incident Response Methodologies 2022 [GitHub repository]. GitHub. Available at: https://github.com/certsocietegenerale/IRM
7. FIN-CSIRT. (2025). Center for the Prevention of Incidents in ICT Systems of Financial Institutions. Available at: https://www.fin-csirt.rs/
8. Mićić M. (2026). Forensic Accounting in the Digital Era: Modern Technologies in Financial Fraud Detection. REVIZOR: Journal of Organizational Management, Finance and Auditing. https://doi.org/10.46793/Rev25112.061M
9. Jeremić N, Jeremić M. and Jakovljević N. (2023). The Importance of Auditing in the Prevention of Financial Fraud. *REVIZOR: Journal for Organizational Management, Finance, and Auditing***.** https://doi.org/10.56362/Rev23104063J

Identifikovanje i prevencija finansijskih prevara u digitalnom okruženju

Apstrakt: Porastom broja finansijskih prevara u digitalnom okruženju, posredstvom novih tehnologija i upotrebom metoda socijalnog inženjeringa, od posebnog značaja se izdvaja razumevanje, identifikovanje i prevencija finansijskih prevara u digitalnom okruženju. Razrađene su i objašnjene najčešće prevare zasnovane na socijalnom inženjeringu i fokusom na fišing prevare. Ukazano je na najčešće vrste finansijskih prevara u digitalnom okruženju, kao i kako se od njih zaštititi i koje preventivne mere preduzimati. Ovaj rad ima za cilj da objasni koje su najučestalije i najopasnije finansijske prevare u digitalnom okruženju, sa posebnim akcentom na fišing prevare i njegove pojavne oblike i vrste. Detaljno je prikazana simulacija fišing napada u strogo kontrolisanim uslovima i pod jasno definisanim pravilima. Cilj ove fišing kampanje je da se demonstrira način na koji prevaranti pokušavaju da manipulišu žrtvom i iskoriste njenu socijalnu notu, u sprezi sa neznanjem, da bi se domogli finansijskih podataka s ciljem da ostvare finansijsku korist.

Ključne reči: finansijske prevare, prevara, fišing, bezbednost, finansije.