ENHANCING ONLINE SECURITY AND AVOIDING INTERNET FRAUD

Maxim ALEXEI[1*], Adrian VREMERE[1], Artemie ILICO[2]

[1]Department of Software Engineering and Automation, group FAF-232, Faculty of Computers, Informatics, and Microelectronics, Technical University of Moldova, Chisinau, Republic of Moldova
[2]Department of Software Engineering and Automation, group FAF-231, Faculty of Computers, Informatics, and Microelectronics, Technical University of Moldova, Chisinau, Republic of Moldova

*Corresponding author: Maxim ALEXEI, maxim.alexei@isa.utm.md

Tutor/coordinator: **Elena GOGOI**, university lecturer, Department of Software Engineering and Automation, Faculty of Computers, Informatics, and Microelectronics, Technical University of Moldova, Chisinau, Republic of Moldova

Abstract. *Regarding our academic writing, we have outlined the many-sided nature of online scams by emphasizing their structure and the psychology behind them. At the outset, we have analyzed multiple forms of Internet fraud, focusing mainly on phishing attacks. Therefore, we have identified the core principles of most online frauds and analyzed in-depth the complexities of phishing, including its reasons, layout, and its detection methods. Furthermore, we explored the main safe Internet practices, such as avoiding public Wi-Fi and using secure software, as effective countermeasure's against potential swindles. On top of that, we emphasize the vital role of education, and awareness in combating online scams, underscoring the increasing involvement of governments and educational institutions in promoting cybersecurity. Over and above that, our paper reveals the significant impact of collaboration within organizations in the domain of cybersecurity, highlighting how those partnerships and information sharing among them play a crucial role in developing effective strategies to combat the increasing wave of digital fraud. Thus, we provided a comprehensive understanding of online deceptions, and proposed strategies in order to enhance online safety.*

Keywords: *cybersecurity education, data protection, online scams, phishing attacks, safety protocols, secure connections.*

Introduction

The Internet is a double-edged tool in today's linked society, full of chances for information and connection but also full of risks for fraud and exploitation. Our investigation into the field of online fraud and security has exposed us to a multitude of different types of scams, from the selling of counterfeit products to phishing schemes, all of which aim to trick naïve consumers into falling for a false web. We identify a recurring pattern underneath these fraudulent operations by analyzing study data from Yonder Consulting [1], Analytics Insight [2], and 211check [3]. This helps to clarify the strategies used by con artists to deceive and take advantage of their victims Furthermore, our investigation reveals the worldwide scope of these scams, with certain countries turning into epicenters of cybercrime, frequently propelled by socioeconomic difficulties.

However, amidst these challenges lies a glimmer of hope, as educational initiatives spearheaded by entities like the Federal Trade Commission (FTC) [4] and the National Cyber Security Centre (NCSC) [5] strive to empower individuals with the knowledge and tools needed to navigate the digital landscape safely. By synthesizing these insights and advocating for proactive measures, including secure online practices and robust authentication mechanisms, we aim to foster a guide of digital resilience and ensure a safer online experience for all.

Understanding Online Scams

At the outset, the Internet is a conduit for dishonest practices that deceive or cause harm to gullible consumers. We strongly believe that these actions sometimes anointed Internet scams, come in various shapes and sizes and include phishing, romance, investment, work-from-home, sweepstakes, and frauds originating in West Africa Moreover, psychologists utilize psychological tricks to play on the needs, weaknesses, and feelings of their victims. Internet fraud can also lead to identity theft, monetary loss, psychological suffering, and legal issues. As a result, it is critical to understand the typical forms of online fraud and how to avoid them.

While each scam exhibits a unique sequence of actions, we found out that Yonder Consulting's research [1] has identified a consistent four-step pattern that characterizes the experience of online fraud. This framework provides valuable insights into the underlying mechanics of scams, enabling a more systematic analysis and informed countermeasures.

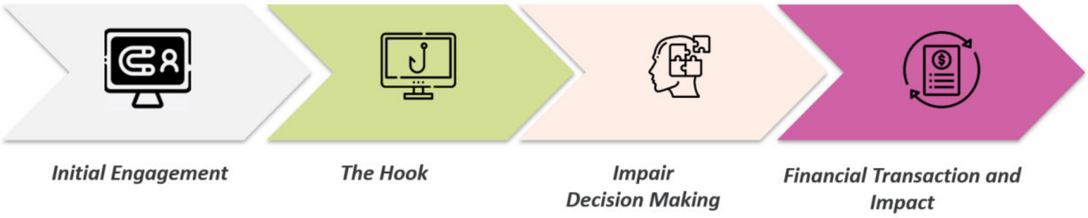

Figure 1. Four key phases of scams or fraud experience

Regarding the initial engagement phase, in this stage, scammers directly interact with victims (e.g., via direct messages on social media) or indirectly (e.g. by sharing fake website links). The goal is to establish communication and pique the victim's interest. If we focus on "the hook," scammers use an enticing "hook" to attract victims. This hook promises clear benefits, such as financial gains or valuable connections. Furthermore, to gain victims' trust, charlatans employ various tactics. These techniques impair rational decision-making and include constant messaging, emotional narratives, promises of returns on investment, charm, and time-sensitive pressure. Finally, after successfully navigating phases 1-3, scammers lead victims to the critical point: parting with their money. Often, victims realize they have been scammed only after the transaction, facing emotional and financial consequences.

A study conducted by Analytics Insight [2] delineates the origins of prevalent online scams across various nations. Ghana, Indonesia, and the Philippines are prolific sources of scams, particularly in the domains of romance, lottery, and employment-related fraud. Moreover, India is notable for scams involving the impersonation of tech support representatives. Victims are often coerced into paying for superfluous software or services. In addition, Romania, Russia, and the United States harbor scammers engaged in multifaceted illicit activities.

These include phishing schemes, credit card fraud, malware attacks, and identity theft.

Furthermore, the insights from the 211 check blog post [3] explain that the quest for monetary gain emerges as the fundamental motivation behind most cyber scams. Notably, the countries highlighted earlier exhibit a pronounced correlation with constrained economic prospects for their population. Therefore, we firmly believe that some citizens resort to carrying out fraudulent behavior as the key to survival. While this observation does not justify the fraudulent conduct, it does underscore its prevalence in the context of online scams.

In our ongoing exploration of the landscape of online security and internet fraud, we delved into a comprehensive study conducted as part of a series of research studies [6], which provided valuable insights into the prevalent forms of online fraud encountered by victims in the United Kingdom. Our analysis revealed a disconcerting reality these fraudulent activities wield a significant impact on the British population, permeating various sectors of society. From educational institutions grappling with phishing attempts, large businesses falling prey to investment scams, and even individuals encountering counterfeit goods schemes in their daily lives, the ramifications of online fraud extend far and wide, and it might end up into catastrophically consequences.

Table 1

Percentage of UK online adults who had ever experienced scams and fraud

Type of online scams	**Percentage of UK adults (%)**
Impersonation	51
Counterfeit goods	42
Investment, pension or “get rich quick”	40
Computer software service fraud or ransomware	37
Fake employment	30
Romance or dating	29
Health or medical	24
Identity fraud	24
Psychic or clairvoyant	18
Holiday	17
Money laundering	14

Besides the data presented (Table 1), where it is clearly stated that the most likely scams people have fallen for in the United Kingdom are impersonation, counterfeit goods, and investment scams, the study [6] also states that men, younger adults aged 18-34 and people with children in the household are more likely than average (87%) to say they have encountered online fraudulent content. Moreover, most scams were encountered by email (30%) and social media (23%). In addition, regarding the financial loss, two out of five victims lost between £1 to £99, while one in five suffered losses of £1000 or more. On top of that, most money was lost due to online counterfeit scams, as stated in the article [6]

Avoiding Phishing Attacks

To begin with, phishing is a form of online scam that tries to trick users into giving up their personal information by pretending to be trustworthy. It can involve stealing passwords, credit card numbers, bank account details, and other sensitive data.

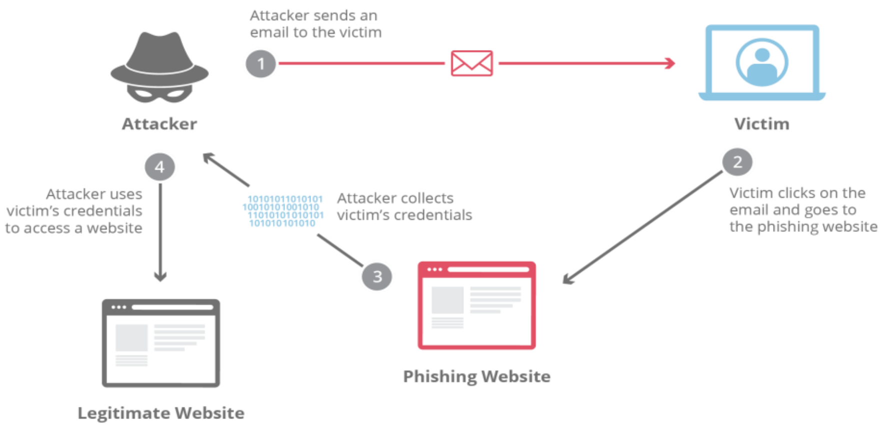
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim’s credentials to access a website
Attacker collects victim’s credentials
3
Phishing Website
Legitimate Website

Figure 2. The way a typical phishing attack is carried out

The structure of a typical phishing attack scenario (Fig. 2) usually consists of the attacker and the victim. In this case, the scammer contacts the potential victim by sending a phishing website link via messaging applications or email. The target accesses the link, and the login field is filled in with personal data. Therefore, the attacker collects the victim’s credentials and uses them to access their personal account through the real website.

We strongly believe that this form of online fraud is worth pointing out, according to an article published by AAG: “Phishing is the most common form of cybercrime, with an estimated 3.4 billion spam emails sent every day” [7]. Phishing messages often look like official emails from banks, service providers, e-pay systems and other entities. The email will urge a recipient to quickly enter/update their personal data for some reason. Usually, the reason is related to data loss or system failure.

Moreover, after some in-depth research, we came to the realization that now it’s easier than ever to create a clone website with the aim of stealing important login data. For example, a hacker can use a tool like Blackeye [8], which is a phishing tool for Linux, to create a fake LinkedIn website in just a few minutes. Since Blackeye has 39 templates for hosting a fake website, covering many of the most popular services on the Internet, such as social media, banking, etc. Each template contains everything needed to host the fake website, including the HTML files and the scripts that run on the hosted site, which can capture the victim’s IP address, user agent, and credentials and send them to the scammer. By using such tools, cyber-criminals can easily create convincing phishing sites and lure unsuspecting users into falling for their scams.

Last but not least, we came to the realization that there are several ways to spot a phishing website of which users should be aware, such as checking the URL of the link they are planning to or have already accessed, whether it has extra characters, or sketchy domains, such as “.cc”, as they are cheaper to be acquired and used for fraudulent reasons. Moreover, if a web address is not secured and encrypted using an SSL certificate, then that should raise a red flag, as well as the Grammatik mistakes found after assessing the content presented on there and the negative reviews left by other users on places, such as “Trust Pilot” or others.

Safe Internet Practices

In the contemporary digital milieu, the security of online activities assumes heightened significance. Based on the knowledge we have acquired from the research done by the AO Kaspersky Lab [8] and the Security National Bank of South Dakota [9], in this subtopic, we are trying to dissect and expound upon the intricacies of foundational Internet safety protocols, encompassing an array of measures ranging from securing Internet connections to judiciously navigating the complex terrain of online interactions.

Within the framework of cyber security, the imperative of securing Internet connections emerges as a cornerstone. Public Wi-Fi, often a necessary convenience, presents vulnerabilities that necessitate meticulous handling. Recommendations include the judicious use of Virtual Private Networks (VPNs) to encrypt data transmissions, thereby mitigating potential cyber threats. In the expansive digital domain, discerning website reliability is a crucial tenet. Key indicators, including secure connections (HTTPS) and adherence to online payment standards, are posited as essential checkpoints. The process of verification mirrors the discerning choices made in a physical marketplace to ensure the trustworthiness of digital transactions.

The vulnerability inherent in weak passwords stands as a critical concern in the cyber security paradigm. Addressing this concern entails the crafting of robust passwords – characterized by length, complexity, and uniqueness. Concurrently, we believe that the integration of password managers is proposed, facilitating the generation and secure storage of intricate passwords for heightened protection in the pursuit of bolstering online account security, the implementation of Multifactor Authentication (MFA) assumes prominence. This method augments traditional authentication processes, demanding additional verification steps beyond conventional usernames and passwords. The integration of MFA, akin to adding supplementary locks, serves as a deterrent against cyber threats.

Moreover, due to the evolving security infrastructure, the software landscape necessitates continual updates to counter emerging vulnerabilities. Developers have to implement vigilant security custodians and release patches to fortify digital protection. Users are urged to adopt the latest iterations of operating systems and applications, thereby aligning with a proactive cyber security stance.

Therefore, we tried to underscore the criticality of adopting a multifaceted approach to Internet safety. By adhering to the delineated protocols, users can fortify their digital presence, fostering a resilient defense against the evolving landscape of cyber threats. In the amalgamation of secure Internet connections, robust authentication mechanisms, and prudent online conduct, individuals can navigate the digital realm with heightened assurance and security.

Role of Education

How much do people in the current world know about online scams? One important indicator of how susceptible modern Internet users are to fraudulent activity is how informed they are of online frauds. Even though more individuals are becoming aware of these scams, many continue to fall for them because they don't have a thorough grasp of them.

For this reason, governments, academic institutions, and cybersecurity institutes are essential in raising the general public's awareness and understanding of online frauds. For example, the United States' FTC [4] provides a wealth of information on identifying and defending against many forms of online fraud. In an effort to inform the public and stop fraud, they try to prevent it by disseminating advice, articles, and warnings on the most recent schemes on their website.

The NCSC in the UK has launched a number of initiatives to inform the public about cyberthreats, including online scams [5]. They work with other groups to raise awareness and offer advice on how to secure digital environments, both personal and professional. Additionally, private groups play a crucial role in increasing awareness. To assist consumers in identifying such risks, corporations such as Google and Microsoft have included fraud detection and alarm systems into their email services [12].

Numerous research' statistics provide insight into how successful these campaigns for awareness and education have been. Awareness programs have resulted in a 25% decrease in phishing success rates, according to a research published by the Cybersecurity and Infrastructure Security Agency (CISA) [13]. According to a Pew Research Center poll [14], 67% of American adults have also grown more circumspect in their online activities as a result of growing knowledge of scams and the fact that phishing attempts can occur on several platforms.

In this arena, the inclusion of cybersecurity subjects in school curricula is another noteworthy trend. These days, a lot of schools provide courses on Internet safety and how to spot scams, giving the next generation the skills they need to use the internet safely. These instructional courses frequently address subjects like spotting phishing emails, appreciating the need of strong passwords, and identifying phony websites. These coordinated efforts have a big effect because it's been shown that nations with strong cyber education initiatives have lower incidence of victims of online scams. This association emphasizes how crucial it is to keep funding campaigns for public awareness and education.

Thus, even if people are becoming more aware of online frauds, continuous awareness and education are still necessary due to the dynamic nature of cyber dangers. We think that in order to lessen the frequency of online frauds and safeguard Internet users everywhere, governments, businesses, and individuals must work together. Our techniques for keeping safe online need to evolve along with technology.

Conclusions

On a final note, our investigation into improving online security and preventing internet fraud has uncovered a complex environment full of many frauds and dishonest tactics. We have shed light on the mechanics and strategies used by internet frauds, which range from phishing schemes to the sale of counterfeit products, by outlining their structure and psychology. We have emphasized the significance of cooperation, awareness, and education in successfully addressing these dangers via our study.

Along with private sector efforts, the FTC [4] and the NCSC [5] have made great progress in educating people and providing them with the means to securely traverse the digital world. Furthermore, including cybersecurity education into curricula is a step in the right direction toward developing a culture of digital resilience in children.

Although there has been improvement, ongoing awareness and plan adaption are necessary due to the dynamic nature of cyber threats. Enhancing online safety is based on our thorough knowledge of online deceptions and the proactive measures suggested in this study. We are getting closer to realizing our objective of creating a safer online environment for all users as we keep improving our strategies and combining our efforts.

References

[1] Yonder Consulting, "Executive Summary Report: Online Scams & Fraud Research", 2023

[2] S. Akash, "Top 10 Internet Scamming Countries in the World in 2023", 2023 [Online]. Available: https://www.analyticsinsight.net/top-10-internet-scamming-countries-in-the-world-in-2023/

[3] E. B. Thomas, "The psychology behind why people create online scams and fraud", in *Data and Statistics*, 2023 [Online]. Available:https://211check.org/blog-the-psychology-behind-why-people-create-online-scams-and-fraud/ - :~:text=The%20desire%20for%20financial%20gain,curiosity%2C%20greed%2C%20and%20compassion https://shorturl.at/knuy6

[4] L. M. Khan, Rebecca Kelly Slaughter, Alvaro M. Bedoya, "The FTC's Efforts in the Greater Fight Against Ransomware and Cyber-Related Attacks" in *A Report to Congress*, 2023

[5] National Cyber Security Center, "Cyber Action Plan" [Online]. Available: https://www.ncsc.gov.uk/Cyberaware/actionplan

[6] Commissioned by Ofcom, "Scale and impact of online fraud revealed", 2023 [Online]. Available: https://www.ofcom.org.uk/news-centre/2023/scale-and-impact-of-online-fraud-revealed

[7] Ch. Griffiths, director of technology and innovation at AAG, "The Latest 2024 Phishing Statistics (updated February 2024)", 2024[Online]. Available: https://aag-it.com/the-latest-phishing-statistics

[8] EricksonAtHome, "blackeye" [Online]. Available: https://github.com/EricksonAtHome/blackeye?tab=readme-ov-file

[9] J. Mackay, the COO of MetaCompliance, "5 Ways to Identify a Phishing Website", in *Phishing and Ransomware* [Online]. Available: https://www.metacompliance.com/blog/phishing-and-ransomware/5-ways-to-identify-a-phishing-website

[10] AO Kaspersky Lab, "Top 10 preemptive Safety Rules and What Not to do Online" [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online

[11] Security National Bank of South Dakota, "Online Safety Guide" [Online]. Available: https://www.snbsd.com/about/online-safety-guide

[12] Microsoft Support, "Protect yourself from tech support scams" [Online]. Available: https://support.microsoft.com/en-us/windows/protect-yourself-from-tech-support-scams-2ebf91bd-f94c-2a8a-e541-f5c800d18435

[13] Cybersecurity & Infrastructure Security Agency, "Phishing Guidance: Stopping the Attack Cycle at Phase One", 2023

[14] E. Anderson. Vogels, Monica Anderson, "Americans and Digital Knowledge in 2019", 2019 [Online]. Available: https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/