UDC 004.056=111

**A. A. Pidlisna**

# FRAUDULENT WEBSITES: HOW TO AVOID BECOMING A VICTIM OF ONLINE FRAUD

Vinnytsia National Technical University

**Анотація**

*Досліджено небезпеку від різних видів шахрайських сайтів. Вказано ознаки, які допоможуть вам розпізнати шахрайський сайт: орфографія, дизайн, запити на дані, відгуки та інші сигнали. Також наведені практичні поради, як уникнути онлайн-шахрайства: перевірка URL, HTTPS, наявність контактної інформації, критичне мислення та інші кроки. Прочитавши дану доповідь ви дізнаєтеся, як розпізнати шахрайський сайт та вберегти себе від онлайн-шахрайства.*

**Ключові слова:** безпека, фішинг, фармінг, сайти, шахрайство.

**Abstract**

*The paper explores the dangers of different types of fraudulent websites. The paper points out the signs that will help you recognize a fraudulent website: spelling, design, data requests, testimonials, and other signals. It also provides practical tips on how to avoid online fraud: checking URLs, HTTPS, contact information, critical thinking, and other steps. After reading this report, you will learn how to recognize a fraudulent website and protect yourself from online fraud.*

**Keywords:** security, phishing, pharming, websites, fraud.

## Introduction

In today's world, where the Internet has become an integral part of people's lives, the number of cyber threats is growing. Among them, fraudulent websites that masquerade as legitimate resources to take possession of personal information, financial assets, and even user identities are attracting special attention.

Online fraud is a serious problem, and it is important to be cautious and careful when interacting with any unverified or questionable web resources.

So, how do fraudulent websites work and what are the warning signs? You will soon find out.

## Research results

Usually, scam websites don’t exist independently – they have a phishing, malvertising, or spamming campaign alongside them. Scammers spread links to their malicious websites so that they appear in:

- phishing emails or text messages
- social media posts and forums
- comments on any page online (usually distributed by bots)
- Search engine advertisements.

*Types of scam websites*. There are different types of scams online, and scam sites also come in different shapes and sizes. Each scam website type has distinctive features that could serve as a red flag for spotting them.

- Phishing websites.

Phishing websites are one type of phishing attack. Fraudsters use URL phishing to distribute the links to these websites via email and fake everything from the sender to every part of the website they pose as. Everything but a trivial nuance in the URL makes it look like a real company, usually one with lots of customers, such as Amazon or PayPal.

- Pharming attack. A more diligent scammer may even use pharming techniques to redirect the legitimate websites to the fraudster’s fake version [1].

A pharming attack is a cyberattack in which victims are redirected or tricked into visiting a malicious website [2].

*An example of a fraudulent scheme using pharming.* The fraudster finds an ad on the OLX online platform, writes to the seller in a messenger (Viber, Telegram, WhatsApp). Then the fraudster agrees to buy the goods, informs the seller that to receive the funds, he needs to follow an individual link and provide his card details. The seller follows the link and enters all the card details. The fraudster asks the seller for the card balance and the SMS code from the bank. Having received the information, the fraudster appropriates funds from the accounts [3].

- Fake online stores and discount pages

Fake e-shops look like real e-commerce sites, except they don't sell anything. They promise you goods or services with discounts or vouchers that sound too good to be true [1].

*How to identify fake websites*. Fake websites are everywhere and they're getting harder to spot. Here's how you can make sure that you're not dealing with a fraudulent website.

*1. Check the domain name closely.* The easiest way to tell that you're on a fake website is when the domain name doesn't match the official website for the company. For example, scammers often use domain names that are similar to — or even contain — the official URL within the fake domain name.

Here are a few examples of how scammers spoof website domains:

- BankoffAmerica.com (adding an extra "f")
- Paypal.com.secure-site.com (in this case, the domain name is actually "secure-site.com" not "paypal.com")
- WaImart.com (using a capital "i" instead of a lower case "l")
- Netflix-support.net (combining a spoofed domain with a different domain extension)
- Delivery.ips.com (adding "delivery" to the URL in hopes that you won't notice they've spelled "UPS" as "IPS")

Always check that you're on the right domain before entering sensitive information. Unless you're sure that you're on a company's official domain, you could be dealing with a fake website [4].

*2. Lack of HTTPS.* Most legitimate sites use an HTTPS connection, which is indicated by a padlock icon in the browser address bar.

Unfortunately, scammers have started to use SSL certificates to fool you into thinking their fake sites are genuine. If you're unsure about a site, click on the padlock and then check any additional information about the security certificate [4].

*3. Use a website checker.* VirusTotal [5] is one of the easiest and most affordable services for checking a website for viruses. This site does not require registration, you just need to paste the link into the search bar.

*4. Poor design and spelling mistakes.* Fraudulent sites often have unprofessional design and many spelling mistakes. Also, scammers usually provide fake contact information (or no contact information at all). If you can't find information about the company on their website, it could be a scam. Also, be wary if the only way to communicate with the company is through a generic contact form. Ideally, you should be able to find the company's physical address and phone number on their website [4].

*5. Run a virus scan if you experience numerous ads and pop-ups.* Sometimes the goal of a fake app or website isn't to steal your information, passwords, or money — but to infect your device with malware.

Hackers create pop-ups and ad-riddled websites that can infect your phone or computer with viruses that let cybercriminals spy on you, scan your device for sensitive data, or lock your device until you pay a ransom.

If you've been to a site like this recently, you need to make sure your device hasn't been compromised.

## Conclusion

The number of fraudulent websites that lie in wait for users in the virtual space is growing rapidly. This requires attention and caution from everyone who intends to interact with web resources. Despite the fact that the Internet is an inexhaustible source of information and opportunities, the potential threat of online fraud is always present.

So, to avoid becoming a victim of online fraud, it is important to follow a few simple rules. First, always check the authenticity of the website before performing any actions or transferring personal information. Secondly, be careful when opening links in the hope of getting rich easily or providing a service that seems too profitable. In addition, you should learn the main methods of online fraud and be able to distinguish them from legitimate offers.

The best defense against fraud is education and vigilance. Scammers are constantly improving their methods, but knowledge and vigilance can help you avoid potential negative consequences. By paying attention to these simple tips, everyone can minimize the risk of becoming a victim of online fraud and enjoy a safe online experience.

## REFERENCES


1) What are scam websites, and how can you tell if a page is fake? URL: https://nordvpn.com/uk/blog/fake-scam-websites/ (date of access: 08.03.2024).
2) What is a pharming attack? URL: https://nordvpn.com/uk/blog/pharming/ (date of access: 08.03.2024).
3) Як уникнути шахрайства під час онлайн-покупок URL: https://business.rayon.in.ua/news/608728-yak-uniknuti-shakhraystva-pid-chas-onlayn-pokupok (date of access: 08.03.2024).
4) How To Identify Fake Websites: 11 Warning Signs URL: https://www.aura.com/learn/how-to-identify-fake-websites (date of access: 09.03.2024).
5) VirusTotal URL: https://www.virustotal.com/ (date of access: 09.03.2024).



***Підлісна Анна Олександрівна*** — студентка групи УБ-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: annapidlisna370@gmail.com

***Магас Людмила Миколаївна*** — ст. викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: magas@vntu.edu.ua

***Anna A. Pidlisna***. – student of UB-22b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: annapidlisna370@gmail.com

***Liudmyla M. Magas*** — FLD senior lecturer in English, Vinnytsia National Technical University, Vinnytsia, email: magas@vntu.edu.ua