Ольга Габорець,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3 ДонДУВС,
доктор філософії, доцент

CLASSIFICATION AND METHODS OF DETECTION OF PHISHING ATTACKS

Phishing remains one of the most widespread and dangerous cyber threats in the digital age, as it targets users through fake websites or messages to steal confidential data such as logins, passwords, and financial information. The steady expansion of digital infrastructure and the growing dependence of individuals, societies, and states on information and communication technologies have contributed to the increasing relevance of this threat. The very nature of the Internet, which allows anonymity and mass reach, makes it a favorable environment for cybercriminals. Phishing is often used not only to commit fraud but also as a component of more complex schemes that can impact national security and global stability. The term "phishing" can be interpreted in different ways, yet its primary goal is consistent – unauthorized acquisition of information.

Cybercriminals use numerous techniques to carry out phishing attacks, which can be broadly categorized based on whether the attack is targeted at a specific individual (spear phishing) or sent to a wide audience (non-targeted phishing). Additionally, methods vary by delivery channel, including email, social media, phone calls, SMS messages, and malicious advertisements. The sophistication of these attacks continues to grow, with criminals often studying their victims to make fraudulent messages appear highly convincing. Modern phishing tactics include clone phishing, fake websites with nearly identical URLs, hidden links, fake login pages, image-based attacks, and pharming, which redirects web traffic from legitimate to malicious sites.

Recognizing phishing attacks has become increasingly difficult for ordinary users, particularly due to evolving tactics and a general lack of cybersecurity awareness. Research shows that people often judge the legitimacy of websites by appearance alone, fail to understand security indicators in browsers, and underestimate the real consequences of data breaches. Because of this, many phishing attacks go undetected until damage has already been done.

To counter these threats, two main approaches to phishing detection are employed. The first is educating users so they can recognize suspicious behavior and fraudulent content. While this strategy is effective in raising awareness, it is not always scalable. The second approach involves technical solutions, such as automated classification systems and protective software tools. Blacklists and whitelists offer one method of recognizing phishing URLs based on known data, but these approaches suffer from delays in updates and limited scope. Heuristic methods analyze characteristics of websites, such as structure and content, to determine legitimacy. Visual similarity techniques compare suspicious sites with known legitimate ones by examining layout and graphical elements.

A promising area of development is the application of machine learning to detect

phishing. These algorithms can adapt to new forms of attacks and are capable of classifying sites based on patterns identified in large datasets. Hybrid models that combine multiple detection techniques can offer higher accuracy and faster response times. A well-optimized set of features used by classifiers can significantly improve the speed and precision of phishing detection. Practical implementation of these technologies may include browser plugins, automated filters, and integrated antivirus modules.

Ultimately, phishing presents a significant challenge to online security, demanding continuous improvements in both human awareness and technical defense tools. The development of reliable classification systems and detection algorithms plays a crucial role in protecting users from ever-evolving threats. The findings of this research can be applied in the creation of effective anti-phishing solutions, contributing to a safer digital environment.

Валерія Гнатенко,
доцент кафедри кримінального процесу
та організації досудового слідства
ННІ № 1 Харківського національного
університету внутрішніх справ,
кандидат юридичних наук
ORCID: http://orcid.org/0000-0003-1714-664

Микола Сорочишин,
курсант групи 201 ННІ №2,
Харківського національного
університету внутрішніх справ,
рядовий поліції,
ORCID https://orcid.org/0009-0007-1296-1879

ПРАВА, ОБОВ'ЯЗКИ ТА ЗАХИСТ НЕПОВНОЛІТНЬОГО ПІДОЗРЮВАНОГО У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Права, обов'язки та захист неповнолітнього підозрюваного у кримінальному провадженні звичайно є надзвичайно важливими, оскільки неповнолітні є особливо вразливою категорією.

Першу чергу звертаю увагу що з моменту встановлення факту неповноліття або виникнення будь-яких сумнівів у тому, що особа є повнолітньою, участь захисника є обов'язковою у кримінальному провадженні щодо осіб, які підозрюються або обвинувачуються у вчиненні кримінального правопорушення, а саме у віці яким ще нема 18 років.

Крім цього, допомога захисника відповідно до ст. 120 КПК України надається за рахунок коштів Державного бюджету України і є безоплатною для підозрюваного, обвинуваченого. Тому право на правову допомогу можна визначити як гарантовану Конституцією України можливість фізичної особи