The American Journal of Political Science Law and Criminology
ISSN 2693-0803 | Open Access

TYPE Original Research
PAGE NO. 79-81
DOI 10.37547/tajpslc/Volume07Issue06-15

Criminal law aspects of combating phishing and carding (Phishing and carding as forms of fraud in the digital environment: legal qualification)

Dusmatov Durbek Rustamjon ugli

Tashkent City Prosecutor's Office Prosecutor of the Department in the field of counteraction shadow economy, 2nd class lawyer, Tashkent city, Uzbekistan

OPEN ACCESS

SUBMITTED 30 April 2025
ACCEPTED 28 May 2025
PUBLISHED 30 June 2025
VOLUME Vol.07 Issue06 2025

CITATION

Dusmatov Durbek Rustamjon ugli. (2025). Criminal law aspects of combating phishing and carding (Phishing and carding as forms of fraud in the digital environment: legal qualification). The American Journal of Political Science Law and Criminology, 7(06), 79–81. https://doi.org/10.37547/tajpslc/Volume07Issue06-15

Abstract: The article examines phishing and carding as forms of fraud committed in the digital environment from the perspective of criminal law. It analyzes the specifics of their legal qualification under the legislation of the Russian Federation and foreign countries, identifying gaps and inconsistencies in the application of criminal law norms. The article also proposes directions for improving legislation and its enforcement practices to enhance the effectiveness of combating these types of cybercrime.

Keywords: Phishing, carding, cybercrime, fraud, digital environment, criminal law, legal qualification, theft.

Introduction: The Development of Digital Technologies and the Internet Has Radically Transformed the Nature of Crime, Giving Rise to New Forms—One of Which Is Digital Fraud. Phishing and carding have now become widespread methods of stealing confidential information and financial assets from individuals and legal entities. These crimes are associated with the use of advanced technologies, the anonymity of offenders, and significant challenges in detection and proof, creating a serious challenge for criminal justice systems. Modern information and communication technologies, on the one hand, contribute to progress across all areas of public life, while on the other hand, they create new opportunities for committing crimes. Notably, phishing and carding have emerged as forms of fraud committed in the digital environment.

These offenses are highly latent, transnational in nature,

and cause substantial harm to society. Their legal qualification, detection, and suppression require clear normative regulation and adaptation of criminal legislation to the challenges of the digital age.

Phishing (from the English "fishing") is a method of social engineering in which a perpetrator, through fake emails, websites, or messages, induces the user to disclose personal and financial information—passwords, card numbers, verification codes, and other sensitive data.

It is a method by which a criminal, using deceptive messages (typically via email or messaging platforms), seeks to obtain confidential data such as usernames, passwords, and bank card details.

Carding refers to the illegal circulation of payment card data. It involves the unauthorized use, purchase, or sale of payment card data, typically with the aim of stealing funds from someone else's account. Offenders use stolen data to carry out transactions or resell it. Carding may involve the creation of fake banking websites, phishing forms, and automated data-harvesting software.

Both forms of crime share several common features:

- Remoteness of execution;
- High level of automation;
- Use of deception and forgery;
- Infliction of financial harm.

From a criminological perspective, these offenses:

- Are committed remotely and anonymously;
- Do not require direct contact with the victim;
- Are often part of organized criminal activity;
- May be mass in nature (one perpetrator — multiple victims).

Under the current Criminal Code of the Republic of Uzbekistan, phishing and carding are not classified as separate offenses. However, they can be prosecuted under existing articles such as Article 168 — Fraud, defined as the unlawful appropriation of another's property through deception or abuse of trust. In the context of phishing, this involves deceiving a user in order to obtain their data or funds.

In practice, however, difficulties arise in differentiating these offenses, particularly in establishing the intent, motive, method of execution, and in qualifying organized and transnational schemes.

In international practice, especially in the European Union and the United States, legislation tends to specifically identify digital forms of fraud. For example, in the U.S., phishing is classified as the "fraudulent acquisition of identifying information" and is regulated under the Computer Fraud and Abuse Act (CFAA). In the EU, Directive 2013/40/EU on attacks against information systems and the General Data Protection Regulation (GDPR) apply. Moreover, the Budapest Convention on Cybercrime (2001) recommends that states criminalize unauthorized access to data and the fraudulent use of digital technologies.

Therefore, international law emphasizes the need for specialized provisions that adequately reflect contemporary methods of digital crime.

Key challenges in applying criminal law to phishing and carding include:

- Lack of uniform qualification criteria;
- Insufficient adaptation of laws to digital methods of deception;
- Difficulties in proving intent, especially in remote offenses;
- Transnational nature of crimes, necessitating international cooperation.

To enhance the effectiveness of criminal-legal responses, it is necessary to:

1. Clarify the elements of fraud by identifying its digital forms as an aggravating factor.
2. Introduce separate articles into the Criminal Code of Uzbekistan dedicated to phishing and the illegal trade in payment data.
3. Strengthen international cooperation, particularly regarding extradition, digital evidence sharing, and the blocking of malicious resources.
4. Develop judicial practice and methodological guidance for law enforcement agencies on the detection and legal qualification of digital fraud.

Given that cybercrime presents a complex and evolving challenge, and Uzbekistan's legal policy in this area is still developing, the country can effectively ensure cybersecurity and digital law and order by implementing systemic improvements in legislation, institutions, and international cooperation. To combat cybercrime more effectively, Uzbekistan should:

- Update national legislation to reflect modern cybercrime techniques;
- Introduce the concept of digital criminology and adapt investigative methods to digital evidence;
- Build professional capacity by training specialists in digital forensics, cyber law, and information security;
- Expand international collaboration, including by acceding to the Budapest Convention;
- Invest in digital infrastructure and automated cyber threat monitoring technologies.

Phishing and carding are dangerous forms of digital fraud that require modern and flexible criminal-legal regulation. Their latency, scale, and technological sophistication present challenges for both law enforcement and legislative processes. Updating criminal law and establishing a unified enforcement practice are essential for effectively combating these crimes.

As high-tech and dangerous forms of digital fraud, phishing and carding demand appropriate criminal-legal responses. In a digitalized society, protecting citizens' property rights and ensuring information security are impossible without improving legislation, law enforcement practice, and international coordination.

REFERENCES

Rogozhin, A.I. Cyber Fraud: Definition, Types, and Methods of Commission. // Legal Science. — 2023. — No. 2. — Pp. 41–47.

Vasiliev, E.V. Carding as a Form of Organized Crime on the Internet. // Criminology: Theory and Practice. — 2022. — No. 4. — Pp. 33–38.

Commentary on the Criminal Code of the Russian Federation / Ed. by L.D. Gaukhman. — Moscow: Yurayt, 2023.

Convention on Cybercrime (Budapest Convention). ETS No. 185. Council of Europe, 2001.

Karabanov, P.L. International Cooperation in Combating Cyber Fraud. // Criminal Law and Procedure. — 2023. — No. 1. — Pp. 22–29.

Shestakov, D.A. Crimes in Cyberspace: Criminal-Legal and Criminological Analysis. — St. Petersburg: Herzen State Pedagogical University Publishing House, 2021.

Vasiliev, E.V. Phishing and Carding as Modern Forms of Internet Fraud. // Criminal Law. — 2022. — No. 4. — Pp. 73–79.

Zimin, I.V. Digital Crime: Challenges and Counteraction. — Moscow: Norma, 2022.