GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 5 May (2024)

HIDDEN DANGERS: ANATOMY OF BANKING FRAUD

Namozova Maftuna Utkirovna
Tashkent State Economic University 3rd Year, Group BIA-40
namozova.maftuna2004@gmail.com +998977333855

ABSTRACT

This article provides a comprehensive examination of the pervasive threat posed by banking fraud in the modern digital world. Delving into various forms and methods employed by fraudsters, the article elucidates complex techniques such as phishing, card cloning, fraudulent transactions, and malware. It exposes the severe consequences for consumers, including financial losses and compromise of personal information. However, the article not only highlights the risks but also equips readers with strategies to protect themselves, advocating for practices such as robust password management, vigilant transaction monitoring, and user education.

Keywords: Banking fraud, financial security, phishing, card cloning, fraudulent transactions, malware, fund loss, compromise of personal information, protective measures, fraud prevention, banking data security, bank account hacking, fraudulent schemes, cybersecurity, fake websites, network attacks, user deception, carding, internet fraud, privacy protection, transaction verification, secure online payments, antivirus programs, mobile security, two-factor authentication, biometric identification, financial transaction monitoring.

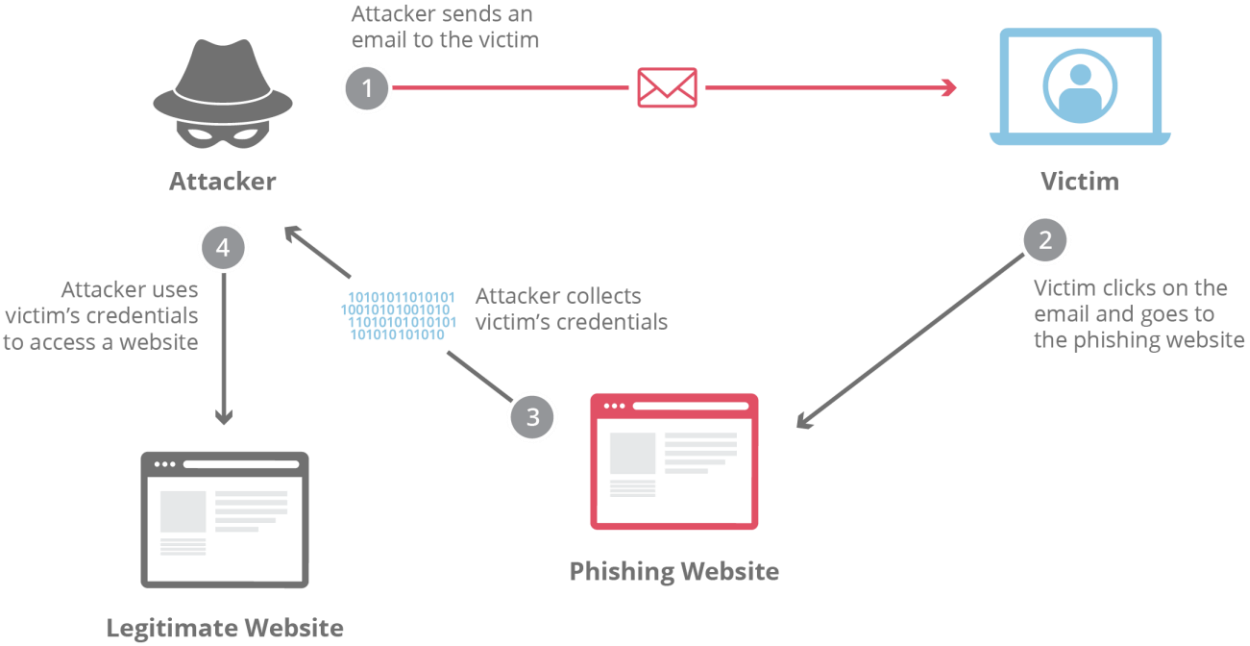
INTRODUCTION

The objective of this article is to furnish readers with a comprehensive comprehension of diverse forms of banking fraud along with their methodologies, while also extensively delving into the detrimental repercussions they entail for personal finances and security. The primary aim is to furnish concrete and efficacious strategies to thwart fraudulent assaults and safeguard financial assets and sensitive data, thereby ensuring security in the digital realm.

In light of an increasingly prevalent transition towards digital financial transactions, the imperative to address the issue of fraud in the banking sector becomes indisputable. Each passing day witnesses a surge in instances of fraud, posing grave threats to financial stability and the integrity of personal data. Understanding the myriad methods and tactics employed by fraudsters, and implementing requisite precautions, becomes imperative for all individuals engaging with banking services. Consequently, the exploration of this subject serves as a pertinent and invaluable resource, facilitating a more conscientious and secure utilization of banking services in the digital age.

Banking fraud constitutes criminal activities perpetrated with the aim of deceiving clients or banking systems to illicitly gain an advantage. This encompasses an array of methods and tactics geared towards the unlawful exploitation of financial resources and personal information. Among the primary forms of banking fraud are:

1.Phishing: This is a method of attack where malicious actors impersonate trusted senders, deceiving clients into providing their personal information such as credit card numbers, passwords, or other confidential details. This often occurs through emails, websites, or social media messages.



The scheme illustrates a phishing attack, which is a type of social engineering technique used to deceive individuals into providing sensitive information such as usernames, passwords, and credit card details. Here's a breakdown of the steps involved in this phishing scheme:

1.Attacker sends an email to the victim: The attacker crafts a deceptive email that appears to be from a trustworthy source, such as a bank, service provider, or a familiar contact. This email often contains a link and urges the victim to act by invoking a sense of urgency or fear.

2.Victim clicks on the email and goes to the phishing website: The link within the email redirects the victim to a fraudulent website. This website is designed to mimic a legitimate website, tricking the victim into believing they are visiting a real, secure site.

3.Attacker collects victim's credentials: On the phishing website, the victim is prompted to enter personal information, such as login credentials. Believing they are on a legitimate site, the victim submits the information, which is then captured by the attacker.

4.Attacker uses victim's credentials to access a website: With the stolen credentials, the attacker can now access the victim's accounts on legitimate websites, leading to identity theft, financial loss, or unauthorized transactions.

5.This diagram effectively outlines the flow and method by which phishing attacks are conducted and emphasizes the importance of vigilance when handling emails and personal information online.

2.Malicious Transactions: These are cases of manipulation with bank accounts or transactions using malware or compromised accounts to illegally transfer funds to other accounts or make purchases of goods and services.

3.Personal Data Theft: Criminals may gain access to clients' personal information through bank database breaches, data leaks, or phishing attacks to use this information for fraudulent activities, such as opening fake accounts or applying for loans in someone else's name.

4.Skimming: This is a method of obtaining confidential information from the magnetic stripes of bank cards by installing special devices (skimmers) on ATMs or payment terminals.

5.Carding: This involves using stolen bank information to make purchases or conduct transactions without the card owner's consent, often through the internet or a network of stores.

6.Use of Malware: Criminals may create and distribute malware such as viruses, Trojans, or spyware to hack into clients' computers or mobile devices and gain access to their bank accounts or personal information.

These forms of fraud represent serious threats to clients' financial security and require constant monitoring and appropriate precautionary measures from both banks and users.In the field of banking fraud, there is a worrying trend of increasing criminal activity. According to the Association of Certified Fraud Examiners (ACFE) report, over 40% of banking institutions reported an increase in fraud cases over the past year. Furthermore, over the last five years, the amount of financial losses from banking fraud has increased by more than 60%, reaching an impressive $20 billion according to the National Association of Cybersecurity and Infrastructure Protection (NACSI).

In 2023, statistics and trends in banking fraud show a significant increase in fraud losses. According to the Federal Trade Commission (FTC), fraud losses in the United States exceeded $10 billion, which is 14% more than the previous year. The majority of these losses are attributed to investment fraud, which amounted to over $4.6 billion.

According to experts from Kroll, most companies expect an increase in financial crime risks in the next 12 months, with significant attention being paid to improving technological means to combat these threats. Experian notes that fraud is becoming increasingly sophisticated, especially with the rise of artificial intelligence and big data used by fraudsters to impersonate identities and manipulate information. In addition to traditional forms of fraud, such as deposit account fraud and synthetic identity theft, there has been increased activity in areas related to social media and peer-to-peer payments.

One of the main dangers consumers face as a result of banking fraud is the loss of funds and personal information. When fraudsters gain access to bank accounts or clients' personal data, they can not only steal money from accounts but also use stolen information to commit other fraudulent activities, such as opening fake accounts or submitting false loan applications. This can lead to significant financial losses and personal security issues for affected consumers.

Banking fraud can have a serious impact on the credit and financial history of affected consumers. When fraudsters make unauthorized transactions or open fake accounts in other people's names, it can reflect on their credit report and score, making it difficult to obtain credit or conduct financial transactions in the future. Victims may face a lengthy process of

investigation and restoring their credit history, which can lead to additional stress and time and money expenses.

One of the most effective ways to protect against banking fraud is to use strong passwords and enable two-factor authentication. Strong passwords should be long and contain a combination of letters, numbers, and special characters to make them harder to crack. Two-factor authentication adds an additional level of security by requiring identity confirmation not only with a password but also through another method, such as sending a code to a mobile phone or using biometric data. Regular monitoring of banking transactions will help to timely detect suspicious activity on your account. This includes checking daily transactions and tracking any unusual or unauthorized operations. If you notice anything suspicious, immediately contact your bank to block the account or conduct additional verification.

Conducting educational programs and disseminating information about methods of banking fraud and signs of deception helps to increase awareness among consumers and makes them more resilient to fraudulent attacks. Training on how to recognize suspicious emails or websites, as well as how to properly respond to suspicious activity, plays a key role in protecting personal information and finances. When communicating with your bank or conducting banking transactions, it is important to use secure communication channels, such as official websites, mobile applications, or phone calls, to avoid interception or manipulation of information. It is also important to be cautious when dealing with strangers, especially online, and avoid providing personal information or agreeing to suspicious offers.

In conclusion, it becomes clear that banking fraud poses a serious threat to both the financial security of individual clients and the integrity of financial systems as a whole. The various methods and techniques used by fraudsters underscore the need for constant monitoring and effective protective measures to prevent losses and protect personal information. Combating banking fraud requires joint efforts from both banks and clients, as well as governmental and non-governmental organizations.

REFERENCES

1. Types of Fraud, Most Common, Types of Fraud in Banks and on the Internet, Types of Phone Money Fraud (sravni.ru) [Russian] (sravni.ru)https://www.sravni.ru/enciklopediya/info/vidy-moshennichestva/
2. Federal Trade Comission https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
3. Beware of Credit Card Fraud! - Central Bank of the Republic of Uzbekistan (cbu.uz) https://cbu.uz/ru/press_center/news/562943/
4. A Look Back: 2023 Biggest Fraud Trends https://www.experian.com/blogs/insights/biggest-fraud-trends/.