УДК 811.111

CYBERSECURITY IN THE FINANCIAL SECTOR: CHALLENGES AND PROTECTION STRATEGIES FOR BANKS
(КІБЕРБЕЗПЕКА У ФІНАНСОВОМУ СЕКТОРІ: ВИКЛИКИ ТА СТРАТЕГІЇ ЗАХИСТУ ДЛЯ БАНКІВ)

Задорожна О.В. – здобувачка вищої освіти групи Ф4/1
Науковий керівник: Матвєєва А.Л., викладач кафедри іноземних мов МНАУ

У статті розглядаються проблеми кібербезпеки у фінансовому секторі з огляду на сучасні реалії. Проаналізовано Інтернет-банкінг, як різновид банківських послуг. Були рекомендації та стратегії запобігання цим проблемам.
Ключові слова: *кібербезпека, фінансовий сектор, банк, дані.*

The article presents the problems of cybersecurity in the financial sector due to the modern reality. Internet banking, like a kind of banking services, was analyzed. There were recommendations and strategies to prevent these problems.
Key words*: cybersecurity, financial sector, bank, data.*

Cybersecurity is an important issue in today's world as such as our daily lives take place online. From online shopping and banking to social media and email, we rely on the Internet for a wide variety of activities. Unfortunately, this dependence also means that we are vulnerable to a growing range of cyber threats, including hacking, malware, phishing and other types of cyber-attacks.

Internet banking is one of the greatest assets of mankind in the banking sphere. However, along with the advantages, this direction also has disadvantages, risks and challenges. In general, banking, like other software applications that can provide access to money, is an attractive target for criminals. Also, today bank clients have to worry not only about how to protect their physical bank card and personal data, but also how to protect themselves, who have at their disposal a "significant" arsenal of various criminal schemes and methods of attacks for obtaining access to their money [3]. Mobile banking means using a special software application developed by the bank. This is different from online banking, which involves logging into the bank's website on your phone and/or computer. Surprisingly, this has some significance when considering security issues. Banks have more control over account security when using an app than when using a website [5].

Privat24 became the first internet banking in Ukraine. Privat24, as a mobile application, was first introduced in 2011 by PrivatBank, which had already been the leader of the domestic banking sector at that time. This mobile application has become an important tool for the bank's customers, which allows them to perform various banking operations precisely through mobile devices.

Table 1.

Security aspects

Bank	Changing the PIN in the application	3D-secure option to disable enhanced authentication	Management of verification of geolocation of the client and payee	Choosing your own CVV in the app	Management of tokenized applications	Management of application resource subscriptions
Monobank	+	+	+	+	+	+
Sense bank	+		+		+	+
Privat-Bank	+					+
Otpbank	+					
Raiffeisen	+					

Since the creation of Privat24, many banking applications have appeared in Ukraine, such as Monobank, Raiffeisen Online, Oshchad24, Alfa-Mobile and others. Each of these applications provides customers with convenient access to banking services using a mobile device and has certain security and user interface features. The EMA Association conducted a study in which these aspects were considered [4].

The only bank that contains all aspects is Monobank, which does not have a physical bank establishment.

Among the main problems faced by Internet banking, those shown in Chart. 1.

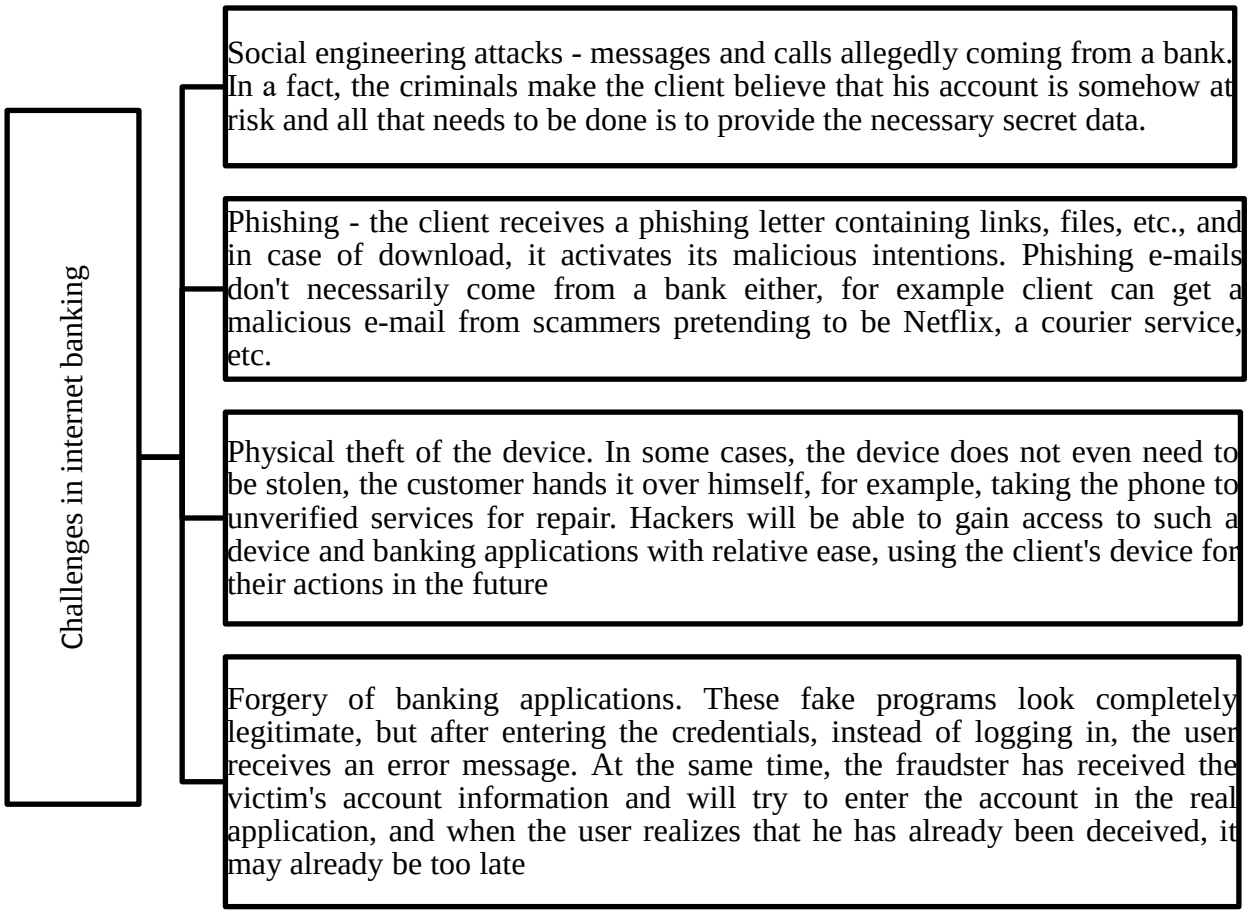

Chart 1. Challenges in internet banking

The diversity of threats in 2024 continues to evolve, shaping the future of banking. Employing effective security tactics is paramount for banks hoping to protect customer data and business assets. There are some of the best banking cybersecurity solutions and strategies, we can name them.

First of all, banks should invest in software to track all digital banking services. These services conduct monitoring and patching activities, which are crucial for maintaining a secure environment. Additionally, monitoring tools aid in mitigating third-party risks and can provide timely alerts to manage and minimize damages in case of a security breach.

Implement risk assessment as a cyber-security audit mechanism. Consistent evaluations of the existing defense framework enable institutions to adjust to emerging threats. By having a thorough understanding of possible security gaps, teams can fortify vulnerabilities or devise efficient incident response strategies, akin to those employed in red team versus blue team simulations. This enhanced resource allocation and decision-making process even empowers security professionals to proactively implement cybersecurity measures [1].

Encryption remains a priority in cyber security for banks. Data retention regulations have tightened, and fraudsters are launching more sophisticated attacks. All security of customer information in banks must be encrypted, whether it is at rest or in transit [2].

Access control is also important. Establish suitable access levels for all systems, applications, and data. For consumers, this entails implementing two-factor authentication or biometrics to enhance account security. For employees, it may require the limitation of privileged users using role-based access control (RBAC). For cybersecurity teams, this can mean tracking logins and logouts based on pre-defined rule sets.

Banks ought to allocate resources towards proactive network security solutions aimed at thwarting potential attacks on their extended banking networks. Firewalls and intrusion detection software serve to safeguard the perimeter, while segmentation and access control measures restrict lateral movements from compromised network areas. Denial of Service (DDoS) protection mechanisms can detect and mitigate malicious traffic, and Wi-Fi security protocols ensure the confidentiality of information during bank transfers.

Banks need to employ various innovative strategies aimed at safeguarding devices on the periphery. Among the potential options are Endpoint Detection and Response (EDR) and Mobile Device Management (MDM) solutions. These tools restrict unauthorized access and can assist in data deletion if a device becomes compromised. Additionally, educating employees about the risks associated with insecure devices and monitoring analytics can serve as proactive security measures.

The last important thing is Data loss prevention (DLP) systems refer to a set of tools designed to prevent data loss or misuse. Examples include intrusion detection systems or anti-virus software. Some solutions even offer special protection against known malware or ransomware. DLP tools are indispensable for preventing data leakage and offer a comprehensive way to strengthen information security in banks.

In summary, along with the improvement of the banking system, new methods appear to harm its security. We analyzed different peculiarities of this sphere and made recommendations how to pretend it and solve.

Література:

1. Adel Ismail AL-ALAWI* The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. Journal of Xidian University. 2020. No:1001-2400. P. 1523 – 1537.
2. Koteshov D. The State of Cybersecurity in Banking 2024. URL: https://anywhere.epam.com/business/cyber-security-in-banking
3. The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them. URL: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/
4. ЄМА. URL: https://www.ema.com.ua/
5. Логачова Є.В. Аналіз особливостей забезпечення кібербезпеки у банківських мобільних додатка. CS&CS. 2023. №1 (23). С. 63 – 74.