CYBERSECURITY IN BANKING

Rogozhkina N.U.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Perepelitsa L.A. – Lecturer

This scientific paper contains information about Cybersecurity politics in banks, its usage in banking and a brief description of the main threats accompanied by the enumeration of the possible ways to protect customers' sensitive data.

Cashless payment and the use of internet banking are as popular as ever these days. These methods are very useful and convenient as they make the payment process more flexible and faster, provide an opportunity of physical distancing, tracking expenses and guarantee financial security. But together with that, the banking and financial services sector faces almost three times more cyber-attacks than any other industry. Banks are where money is. Additionally, the banks also possess data of millions of users. So, for cybercriminals, attacking banks offers multiple avenues for profit through extortion, theft, and fraud. More and more, financial services organisations are operating under a constant state of attack, leaving IT and security teams challenged in their ability to collect, disseminate and interpret malicious events [1].

Cybersecurity politics in banks is a practice of protecting critical systems, information and customer's assets from malicious attacks and unauthorised access. To keep sensitive data secure, Cybersecurity in banks must be able to counter threats such as malware, unencrypted data, phishing, third-party services and spoofing.

Malware or malicious software is a special computer program aimed to gain access to personally identifiable information. The consequences of a malware attack can be very serious and their elimination is extremely difficult. To prevent the attack, it is important to download files only from secure sources, make use of licensed and up to date software. Also, personal data should not be shared in suspicious websites. A Password manager can also be used in order to avoid viruses [2].

Data encryption is a good method of data protection. The main idea of this method is translating data into another form. Data is turned into a code and only a special key or a password allows access to the information. It helps to make customers' private information more safe and secure, as cybercriminals are not able to make use even of stolen data. Unencrypted data is considered to be more vulnerable to cyber-attacks and can cause damage to either financial institutions or the end-users. It will not be superfluous to protect data with passwords, check and update current passwords with more secure ones.

Phishing refers to a cyber fraud consisting of mass e-mail sending on behalf of banks and financial organisations or private messaging in different services and social networks. These e-mails and messages can look like real bank correspondence and have a replicated logo of a trustworthy organisation. They may contain a request for downloading an attached document or a link to follow. Requests are usually written in a specific way to evoke users' sense of importance and urgency. Cybercriminals try to trick the recipients and discover their personal financial information such as an account number and a password.

It is worth mentioning that there are two more dangerous types of phishing: smishing and vishing. Smishing is a combination of words SMS and phishing. Vishing combines words voice and phishing.

Cybercriminals practicing smishing, use text messages instead of e-mails to acquire customers' sensitive data. Usually, a victim of smishing receives a message with a link that might be used to verify or reactivate a bank account. But actually, it leads to a fake website and a customer's phone number goes to a fraudster. To prevent a leak of personal information and an assets loss, it is enough just not to click on a malicious link, not to tell the PIN, and contact the bank assistant immediately. The Cybersecurity bank regulation introduce countermeasures to protect customer's data and find a fraudster out.

Vishing is a form of scam that is implemented with the help of phone calls. Victims of vishing are asked about their security, financial information and money transferring. Cybercriminals are usually interested in credit or debit cards' PINs. It is very important to report an incident to the bank and be aware of unsolicited telephone calls.

To be on the safe side and to protect personal information browsers, antiviruses, operating systems and mobile bank apps should always be updated. Great role plays the fact of paying attention to the style of mails and cases of poor grammar in identifying fraudulent activities. It would be helpful always to compare the address of a suspicious message with the previous correspondence from the bank. There are some rules that can help avoid an attempt of phishing: confidential information should never be shared, only trustworthy links should be followed, suspicious e-mail addresses and attachments should never be opened or downloaded.

To provide the best service to their customers, banks often use third-party services. One of the most popular third-party services is a Third-Party Provider. It is an authorised online service that can take part in online transactions.

One of the types of a Third-Party Provider called Payment Initiation Service Provider (PISP) is used to make online payments even without leaving a payment window. And another one, Account Information Service Provider (AISP), can view information about customers' balance, payments and transfers for a certain period of time [3]. These services work with extremely sensitive data. That is why vendors to whom third-party services belong to must assure an appropriate level of cybersecurity.

Not so long ago banks faced a new threat. Spoofing refers to the process of getting secure data with the help of a fake organisation's site. Cybercriminals create websites with the address that is similar to the address of a real bank's website. Their design and functions seem to be the same. When a user enters login credentials into corresponding fields, personal information is stolen. Fraudsters are able to use it later. Spoofing can also contribute to malware spreading and bypassing access control.

These threats have become increasingly serious with the time. Bank's Cybersecurity must be constantly improved to ensure all the customers in its ability of personal data protection.

To make it easier to track expenses and control a current account balance, additional limits can be added. It means that the accessible amount to spend without the permission must be as small as possible. For further operations with bigger sums, PIN must be entered. SMS or e-mail notifications for all the payments tracking should be enabled as well.

Multifactor authentication, also called two-factor authentication, should not be neglected too. Two-factor authentication means that before gaining access to a service or an account one more log in step must be passed. It increases log in security and guarantees safety of personal data.

There are various methods of two-factor authentication.

The easiest one is to set up a password and a keyword. Usually users remember them well. But it is not hard either for cybercriminals to figure them out.

Another method is SMS or e-mail messages. In order to log in the system a message with a unique security code is received. This method is convenient enough because a user can get an access to the service immediately. The main disadvantage of this method is the possibility of using a customer's phone number and personal information by not very trustworthy services and hacker attacks. A hacker can gain information from an SMS text.

Time-Based One-Time Passwords (OTP) are also deserved to be mentioned. Following this method, a user scans a QR code with a secret key that must be loaded into the app and creates a temporary password. It changes regularly. While logging in a user have to enter not only a password but also a code as the second step of two-factor authentication.

Push notification is also considered one of the most effective methods of two-factor authentication. User receives a notification with some information about the log in attempt after password is entered. It is enough to tap 'Approve' or 'Decline' in response to the request. Push notifications are highly advantageous as they contain information about each log in try. Device type, IP address, and general location are shown to the user. Additionally, as the push notification is tied to your phone, there is no risk of copying down the secret code or stealing an SMS [4]. One of the drawbacks of this method is the need of Internet connection availability on user's phone. It is important to be very careful and not to ignore push messages.

Face and voice recognition, fingerprint scans are widely spread nowadays. They fall under the category of biometrics. In case of a try to get access to the biometric security system, it scans, analyses and compares the information received with records that currently exist [5]. Due to rather low cost, fingerprint sensors are popular among biometric security systems. As it is almost impossible to forge the biometric data, this method is highly appreciated: it makes biometric security system extremely difficult to hack. The main reason why this technology is not used as extensively as it might be is that if user's biometrics are compromised, it is not possible to reset them. Equally significant is that most people are not comfortable about giving their fingerprints, voice and face to the companies. It is worth adding that environment has a great impact on the work of a biometric system. Low temperatures can cause fatal errors and lead to detrimental results.

As the world moves towards developing a digital society, the threat of cybercrime increases as well. Leveraging techniques and practices that are designed to protect sensitive data is paramount to Cybersecurity politics in banks. Whether it is an accidental breach or a well-planned cyberattack, the strength of Cybersecurity in banks determines the safety of personally identifiable information.

References:

1. Cybersecurity in Digital Banking: Threats, Challenges and Solution – [Electronic resource]. – Access mode: https://enterslice.com/learning/cybersecurity-in-digital-banking-threats-challenges-and-solution/ – Date of access: 29.03.2022.
2. Top 10 Most Dangerous Banking Malware That Can Empty Your Bank Account – [Electronic resource]. – Access mode: https://heimdalsecurity.com/blog/banking-malware-trojans/ – Date of access: 29.03.2022.
3. What's a Third-Party Provider (TPP) and How Does This Relate to Open Banking? – [Electronic resource]. – Access mode: https://help.bankline.rbs.com/help/other_services/third_party_providers/whats_a_TPP – Date of access: 29.03.2022.
4. The Pros and Cons of Two-Factor Authentication. Types and Methods – [Electronic resource]. – Access mode: https://www.makeuseof.com/tag/pros-cons-2fa-types-methods/ – Date of access: 29.03.2022.
5. Everything You Need To Know About Biometrics in Cybersecurity – [Electronic resource]. – Access mode: https://www.privacyaffairs.com/biometrics-in-cybersecurity/ – Date of access: 29.03.2022.