Digital Safety in Financial and Banking Institutions

Target Group

Financial and Banking Sector

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Digital Safety in Financial and Banking Institutions

Target group: Financial and Banking Sector


Privacy Policy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

January 2025

Doha, Qatar

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Contact the Cyber Excellence Department

00974 404 663 79

00974 404 663 62

www.ncsa.gov.qa/

academy@ncsa.gov.qa

Dear Participant,

In light of the rapid technological advancements and the pervasive presence of the internet in various aspects of life, cyber threats have become challenge all segments of society encounter. This necessitates efforts to raise awareness about digital safety concepts, which serve as the shield protecting society from these threats.

As part of the «National Initiative for Digital Safety» efforts to enhance digital safety indicators within society, the National Cyber Security Agency presents this booklet, with a collection of general tips and guidelines related to digital safety.

Table of Contents	Page

Introduction

As the financial and banking sectors embrace digital transformation, cyber risks have surged. The COVID-19 pandemic exacerbated these risks due to a sudden spike in remote access, cloud technologies, and cashless transactions. Despite the benefits of digitalization in the financial and banking sector, the risk of data breaches and cyberattacks haunts the sector institutions as well as all countries of the world due to the significant financial losses for the sector in the event of the success of such cyberattacks.

Therefore, it is important to enhance digital safety in the financial and banking sector to protect the future of this critical industry. To safeguard their systems and networks from cyber threats, financial and banking institutions are implementing a range of measures. Banks and financial and banking institutions are using specially designed tools and technologies to detect and prevent various attacks, such as hacking, data breaches, identity theft, malware, viruses, and unauthorized access to sensitive networks and data.

Financial institutions use cybersecurity measures to protect customer assets, prevent sensitive data loss, and avoid operational disruptions, and the subsequent financial losses and threats to customers. in order to implement these measures, security experts have been employed to monitor networks for suspicious activity and intervene quickly to prevent cyberattacks.

Financial institutions implement robust cybersecurity measures to protect their reputation and credibility. If a customer falls victim to malicious attacks, banks' and financial institutions' reputation will be damaged, and it may face hefty fines and legal penalties under the financial and banking sector regulations.

Today, the financial and banking sector is more vulnerable than ever to numerous threats due to the rise of mobile banking apps, third-party breaches, and the risks associated with cryptocurrencies. To effectively combat these threats, cybersecurity measures alone, such as security audits, advanced firewalls, and multi-factor authentication, are insufficient. It's imperative to extend these measures to include comprehensive awareness and education programs for employees within banks and financial institutions to promote secure practices.

Caution!

The financial and banking sector is now more vulnerable than ever to threats posed by mobile banking apps, third-party breaches, and the risks of cryptocurrencies.

Financial and banking sector here doesn't just mean traditional banks. This sector includes credit cards like Visa and Mastercard, payment processors like PayPal, online retailers like Amazon and Apple, and digital wallets. The emergence of cryptocurrencies like Bitcoin, used as an alternative to traditional money, has also made them a target for cybercriminals.

In addition, these institutions should invest in AI and machine learning to detect cyber threats immediately, ensuring compliance with cybersecurity standards. However, they must be vigilant about the dual-use nature of AI in cybersecurity. While AI can be used to defend against cyberattacks, cybercriminals can also leverage generative AI to launch sophisticated attacks, like crafting highly convincing phishing emails.

Did you know?

Cybercrime costs are projected to reach a staggering $10.5 trillion annually by 2025.

01

Chapter 1

Digital Safety in the Financial and Banking Sector

- Part 1: **Digital Safety of Financial and Banking Services**
- Part 2: **Importance of Digital Safety for Financial and Banking Services**
- Part 3: **Challenges of Digital Safety in Financial and Banking Institutions**

First: Digital Safety of Financial and Banking Services Digital

Technology is currently witnessing many continuous changes that impose complex security requirements to operate systems and achieve the required goals at work. Because of the sensitivity of financial and banking institutions' work and the critical services they provide, pressure is increasing on them to provide digital safety for their systems and networks in light of the escalation of internal and external cyber threats.

The importance of digital safety for financial and banking services comes due to the dangers surrounding sensitive personal data, such as bank details and passwords, in addition to unauthorized access from malicious actors using malicious attacks such as viruses. All of the above places the burden of securing systems, networks, and all work steps on the financial and banking institutions; first, to protect their customers' data, and second, to protect its reputation from damage in the event of data loss or breach.

Second: Importance of Digital Safety for Financial and Banking Services

The need to adopt cyber security strategies to protect the work of financial and banking institutions has become a must, especially with the digital development that started to be a key element in cash transactions, and the accompanying emergence of a variety of cyber threats and attacks that significantly affect banking operations, in addition to the inevitable financial losses for customers and institutions alike.

That is why the importance of digital safety for financial and banking services arises from the negative effects of potential cyber threats, which require institutions to adopt strong security standards to prevent data leaks, data loss and any kind of security violations.

Generally, the importance of digital safety for financial and banking institutions is due to the following:

Inefficient security standards in institutions lead to cybercriminals infiltrating, successfully carrying out their attacks, and stealing sensitive data. By the adoption of strong cybersecurity policies, these institutions can efficiently thwart those attacks.

The importance of digital safety depends not only on financial and banking institutions but also on customers themselves to avoid fraudulent practices, which target them in deceptive ways that cybercriminals use to allure victims to disclose their important financial data, such as credit card numbers. This, as a result, paves the way for unauthorized access to bank accounts and the theft of funds from them[1].

Cybercriminals resort to innovative fraudulent methods, such as offering fake and valuable gift offers at the same time, such as expensive computers, smartphones, and other gifts aimed at carrying out an enticing fraud for bank customers to disclose their sensitive data.

Caution!

Cybercriminals resort to innovative fraudulent methods, such as offering fake gift offers at the same time, such as expensive computers, smartphones, etc., to bank customers to reveal their sensitive data.

1. Narayanan, Lakshmi. Benefits and Importance of Cybersecurity in Banking Sector Teceze, February 2024. On site: https://teceze.com/cybersecurity-in-banking-importance-and-threats-challenges-benefits

Third: Cybersecurity Challenges in Financial and Banking Institutions

Cybercrime rates have significantly increased in recent years, making it the biggest threat to the financial and banking sector due to the diversity and complexity of hacker methods, which has made it difficult to defend against cyberattacks.

The following are the most important challenges facing cybersecurity in financial and banking institutions:

1. Mobile Banking Applications

Mobile banking is an online service provided by a bank or financial institution to customers to enable them to conduct their cash transactions through a phone or tablet. The service allows customers to directly access their available accounts or banking data.

With the increasing reliance on applications to conduct financial transactions and the lack of strong security measures, banking applications have become one of the most pressing concerns for financial and banking institutions because of the exposure to cyberattacks as cybercriminals tend to target less secure banking systems and anonymous (third party) networks for unauthorized access to networks and data, so this type of service is still subject to development to ensure the safe use by customers online.

There are various services offered by mobile banking applications, such as:

- Account information, including account history, monitoring deposits, card and loan data, and other sensitive data.
- History of financial transactions, such as money transfers between accounts, invoices payment, and deposit checks.
- Support services, such as credit requests, complaints, and ATMs location[1].
- Investment services, such as stock prices and notices related to securities prices.

Caution!

Digital safety is not just the responsibility of financial and banking institutions; customers must also be vigilant against fraudulent practices designed to trick them into revealing sensitive financial information, such as credit card numbers.

1. Mobile Banking: What are the Advantages and Imminent Challenges? The Salmon Factor, On site: https://thesalmonfactor.com/mobile-banking-advantages-and-imminent-challenges.

Thus, we see that mobile banking offers numerous benefits. It allows 24/7 access to banking services and reduces transaction costs and time.

With the surge in using smartphones and tablets for financial transactions, financial and banking institutions must now effectively address the challenges associated with this, **most importantly:**

Strict adherence to digital safety standards:

Mobile banking does require an internet connection, posing a challenge to banks, financial institutions, and app developers due to the threat of cybercrime[1].

App Security:

Beyond credit card security provided by financial and banking institutions, devices like phones and tablets need strong security measures protecting online transactions.

Device Authentication:

To prevent unauthorized devices from making financial transactions, financial and banking institutions must coordinate with customer devices through authentication before processing any financial transactions.

1. Banking on Security: Navigating the Cyber Threat Landscape in the Digital Age, the global treasurer, April 2024, on site: https://www.theglobaltreasurer.com/2024/04/04/banking-on-security-navigating-the-cyber-threat-landscape-in-the-digital-age/

Customer Behaviour:

A significant challenge faced by mobile banking services and data security is customer behaviour. Research has shown that more than half of users of these services exhibit risky behaviour and are unaware of the risks associated with fraud. This became evident when financial and banking institutions received numerous complaints from their customers, which upon review revealed that they did not enable two-factor authentication during financial transactions[1].

Time:

The use of banking applications is subject to time constraints; customers cannot use them for long periods or leave them open without use for a certain period as this increases the chances of fraudulent transactions. This makes the time factor one of the challenges facing these applications; as customers rely on them to accomplish many essential tasks, which requires that the applications be compatible with the customer's tasks and behaviour.

1. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/

Studies show that over **70% of users have felt frustrated** with a mobile banking application due to their inability to complete the required tasks in a timely manner, leading many of them to cancel their subscriptions or uninstall the application[1].

Did you know...?

A recent survey revealed a steady growth in mobile threats by 40% as online banking services have surged. 'Faketoken', a type of Trojan horse, has been identified as a primary culprit behind this increase. This malware is capable of stealing SMS codes sent to users for two-factor authentication[2].

1. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/
2. Alexander Eremin, The Faketoken Trojan sends out offensive texts, Kaspersky, January 2020. on site: https://www.kaspersky.com/blog/faketoken-trojan-sends-offensive-sms/32048/

2. Phishing Attacks

Phishing attacks are a common threat in the field of cybersecurity within the banking industry. The financial sector is the most targeted area by this type of cyberattacks. In 2023, more than 23% of phishing attacks worldwide targeted financial institutions. Cybercriminals pose as legitimate banks or financial institutions and carry out their attacks by sending fraudulent forms, misleading emails, or messages containing malicious links in order to obtain sensitive data[1].

The means by which cybercriminals carry out phishing attacks is to create a sense of urgency or panic; they deceive victims by making them believe that their accounts are facing suspicious activity, which requires them to provide their data immediately prompting hasty decisions.

Caution!

Cybercriminals use phishing attacks to create a sense of urgency or panic. They trick victims into believing their accounts are experiencing suspicious activity that requires immediate provision of their data, leading them to act without thinking.

1. Sasovets, Ihor. Cyber Security in Banking: How We Address Rising Challenges, Tech Magic, May 2024. on site: https://www.techmagic.co/blog/cybersecurity-in-banking/

There are examples of phishing attacks against financial and banking institutions, some of which are the following:

Carbanak

Financial and banking institutions are subjected to phishing attacks in various ways. For example, a group called 'Carbanak' targeted banking networks around the world, leading to the theft of more than one billion dollars, after the group issued orders to ATMs to dispense cash at specific times to their affiliated individuals[1].

An unprecedented cyber heist was uncovered through investigations involving Interpol, Europol, and authorities from various countries around the world; approximately one billion US dollars was stolen over two years from financial institutions worldwide. The attack was carried out by a multinational group of cybercriminals from Russia, Ukraine, and other European countries, as well as China.

1. The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide, Kaspersky, February 2015. on site: https://www.kaspersky.com/about/press-releases/2015_the-great-bank-robbery-carbanak-cybergang-steals--1bn-from-100-financial-institutions-worldwide

The criminal group, Carbanak, used sophisticated techniques to steal money directly from banks, bypassing users (customers). Operating since 2013, the group targeted up to 100 banks, electronic payment systems, and other financial institutions in 30 countries, including: Russia, the United States, Germany, China, Ukraine, Canada, Hong Kong, Taiwan, Romania, France, Spain, Norway, India, the United Kingdom, Poland, Pakistan, Nepal, Morocco, Iceland, Ireland, the Czech Republic, Switzerland, Brazil, Bulgaria, and Australia. The stolen amounts in each attack carried out by the group against banks were estimated at around 10 million dollars. Each attack took between two and four months starting from the infection of the first computer belonging to the bank or its subsidiaries, through phishing and malware to gain unauthorized access to internal networks and other computers; to follow the progress of transactions related to monetary transfers on the screens of employees in the targeted bank in order to mimic their activity and transfer and withdraw funds[1].

1. Robert E. Holtfreter & Adrian Harrington, Employees are the weakest links, part 1, Data breaches and untrained workers, fraud Magazine, May/June 2016.on site: https://www.fraud-magazine.com/article.aspx?id=4294992844

Dyreza Trojan Malware

Among the fraudulent attacks that have targeted financial and banking institutions is the Dyreza banking Trojan which mimics secure bank connections. It has been distributed to 100,000 devices worldwide[1].

Malicious software has targeted customers of British banks, including Barclays and HSBC, through malicious emails aimed at installing the Dyreza malware on their computers. These emails direct users to websites containing obfuscated JavaScript code, which subsequently installs a Trojan horse.

In just one day, 30,000 malicious emails were sent from servers in the UK, France, Turkey, the US and Russia, stealing users' online banking login credentials.

The Dyreza malware, once installed on users' devices, remains dormant until the user enters their login credentials on a banking

1. Stuart, Dredge, Banking trojan Dyreza generating 'tens of thousands' of malicious emails a day, The Guardian, February 2015. on site: https://www.theguardian.com/technology/2015/feb/16/banking-trojan-dyreza-malicious-emails

or financial institution's website. At this point, cybercriminals inject malicious JavaScript code, allowing them to steal login credentials and manipulate accounts secretly.

Dyreza malware was first discovered in 2014, and its attacks relied on deceptive emails that appeared to be official communications from banks. The alarming aspect of this malware is its ability to bypass the SSL security used in online banking services. As for mitigating the risks and threats posed by this malware, the responsibility lies primarily with the end-user or customer, rather than solely with the targeted financial and banking institutions[1]. For phishing attacks targeting financial and banking institutions, as seen in the previous examples, it has been observed that they have been carried out through fraudulent emails that could be easily detected as fake if the employee within the institution or the end-user (customer) was aware of fraud techniques. This necessitates cybersecurity awareness and digital literacy for both.

Did you know...?

- More than 90% of all successful hacking attacks begin with a phishing attack. Estimates suggest that the number of phishing emails has quadrupled in just one year; approximately 15 billion spam emails are sent daily, with half targeting or impersonating financial institutions[2].
- In 2016, one million banking Trojan attacks were discovered, representing a 30.6% increase over 2015. Approximately half of all phishing attacks involved redirecting users to a fake banking website or a page created to steal login credentials.

1. Chickowski, Ericka, Dyre New Banking Trojan, Dark Reading, June 2014. on site: https://www.darkreading.com/vulnerabilities-threats/a-dyre-new-banking-trojan.
2. Moramarco, Stephen. Phishing attacks in the banking industry, Info Secinstitute, January 2019. on site: https://www.infosecinstitute.com/resources/phishing/phishing-banking-industry/

3. AI- associated cyberthreats

The emergence of generative AI tools represents a massive technological leap, with its effects on the financial system ranging from benefits to harms. Theoretically, AI benefits the financial system, but practically, its overall impact is linked to how the challenges related to data, model development, and deployment are addressed at the level of financial institutions and the financial system as a whole.

If artificial intelligence tools are used extensively in the financial system, operational risks, including cyber risks, will increase.

Did you know...?

- Since late 2022, there has been a significant increase in interest in artificial intelligence, and the volume of jobs and innovations related to it has grown. Additionally, Google searches for terms related to artificial intelligence have surged since the launch of ChatGPT.
- According to a recent study, 64% of company CEOs believe that artificial intelligence will increase their productivity, while 40% of business owners expressed concern about the increasing reliance on technology[1].

1. Haan, Katherine & Rob Watts, How Businesses Are Using Artificial Intelligence In 2024, Forbes, Apr 2023. on site: https://www.forbes.com/advisor/business/software/ai-in-business/

Although artificial intelligence significantly enhances data processing and generation, data quality remains a concern surrounding its use in the financial and banking system. This is due to the biases or errors inherent in the data used to train artificial intelligence models.

Generally, if artificial intelligence models, including machine learning and deep learning models, rely on biased, incomplete, or erroneous data, the AI model is expected to produce unreliable or biased results. Given that modern AI models are more complex than traditional models, it has become necessary for employees to understand and reconstruct the predictions made.

If financial and banking institutions rely on incorrect artificial intelligence predictions when making decisions without verification, this can lead to economic losses and unregulated market fluctuations. Additionally, the complexity of artificial intelligence makes it difficult to pinpoint the root cause of errors or to justify any decision based on it, raising questions about who bears the responsibility for the resulting malfunctions and unexpected consequences.

Regarding the implications of AI for financial stability, if most financial institutions use the same underlying models or similar models provided by a limited number of providers, AI-based decisions are expected to suffer from similar biases and technological challenges. Financial stability is thus at risk, due to supplier concentration and high technological penetration. Conversely, if the number of institutions using AI is limited and there is an increase and diversification in the number of different technology providers, the risks arise partly based on the individual institutions' use cases.

However, if artificial intelligence technology spreads in financial institutions and the number of suppliers increases, the risks resulting from artificial intelligence at the micro-level will be tangible, leading to consequences for financial stability[1].

In conclusion, artificial intelligence can bring both benefits and risks at the level of financial institutions and the entire financial system. While it can benefit consumers, companies, and economy by potentially increasing the efficiency of financial intermediation through faster and more comprehensive information processing, supporting decision-making, and achieving financial stability, the technological challenges associated with artificial intelligence increase risks related to bias and misuse, leading to distortions in financial market outcomes and weakening the operational framework. In other words, it is a double-edged sword.

1. Narechania, Tejas N. and Sitaraman, Ganesh, An Antimonopoly Approach to Governing Artificial Intelligence, January 2024. on site: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=4597080

4. Cryptocurrencies-associated threats

Despite the developments in cryptocurrency markets and the attraction of many customers, traditional banks remain cautious about using them. According to a study conducted by the Association of Certified Anti-Money Laundering Specialists (ACAMS) and the UK Royal Institute of Chartered Surveyors, approximately 63% of respondents working in the banking industry viewed cryptocurrencies as a risk, rather than good opportunity for the financial and banking sector as claimed by some of them[1].

In addition to the fluctuations experienced by cryptocurrency prices (particularly Bitcoin), the reasons for this can be attributed to market size, liquidity, and the number of market participants, which makes cryptocurrency not a stable investment tool over time. Central bank digital currencies reduce the attractiveness of assets, the reason why some banks do not believe they can successfully enter this field. Additionally, the decentralized nature of cryptocurrency is seen as a tool to undermine the authority of central banks; therefore, some believe that these banks will not be able to control the money supply.

Caution!

Approximately 63% of respondents working in the banking industry perceive cryptocurrencies as a threat rather than a good opportunity for the financial and banking sector, due to the volatility of their prices.

1. Izenman, Kayla. this regulator wants to help banks embrace cryptocurrency, Rusi, October 2020. on site: https://rusi.org/in-the-news/regulator-wants-help-banks-embrace-cryptocurrency.

Moreover, crypto assets are not suitable for most individual investors, whether as an investment, a store of value, or a means of payment, due to their increasing financial losses. The risks of consumer protection include:

- Misleading information.
- Absence of rights and protections, such as complaint procedures or mechanisms for rights recovery.
- Complexity of transactions.
- Fraud and malicious activities, such as money laundering, cybercrime, hacking, and ransomware.
- Market manipulation resulting from a lack of price transparency and low liquidity.

Increased involvement of financial institutions could further fuel the growth of crypto assets, thereby increasing financial stability risks. This means that exposure to crypto assets on a capital basis by regulated institutions - especially if these assets are not backed by any underlying asset - could jeopardize capital, and have potential impacts on investor confidence, lending, and financial markets. In addition, financial institutions may face reputational risks.

Caution!

Customer protection against cryptocurrency risks includes misleading information and absence of rights and protection such as complaint procedures or mechanisms for rights recovery, complexity of transactions, fraud and malicious activities, such as money laundering, cybercrime, hacking, and ransomware, and market manipulation resulting from a lack of price transparency and low liquidity.

Challenges facing financial and banking sector include:

5G networks:

The widespread deployment of fifth-generation networks, with their increased bandwidth and reduced latency, has introduced new security challenges related to 5G network vulnerabilities. The opportunities for carrying out Distributed Denial of Service (DDoS) attacks are increasing.

Behavioural Biometrics:

Behavioural biometrics utilizes user behaviour patterns, such as typing patterns, mouse movements, and touchscreen gestures, to verify user identities. This technology can be leveraged to enhance security by continuously monitoring user interactions to prevent unauthorized access and fraudulent activities[1].

Ransomware development:

The evolution of ransomware attacks is expected to lead to more targeted and customized attacks. One of the advanced techniques introduced to ransomware is 'double extortion', which refers to the threat of leaking stolen data to exert additional pressure on victims.

1. Cyber Shockwave: Exposing the Major Finance Industry Breaches of 2023 and Critical Lessons Learnt. Data Dynamic Sinc, on site: https://www.datadynamicsinc.com/blog-cyber-shockwave-exposing-the-major-finance-industry-breaches-of-2023-and-critical-lessons-learnt/

Caution!

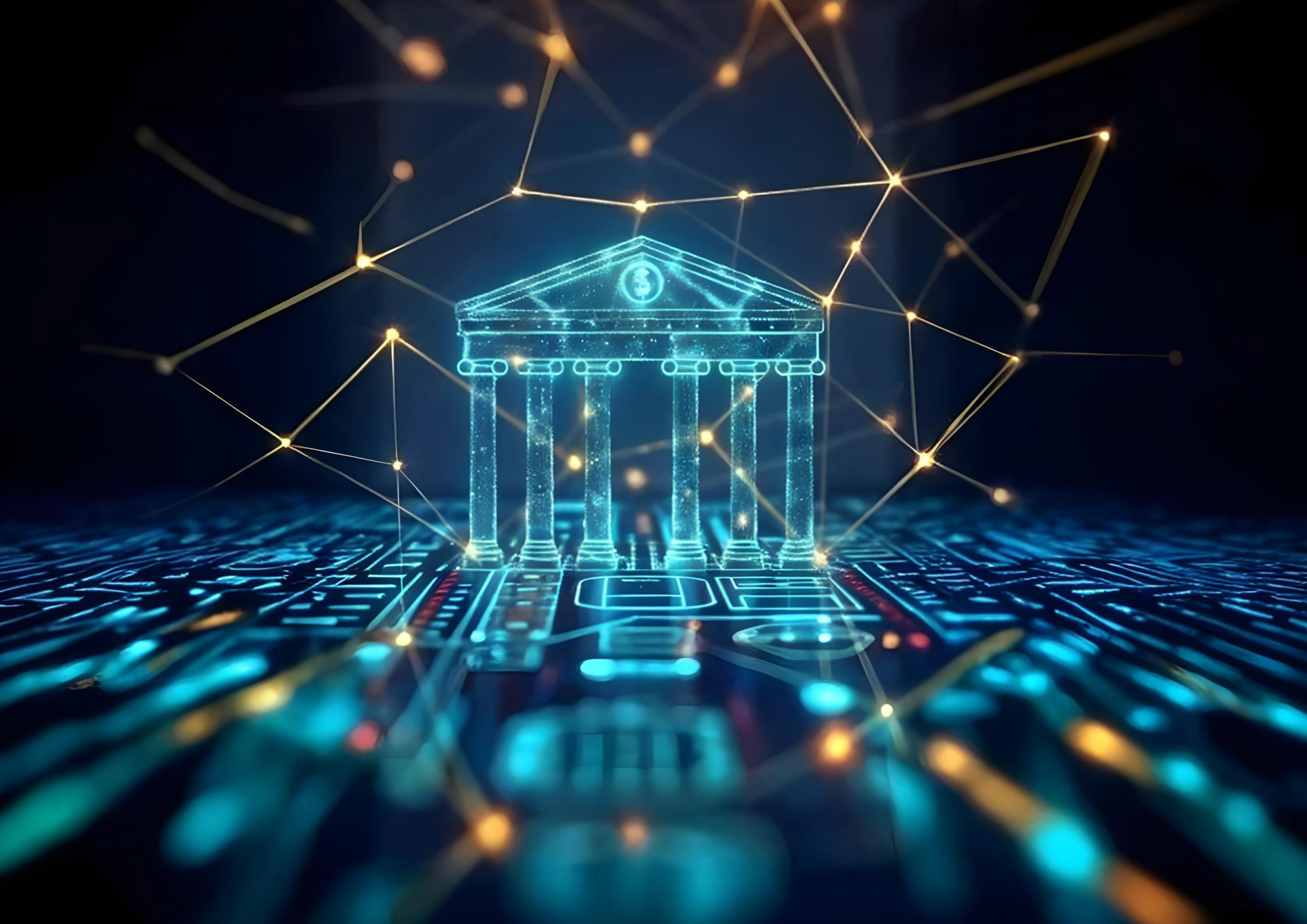
Among the advanced techniques introduced to ransomware is 'double extortion,' which seeks to threaten the leaking of stolen data to exert more pressure on victims.

Deepfakes and Identity Fraud:

Deepfake technology is used to create realistic fake audio and video content that mimics the original, with the aim of identity fraud and carrying out social engineering attacks.

Cloud Security:

With the increasing reliance on cloud data storage, the issue of securing cloud environments has become a pressing concern. Misconfigurations and insecure application programming interfaces can expose cloud services to breaches, leading to the theft of sensitive data.



02

Chapter Two

Strategies for Enhancing Digital Safety in the Financial and Banking Sector

- First: **Digital and Knowledge Gaps in the Financial and Banking Sector**
- Second: **The Role of Employees Within Financial and Banking Institutions in Achieving Digital Safety**

First: Digital and Knowledge Gaps in the Financial and Banking Sector

1. Knowledge Gaps

Knowledge gaps refer to the lack of cybersecurity awareness among employees in the financial and banking sectors; this allows criminals to deceive these employees and lure them into falling victim to phishing attacks, or to induce them to leak important banking information unknowingly. In general, the personal information and financial data held by financial and banking institutions make them clear targets. Cybercriminals achieve significant financial gains from this type of information, either by selling it on the dark web or by transferring funds from hacked personal accounts to their own accounts.

Therefore, internal vulnerabilities within banks and financial institutions are among the most dangerous loopholes exploited by these criminals. Notably, these vulnerabilities may be unintentionally created by employees.

2. Increasing number of users of financial and banking services

With a shortage of cybersecurity professionals and an increasing number of users of financial and banking services, this has led to a vulnerability in the financial and banking sector. Institutions are forced to deal with a diverse range of contact points, over which they have little control regarding how these users interact, giving cybercriminals more opportunities to carry out their attacks.

Personal devices of users can be exploited by cybercriminals to infiltrate financial networks, especially if users do not enable security features such as multi-factor authentication. In the face of this threat, it is important to implement policies to protect network users. These policies should help secure internal connection points, such as multi-factor authentication and access rights reviews. Additionally, features like Risk-Based Authentication (RBA) can apply the appropriate level of authentication based on the user's circumstances, such as whether they are connecting to the network locally or remotely[1].

1. Nair, Ajit. What is Risk-Based Authentication and why banks should implement it? Wibmo, on site: https://wibmo.co/what-is-risk-based-authentication-and-why-banks-should-implement-it/

3. Technology Gap

Financial and banking websites and applications have become vulnerabilities in the infrastructure of financial and banking institutions; they have been the most susceptible to hacking. A recent study found that 80% of the websites tested were vulnerable to cross-site scripting (XSS) attacks, which enable cybercriminals to execute malicious code on a website or application and thus gain access to user cookies and all sensitive data[1].

Caution!

Financial and banking websites and applications represent a significant vulnerability within the financial and banking infrastructure; they have been the most susceptible to breaches. Cross-site scripting (XSS) attacks have posed the most prominent threat to 80% of websites examined in one study.

These vulnerabilities lead to a lack of trust between the user and the institution. Therefore, for financial and banking institutions to be able to compete and mitigate cyber risks, they must secure their websites and applications. This includes developers testing the code during the application development phases and assessing the applications' ability to withstand hacking attempts.

1. Whittaker, Zack, Bank web apps are the "most vulnerable" to getting hacked, new research says, ZD NET, April 2018. On site: https://www.zdnet.com/article/bank-sites-and-web-apps-are-most-vulnerable-to-hackers/

Enabling web application firewalls, whether they are software, dedicated hardware, or standard device firewalls, helps prevent unauthorized access to administrative sections of websites or financial and banking applications.

Did you know?

1. 95% of cybersecurity issues resulted from human errors.
2. A cyberattack takes place every 39 seconds.
3. The estimated cost of data hacking in 2023 globally is 4.45 million dollars.
4. 15% of institutional breaches resulted from lost devices, whether they were institution-owned or personal devices.

Caution!

15% of data breaches in financial and banking institutions were caused by lost devices, whether they were institution-owned devices or personal devices belonging to employees.

Second: The role of employees within financial and banking institutions in achieving digital safety

Employees represent the human firewall and the first line of defence against cyber threats faced by financial and banking institutions. The more cybersecurity skills an employee possesses, the better equipped the institution is to prevent potential security breaches. This responsibility does not solely rest on the IT department; every employee has a crucial role to play.

Therefore, employees should be made aware of the following:

- Employee empowerment through digital safety awareness; awareness programs equip employees with the necessary skills to identify phishing attempts, social engineering tactics, and understand the importance of strong password practices[1].
- Incident reporting: Encouraging a culture of transparency is essential to motivate employees to report suspicious activities promptly and take advantage of open communication channels between employees and the IT department.

1. Henning, Jon, Explaining the Crucial Role Employees Play in Cybersecurity, Coordinated Business Systems, January 2024. on site: https://2u.pw/jPXiKXee.

- With the global trend of remote work, new challenges have emerged that have forced organizations to secure both their internal and external environments. This has created a need to increase the awareness of the workforce regarding the importance of securing the work environment around them, such as ensuring the security of Wi-Fi connections, updating antivirus software, and using encrypted communication channels.
- The ongoing evolution of cyberattacks has created an urgent need for adherence to regular updates and communication from the IT department, keeping employees informed about emerging threats.
- Employees must recognize that the company's email is not merely a communication tool, but also a gateway for phishing attacks and data breaches. They must understand that the threat of cyberattacks is imminent and that they, their customers, and the entire organization are potential targets.
- Once employees know how to identify suspicious or fraudulent emails, phishing attacks can be reduced by 60%[1].
- Digital safety training reduces the internal chaos caused by breaches.
- Adherence to the security policies and practices adopted within the organization, such as password creation rules, access controls, and data sharing.

1. The Role of Employee Training in Cybersecurity for Banks. Register Bank, on site: https://register.bank/media/cybersecurity-employee-training-banks/

Exercises are based on the material presented in this booklet, and provided here without answers. An answer key is provided at the end of the booklet.

Exercise 1

- **Choose the correct answer**

1. Inadequate security standards in financial and banking institutions lead to.....

1. Data theft.
2. Infiltration by cybercriminals.
3. Customer hacking.
4. All the above.

2. The increasing use of AI tools in the financial system causes.....

1. Emergence of herd behaviour.
2. Customer discrimination.
3. Increased operational risk.
4. All the above.

3. Consumer protection risks arising from investing in cryptocurrencies include.....

1. Circulation of accurate information that raises customer concern.
2. Absence of rights and protection.
3. Ease of transactions.
4. All the above.

4. One of the threats resulting from the use of cryptocurrencies as a result of the use of Blockchain technology is.....

1. Social engineering attacks.
2. Phishing.
3. Money laundering.
4. All the above.

5. The evolution of ransomware attacks is expected to result in more targeted and customized attacks. Among the advanced technologies introduced into them are.....

1. Reverse blackmail.
2. Dictionary attacks.
3. Double blackmail.
4. All the above.

6. One of the recommendations to mitigate supply chain risks is

1. Reducing investment in technology.
2. Utilizing surveillance and early warning systems.
3. Stabilizing the supplier base.
4. All the above.

7. Weaknesses in the cybersecurity of the financial and banking sector include

1. Incorrect configuration of systems and servers.
2. Retention of personal information and financial data.
3. Reliance on third-party vendors.
4. All the above.

Exercise 2

Mark the following statements as (True) or (False), and correct and errors if found:

1. Used devices such as phones and tablets require strong security measures to protect financial transactions conducted through them online. (.....)

.....

2. Coordination between financial and banking institutions and customer devices before transactions can help prevent unauthorized access. (.....)

.....

3. The widespread use of artificial intelligence tools in the financial system helps to reduce operational and cyber risks. (.....)

.....

4. Although artificial intelligence enhances data processing and generation, data quality remains a concern surrounding its use in the financial and banking system. (.....)

.....

5 complexity of artificial intelligence does not reflect on its ability to identify root causes and make decisions quickly and clearly. (.....)

.....

6 Among the services provided through mobile banking applications are investment services such as stock prices and notifications related to securities prices. (.....)

.....

7 Phishing attacks are a common threat to the banking industry. (.....)

.....

8 Customer behaviour does not pose a challenge to the services provided by financial and banking institutions. (.....)

.....

9 Banking services applications break the constraints of time, as customers can use them for extended periods or leave them open without use for a while. (.....)

.....

10 Data quality is one of the benefits resulting from the use of artificial intelligence in financial and banking institutions. (.....)

.....

Exercise 3

Complete the following sentences:

1. ..... is an online service provided by a bank or financial institution to enable customers to conduct their financial transactions through a mobile phone or tablet. The service allows customers to directly access their available accounts or banking data.

2. Without ....., financial and banking institutions cannot cope when a cyberattack or security breach occurs, as it mitigates the resulting effects.

3. The means by which cybercriminals carry out phishing attacks is.....; Where they deceive victims by making them believe that their accounts are facing suspicious activity.

4. Among the advanced technologies that have been introduced to ransomware.....which leaks the stolen data to exert more pressure on the victims.

5. ..... is a technology used to create audio and video content that imitates the original with the aim of identity theft.

6. Cybercriminals resort to innovative fraudulent methods such as..... to carry out a tempting fraud scheme targeting bank customers to reveal their sensitive data.

7. It is necessary for financial and banking institutions to coordinate with customer devices through..... before conducting financial transactions to prevent unauthorized devices from making financial transfers.

8. The risks to consumer protection arising from encrypted assets include ....., ..., ...

9. The widespread deployment of 5G networks has significantly increased opportunities for the execution of .....attacks.

10. ..... uses user behaviour patterns, such as typing patterns, mouse movements, and touchscreen gestures, to verify user identities.

Answers of the Exercises

Question

Exercise 1: Choose the correct answer.

Answer

1. All the above.
2. All the above.
3. Lack of rights and protection.
4. Money laundering.
5. Double extortion.
6. Using monitoring and early warning systems.
7. All the above.

Question

Exercise 2: Mark the following statements as (True) or (False), and correct and errors if found:

Answer

1. True.
2. True.
3. False; the widespread use of AI tools leads to increased operational risks, including cybersecurity risks.
4. True.
5. False; the complexity of AI makes it difficult to identify the root cause of errors or justify any decision based on it, raising the question of who is responsible for the consequences of any failures and their unexpected outcomes.

6. True.

7. True.

8. False; one of the challenges facing mobile banking services and data security is customer behaviour. Research has shown that more than half of users of these services exhibit risky behaviour and are unaware of the risks associated with fraud.

9. False; the use of mobile banking applications is not subject to time constraints; a customer cannot use them for a long time or keep them open without use for a period, as this increases the chances of fraudulent transactions.

10. False; rather, it is one of the concerns surrounding its use in the financial system, because of biases or errors inherent in the data on which AI models were trained.

Question

Exercise 3: Complete the following sentences:

Answer

1. Mobile phone banking
2. Incident response plan
3. Creating a sense of urgency and panic
4. Double extortion
5. Deep Fake

6 Gift offers

7 Authentication

8 Misleading information, Lack of rights and protection, Fraud and malicious activities

9 Distributed Denial of Service (DDoS)

10 Behavioural biometrics

References

1. Narayanan, Lakshmi. Benefits and Importance of Cybersecurity in Banking Sector Teceze, February 2024. On site: https://teceze.com/cybersecurity-in-banking-importance-and-threats-challenges-benefits
2. Mobile Banking: What are the Advantages and Imminent Challenges? The Salmon Factor, On site: https://thesalmonfactor.com/mobile-banking-advantages-and-imminent-challenges.
3. Banking on Security: Navigating the Cyber Threat Landscape in the Digital Age, the global treasurer, April 2024, on site: https://www.theglobaltreasurer.com/2024/04/04/banking-on-security-navigating-the-cyber-threat-landscape-in-the-digital-age/
4. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/
5. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/
6. Alexander Eremin, The Faketoken Trojan sends out offensive texts, Kaspersky, January 2020. on site: https://www.kaspersky.com/blog/faketoken-trojan-sends-offensive-sms/32048/

7. Sasovets, Ihor. Cyber Security in Banking: How We Address Rising Challenges, Tech Magic, May 2024. on site: https://www.techmagic.co/blog/cybersecurity-in-banking/

8. The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide, Kaspersky, February 2015. on site: https://www.kaspersky.com/about/press-releases/2015_the-great-bank-robbery-carbanak-cybergang-steals--1bn-from-100-financial-institutions-worldwide

9. Robert E. Holtfreter & Adrian Harrington, Employees are the weakest links, part 1, Data breaches and untrained workers, fraud Magazine, May/June 2016. on site: https://www.fraud-magazine.com/article.aspx?id=4294992844

10. Stuart, Dredge, Banking trojan Dyreza generating 'tens of thousands' of malicious emails a day, The Guardian, February 2015.onsite:https://www.theguardian.com/technology/2015/feb/16/banking-trojan-dyreza-malicious-emails

11. Chickowski, Ericka, Dyre New Banking Trojan, Dark Reading, June 2014. on site: https://www.darkreading.com/vulnerabilities-threats/a-dyre-new-banking-trojan

12. Moramarco, Stephen. Phishing attacks in the banking industry, Info Secinstitute, January 2019. on site: https://www.infosecinstitute.com/resources/phishing/phishing-banking-industry/

13. Haan, Katherine & Rob Watts, How Businesses Are Using Artificial Intelligence In 2024, Forbes, Apr 2023. on site: https://www.forbes.com/advisor/business/software/ai-in-business/

14. Narechania, Tejas N. and Sitaraman, Ganesh, An Antimonopoly Approach to Governing Artificial Intelligence, January 2024. on site: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=4597080

15. Izenman, Kayla. this regulator wants to help banks embrace cryptocurrency, Rusi, October 2020. on site: https://rusi.org/in-the-news/regulator-wants-help-banks-embrace-cryptocurrency.

16. Cyber Shockwave: Exposing the Major Finance Industry Breaches of 2023 and Critical Lessons Learnt. Data Dynamic Sinc, on site: https://www.datadynamicsinc.com/blog-cyber-shockwave-exposing-the-major-finance-industry-breaches-of-2023-and-critical-lessons-learnt/

17. Nair, Ajit. What is Risk-Based Authentication and why banks should implement it? Wibmo, on site: https://wibmo.co/what-is-risk-based-authentication-and-why-banks-should-implement-it/

18. Whittaker, Zack, Bank web apps are the “most vulnerable” to getting hacked, new research says, ZD NET, April 2018. On site: https://www.zdnet.com/article/bank-sites-and-web-apps-are-most-vulnerable-to-hackers/

19. Henning, Jon, Explaining the Crucial Role Employees Play in Cybersecurity, Coordinated Business Systems, January 2024. on site: https://2u.pw/jPXiKXee.

20. The Role of Employee Training in Cybersecurity for Banks. Register Bank, on site: https://register.bank/media/cybersecurity-employee-training-banks/