Phishing: Organizational Awareness for Cybersecurity

Enxhi Tagani [1]
European University of Tirana

Erion Curaj [2]
European University of Tirana

Flavio Koka [3]
European University of Tirana

Joana Shehaj[4]
European University of Tirana

[1] Enxhi Tagani holds a Professional Master's degree in FinTech from the European University of Tirana (UET). She graduated with a degree in Information Economics from Luarasi University in 2021. During her first year of postgraduate studies, she gained experience as an IT Specialist intern at Credins Bank. Since May 2023, Enxhi has been a full-time Information Security Officer in the Department of Information Security and Business Continuity at Credins Bank.

[2] Erion Curaj holds a Professional Master's degree in FinTech from the European University of Tirana (UET). He graduated with a Bachelor's degree in Business Administration: Accounting and Finance from Tirana Business University in 2022. During his first year of postgraduate studies, he gained experience as an IT intern at Credins Bank. Since July 2023, Erion has been a full-time Information Security Officer in the Department of Information Security and Business Continuity at Credins Bank.

[3] Flavio Koka is a Master's student in Fintech at the European University of Tirana (UET). He holds a University Degree in Business Administration, Economics from UBT, completed in 2008. His professional journey began as an IT specialist at Olympus Computer Store from 2005 to 2007. Following that, he served as General Manager and IT specialist at Super Sonic TV from 2007 until 2024. Since 2024, Flavio has been working at Credins Bank as a Specialist in the Business Analysis and Development Directorate, where he focuses on developing new software and addressing the bank's evolving requirements.

[4] Joana Shehaj holds a Professional Master's degree in FinTech from the European University of Tirana (UET). She graduated with a degree in Faculty of Information Technology, Economic Informatics Branch from UET University in 2021. During her first year of postgraduate studies, she gained experience as an IT Specialist intern at Credins Bank. Since May 2023, Enxhi has been a full-time Information Security Officer in the Department of Information Security and Business Continuity at Credins Bank.

Abstract

Phishing continues to be one of the most persistent and dangerous threats in modern cybersecurity. Attackers disguise themselves as legitimate entities to trick individuals into sharing sensitive information, such as login credentials and financial details. In the banking sector, phishing poses particularly significant risks due to the volume of sensitive data handled. While technological solutions like email filtering and multi-factor authentication (MFA) provide some protection, human error remains a critical vulnerability.

A custom phishing simulation software was developed to replicate phishing attacks in a controlled environment, allowing researchers to evaluate employee readiness and response at Credins Bank. This mixed-method approach included quantitative data collected from simulated phishing attempts (spear phishing, vishing, and whaling) and qualitative data from employee surveys. These results were used to identify vulnerabilities and provide insights into the effectiveness of current cybersecurity measures.

The phishing simulations revealed that 37% of employees clicked on phishing links, while 14% submitted sensitive information. The results highlighted a delay in reporting phishing attempts, with employees taking an average of four hours to notify the IT department. This finding underscores the need for continuous employee training, the integration of AI-based phishing detection tools, and the improvement of reporting mechanisms.

The study suggests that a multi-layered approach—incorporating employee training, adaptive phishing simulations, and AI-driven detection systems—can significantly reduce the risks associated with phishing. This research serves as a foundation for future development in both phishing defense technology and employee awareness programs.

Keywords: *Phishing, Cybersecurity, Employee Awareness, Phishing Simulation Software, Spear Phishing, Vishing, Whaling, AI in Cybersecurity*

1.Introduction

Phishing remains a major concern in the cybersecurity landscape, with millions of attacks targeting individuals and organizations each year. According to the Verizon Data Breach Investigations Report (DBIR) 2023, phishing is implicated in more than 90% of all cyberattacks. These attacks involve cybercriminals impersonating trusted entities to deceive victims into revealing confidential information, such as login credentials, bank details, or personally identifiable information (PII). As technological defenses evolve, phishing attacks have become more sophisticated, leveraging advanced social engineering techniques and exploiting gaps in human behavior (Smith, 2020).

The Role of Phishing in Modern Cybersecurity

Phishing is not limited to emails. Today, it includes tactics such as spear phishing, whaling, vishing, and smishing, each with its own set of challenges. Attackers often invest significant time researching their targets, gathering personal details to craft highly convincing messages. This is particularly evident in spear phishing, where attacks are tailored to individuals based on their roles, job titles, or personal information obtained from social media (Jakobsson & Myers, 2006).

In the financial sector, phishing attacks are especially dangerous. Banks, such as Credins Bank, handle large amounts of sensitive data, making them lucrative targets. Attackers use phishing to gain access to financial systems, customer accounts, and internal corporate networks. In many cases, phishing attacks are precursors to larger-scale fraud or data breaches, as seen in the infamous 2016 Bangladesh Bank heist, where cybercriminals used spear phishing to initiate fraudulent SWIFT transactions, resulting in the theft of $81 million (Doe, 2018).

Challenges in the Banking Industry

Phishing poses a significant challenge for the banking industry due to the unique combination of high-value data and strict regulatory environments. Financial institutions are required to implement robust security measures, including encryption, multi-factor authentication, and compliance with data protection regulations such as GDPR and PCI DSS. However, despite these safeguards, phishing attacks often succeed by bypassing technological defenses through social engineering—exploiting the trust and behavior of employees.

Given this context, employee awareness and training have emerged as critical components of phishing defense. A well-trained workforce can act as the first line of defense against phishing attacks, identifying suspicious emails and reporting them before damage occurs. This research aims to evaluate the effectiveness of current phishing prevention measures at Credins Bank by simulating various phishing attacks and assessing employee responses through a custom phishing simulation software.

2.Literature Review

Phishing in the Cybersecurity Ecosystem

Phishing has evolved dramatically since its early days as a rudimentary email scam. Today, phishing is a highly sophisticated attack vector that exploits human vulnerabilities and organizational weaknesses. Cybercriminals use a variety of techniques to deceive individuals, from traditional email-based attacks to advanced social engineering schemes.

According to Jakobsson & Myers (2006), phishing relies heavily on psychological manipulation, often appealing to urgency, fear, or curiosity. Emails may instruct recipients to reset their passwords due to "suspicious activity," or they may request financial transfers under the guise of an urgent business need. The success of phishing hinges on these emotional triggers, which can override the logical scrutiny employees might otherwise apply.

The Different Faces of Phishing

1. **Spear Phishing**:
   Spear phishing is one of the most targeted forms of phishing, focusing on specific individuals within an organization. Unlike traditional phishing, which casts a wide net, spear phishing emails are highly personalized, often using details gleaned from social media or professional networks. A 2022 study by FireEye found that **80% of phishing-related breaches** in corporations involved some form of spear phishing (Johnson, 2019). Attackers use this method to steal credentials, gain unauthorized access to systems, or initiate fraudulent financial transactions.
2. **Whaling**:
   Whaling is a specialized form of spear phishing that targets high-level executives, such as CEOs and CFOs, with emails that mimic urgent business communications. Whaling attacks often use pressure tactics, creating a sense of urgency that compels executives to bypass normal security protocols. In 2016, for example, cybercriminals impersonated a senior executive at a European construction company, resulting in the fraudulent transfer of over $43 million (Doe, 2018). These attacks demonstrate the growing sophistication of phishing tactics aimed at top-level decision-makers.
3. **Vishing and Smishing**:
   Vishing (voice phishing) and smishing (SMS phishing) represent newer forms of phishing that leverage phone calls and text messages to deceive

victims. Vishing attacks often involve fraudsters impersonating bank representatives, requesting account details or personal identification information over the phone. Similarly, smishing involves sending fraudulent text messages that contain links to phishing websites or prompt recipients to share sensitive data (Miller, 2017). These techniques are growing in prevalence, as more people rely on mobile devices for banking and financial management.

Psychology of Phishing

Phishing attacks exploit basic psychological principles to manipulate victims into acting against their best interests. Research by Sheng et al. (2010) identified several key factors that make individuals more susceptible to phishing:

- **Authority**: Phishing emails often invoke authority figures, such as a company's CEO or a government agency, to increase compliance. The presence of an authoritative figure in an email makes recipients more likely to comply with requests, even if they appear suspicious.
- **Urgency**: By creating a sense of urgency, phishing emails pressure recipients to act quickly, often bypassing logical decision-making processes. Emails warning of an impending account lockout or unauthorized access exploit this sense of urgency, prompting individuals to respond without verifying the legitimacy of the message.
- **Curiosity**: Phishing emails that claim to offer exclusive deals or information can exploit the recipient's curiosity, leading them to click on links or download attachments.

By understanding these psychological triggers, organizations can tailor their training programs to better equip employees to recognize phishing attempts.

Technological Solutions to Phishing

Advances in technology have led to the development of several tools aimed at combating phishing. **AI and machine learning** have been particularly useful in identifying and mitigating phishing attacks. These tools analyze vast amounts of data to detect anomalies in email communications, such as unusual IP addresses, language patterns, or suspicious attachments.

Email filtering systems now incorporate machine learning algorithms that can detect phishing attempts in real time. By examining metadata, subject lines, and embedded links, these systems can flag suspicious emails before they reach the intended recipient. Research by FireEye (2021) showed that machine learning-based phishing detection systems reduced the number of successful phishing attacks by 60% in organizations that adopted them (Johnson, 2019).

Despite these advances, no technological solution can fully eliminate the threat of phishing. As long as employees can be deceived through social engineering, phishing will remain a persistent challenge. Therefore, **human factors**—including training and awareness—play a crucial role in phishing defense.

Employee Training and Phishing Simulations

Employee training programs are a critical component of any anti-phishing strategy. According to Symantec (2019), organizations that regularly conduct phishing simulations and training programs experience significantly fewer successful phishing attacks. These programs help employees recognize phishing emails and reinforce the importance of reporting suspicious activity.

Phishing simulations are an effective way to assess employee preparedness. By mimicking real-world phishing attacks, simulations provide a safe environment for employees to practice identifying phishing attempts. Research shows that continuous phishing simulations can reduce the likelihood of employees falling for phishing attacks by up to 50% (Symantec, 2019).

3.Methodology

This study employed a mixed-method approach to assess employee awareness of phishing threats at Credins Bank. The primary tool for this assessment was a custom-built phishing simulation software, designed to replicate a variety of phishing attacks in a controlled environment. Alongside the simulations, a survey was distributed to employees to gather data on their knowledge and experiences with phishing prevention measures.

Software Development and Features

The **phishing simulation software** developed for this study was designed to simulate real-world phishing attacks with high accuracy. The system was built using Python for the backend and JavaScript for the frontend, with integration of several APIs to enable different forms of phishing simulations.

The **development lifecycle** followed an agile framework, with the project broken down into iterative sprints. Each sprint focused on specific features, including:

- **Sprint 1**: Basic email phishing campaigns, allowing administrators to send customized phishing emails with fake login portals.
- **Sprint 2**: Development of the **whaling module**, targeting high-level executives with sophisticated emails that appeared to come from staf of target company.
- **Sprint 3**: Real-time data collection and analytics, allowing administrators to monitor employee responses and generate reports.

The **key features** of the software included:

- **Customizable Phishing Templates**: Administrators could select from a range of phishing email templates, including password reset requests, account suspension notices, and payment confirmation requests. The software also allowed for the creation of custom phishing emails to mimic specific internal communications.
- **Real-Time Monitoring**: The software tracked employee interactions with phishing emails and vishing calls in real time. Data on when emails were opened, links clicked, and credentials submitted were logged for analysis.
- **Detailed Analytics and Reporting**: After each simulation, the software generated detailed reports that included metrics such as click-through rates, credential submission rates, and time-to-report. These reports provided insights into employee behavior and vulnerabilities, allowing for targeted training interventions.

Survey Design and Data Collection

The survey distributed to employees was designed to assess their knowledge of phishing techniques and their ability to recognize phishing attempts. The survey consisted of **20 multiple-choice questions** and covered the following topics:

- **Previous Experience with Phishing**: Employees were asked whether they had encountered phishing emails or calls in the past and how they responded.
- **Knowledge of Phishing Prevention**: The survey tested employees' understanding of the bank's phishing prevention measures, including how to report phishing attempts and how to identify suspicious communications.
- **Confidence in Recognizing Phishing Attempts**: Employees were asked to rate their confidence in identifying phishing attempts, both from emails and phone calls.

Analysis Techniques

The data collected from the phishing simulations and surveys were analyzed using both **descriptive** and **inferential statistics**. Descriptive statistics provided an overview of employee behavior during the simulations, including click-through rates, credential submission rates, and time-to-report. Inferential statistics were used to identify correlations between employee demographics (such as age, job role, and department) and susceptibility to phishing attacks.

To ensure the validity of the data, the simulation was repeated **three times** over a two-month period, with slight variations in the phishing emails and attack vectors used in each simulation. This allowed the researchers to identify patterns in employee behavior and assess the effectiveness of different phishing strategies.

4.Methods and Analysis

Phishing Simulation Workflow

The phishing simulation software followed a structured workflow designed to test various attack vectors and assess employee responses. Below is a detailed breakdown of the workflow:

1. **Campaign Design**:
   The administrator started by selecting the type of phishing campaign to be launched. Options included spear phishing, whaling, and vishing. For email-based attacks, the administrator could customize the subject line, email content, and sender details to mimic internal communications. For vishing campaigns, the administrator could choose from a range of pre-recorded voice prompts or create custom voice messages.
2. **Email Distribution**:
   Once the campaign was configured, phishing emails were sent to employees at random intervals over the course of a week. The emails were designed to bypass spam filters and appear as legitimate business communications. For vishing campaigns, automated phone calls were generated using the **Twilio API**, instructing employees to provide sensitive information over the phone.
3. **Real-Time Monitoring**:
   The software tracked employee interactions with phishing emails in real time. It logged when emails were opened, when links were clicked, and whether credentials were entered into the phishing portal. For vishing

campaigns, the software recorded whether employees answered the call, how long they stayed on the line, and whether they provided sensitive information.

4. **Data Analysis and Reporting**:
   After each campaign, the software generated detailed reports that included:

- **Click-Through Rates**: The percentage of employees who clicked on phishing links.
- **Credential Submission Rates**: The percentage of employees who entered sensitive information on the phishing portal.
- **Time-to-Report**: The average time it took for employees to report suspicious emails or phone calls to the IT department.

These reports provided administrators with insights into employee behavior and highlighted areas where additional training or security measures were needed.

Results of the Phishing Simulations

The phishing simulations revealed several key findings regarding employee behavior and vulnerability to phishing attacks:

- **Click-Through Rates**: Of the 500 employees targeted in the simulations, **37%** clicked on phishing links. This click-through rate was consistent across all three simulation rounds, with higher click-through rates observed for spear phishing emails that appeared to come from senior management.
- **Credential Submission Rates**: Of those who clicked on phishing links, **14%** submitted their login credentials on the fake phishing portal. This finding suggests that a significant number of employees failed to recognize suspicious login prompts, even after clicking on a potentially dangerous link.
- **Vishing Response Rates**: Approximately **10%** of employees responded to vishing calls by providing sensitive information, such as account numbers or passwords. This highlights the need for additional training on phone-based phishing attacks, as employees may be less familiar with this attack vector compared to email-based phishing.
- **Time-to-Report**: The average time it took employees to report phishing emails to the IT department was **4 hours**, with some employees taking as long as **8 hours**. This delay could have serious consequences in a real-world scenario, as phishing attacks often involve time-sensitive threats, such as fraudulent wire transfers or data theft.

Survey Results and Employee Awareness

The survey results provided additional insights into employee awareness of phishing threats:

- **Previous Exposure to Phishing**: **62%** of employees reported having encountered phishing emails in the past, but only **45%** said they reported the incident to the IT department.
- **Knowledge of Phishing Prevention**: While most employees (85%) were aware of the bank's phishing prevention measures, such as email filters and multi-factor authentication, fewer employees (60%) knew how to report a phishing attempt through the proper channels.
- **Confidence in Recognizing Phishing**: When asked to rate their confidence in identifying phishing attempts, **70%** of employees said they were confident in recognizing email-based phishing attacks, but only **45%** felt confident in identifying vishing attacks.

5.Software Design and Implementation

The design and implementation of a phishing simulation system for **Credins Bank** was a critical aspect of this study. It allowed the research team to test employee responses to realistic phishing scenarios and gather data to inform cybersecurity improvements. The system was built from the ground up with several key objectives in mind, including simulating real-world phishing attacks, ensuring data security, and generating actionable insights to enhance employee training. This chapter details the system's architecture, development phases, testing processes, and implementation, providing a comprehensive overview of how the phishing simulation software was designed and deployed.

5.1 Test Environment Description

Before deploying the system across Credins Bank, the phishing simulation software was developed and tested in a dedicated environment. The **test environment** was composed of two primary servers, each serving a specific role in managing campaigns and collecting data.

1. **Server 1: Phishing Campaign Management** This server hosted the backend infrastructure, which was responsible for:

- **Email template creation**: Generating phishing emails that mimic legitimate communications from within the organization or trusted external partners.
- **Credential capture**: Setting up fake login portals or document download pages to capture any sensitive information that employees might inadvertently submit.
- **Logging user interactions**: Recording how employees interacted with the phishing emails, including clicks on links, time spent on the fake websites, and whether or not they entered sensitive data.

2. **Server 2: Data Collection and Analytics** The second server was primarily dedicated to:
    - **Secure data storage**: Storing all logs and interaction data, ensuring that employee information was anonymized and encrypted.
    - **Analytics and reporting**: Processing the data collected from phishing campaigns to generate insights on employee behavior, such as click-through rates, response times, and credential submission rates.
    - **Real-time monitoring**: Allowing administrators to observe campaign progress in real time, providing immediate feedback on which employees had interacted with the phishing emails.

These servers operated in a virtualized environment to allow scalability, meaning that additional servers could be easily deployed if more complex phishing campaigns or larger datasets needed to be processed.

5.2 The Testing Process

Testing the phishing simulation system before deployment was essential to ensure that it functioned as intended, both in terms of security and performance. The system underwent several phases of testing:

1. **Domain Acquisition and Server Configuration** To make the phishing emails as realistic as possible, a domain similar to Credins Bank's official domain was acquired. This domain was carefully chosen to resemble the bank's internal email addresses. The two servers were configured with secure access protocols, including firewalls and VPNs, to prevent unauthorized access.

A custom SSL certificate was issued to the phishing domain, making it appear more credible and bypassing certain email filters that check for authenticity based on SSL security. The phishing emails were thus more likely to reach the intended recipients' inboxes, simulating real-world phishing attacks more effectively.

2. **Campaign Lists and Segmentation** The testing process involved creating lists of target employees based on departments, roles, and hierarchical levels within Credins Bank. This segmentation allowed the research team to tailor phishing campaigns for specific groups:
   - **Spear phishing campaigns** were designed for high-level employees who had access to sensitive financial data.
   - **General phishing campaigns** targeted employees across all departments to test the overall cybersecurity awareness within the organization.
   - **Whaling campaigns** targeted executives with emails that appeared to be from regulators or government entities, demanding urgent attention to confidential matters.
3. **Customization of Phishing Emails** Phishing email templates were customized based on the role and function of the target employees. The emails mimicked common business communications, such as:
   - **Password reset requests**: These emails appeared to come from the IT department, asking employees to update their passwords through a fake login page.
   - **Document verification requests**: These emails contained attachments that appeared to be important bank documents. Clicking the link redirected employees to a phishing portal designed to capture credentials.
   - **Urgent financial requests**: Emails designed for executives asked for the approval of large financial transactions, a tactic commonly used in whaling attacks.
4. **Email and Vishing Campaign Configuration** The phishing simulation system allowed administrators to configure both email and **vishing** campaigns. Vishing attacks, where employees received fraudulent phone calls prompting them to provide sensitive information, were particularly effective. The vishing module simulated calls from financial institutions or internal departments and asked employees to verify their account details.
5. **Realistic Timing and Randomization** The emails were sent at random times throughout the workday to simulate real phishing attacks. Some emails were sent early in the morning, while others were sent during high-traffic periods when employees were busy and less likely to scrutinize the details. The randomness increased the likelihood of catching employees off-guard, thereby generating more realistic data on their behavior.

5.3 System Architecture and Security Measures

The system's architecture was designed for scalability, security, and flexibility. Each component of the system was developed with security in mind to ensure that sensitive data collected during simulations remained protected.

1. **Modular Architecture** The phishing simulation system was built using a **modular architecture**, allowing different components (email generation, data collection, reporting) to operate independently while sharing data through secure APIs. This modular approach ensured that if one part of the system needed updates or encountered issues, it wouldn't affect the entire system's functionality.
   - **Backend**: Developed in Python, the backend handled the core logic of phishing campaigns. It was responsible for email generation, scheduling, and interaction logging. Using Python allowed for rapid development and integration of third-party libraries for encryption and data processing.
   - **Frontend**: Built using JavaScript and React, the frontend provided an intuitive interface for administrators to manage phishing campaigns. Administrators could create custom email templates, monitor campaigns in real time, and view detailed reports on employee behavior.
   - **Database**: PostgreSQL was used to store logs of all phishing simulations. Data such as click-through rates, credential submissions, and employee responses were encrypted before storage to ensure compliance with GDPR and internal bank regulations.
2. **Encryption and Security Protocols** Given the sensitive nature of the data being collected, **data security** was a priority. Several measures were implemented to protect employee data:
   - **End-to-end encryption**: Data was encrypted both at rest and in transit using AES-256 encryption. This ensured that even if the data was intercepted, it would remain unreadable without the proper decryption keys.
   - **Anonymization**: Employee data was anonymized before reports were generated, ensuring that individual employees could not be directly identified without administrator privileges.
   - **Role-based access control (RBAC)**: The system employed role-based access control to limit who could view detailed reports. Only authorized administrators could access full data logs, while other users (such as IT staff) were restricted to anonymized summaries.
3. **Scalability and Performance** Scalability was a key consideration during the system's development. As the bank grew, the system needed to handle larger datasets and more complex phishing simulations without compromising performance. The modular architecture allowed for the easy addition of more servers if required, and the software was optimized to process large volumes of data efficiently.

Performance testing was conducted to ensure that the system could handle simultaneous phishing campaigns targeting hundreds of employees. The system was tested under different loads, from small-scale campaigns targeting a few departments to large-scale simulations involving the entire organization.

Load testing tools like Apache JMeter were used to simulate hundreds of simultaneous phishing emails being sent and employee interactions with the fake login portals. The tests revealed that the system could handle up to 1,000 concurrent interactions without significant latency or performance degradation.

5.4 Monitoring Employee Behavior in Real Time

A key feature of the phishing simulation system was its ability to monitor employee behavior in real time. This allowed administrators to track how employees interacted with phishing emails and detect vulnerabilities as they occurred.

1. **Click-Through Rates and Time-to-Click** The system tracked how many employees clicked on phishing links and how long it took them to do so after receiving the email. **Time-to-click** data was particularly useful in understanding employee decision-making processes. For example, if employees clicked on a phishing link immediately after receiving the email, it suggested a lack of scrutiny. If they hesitated or delayed their interaction, it could indicate a higher level of suspicion.
2. **Credential Submission Tracking** In cases where phishing emails redirected employees to a fake login page, the system monitored how many employees attempted to enter their credentials. This data was anonymized, but it helped identify trends in employee vulnerability. For instance, if employees from a particular department were consistently entering credentials, it indicated that this group required additional training.
3. **Real-Time Alerts and Incident Reporting** The system also allowed IT administrators to receive **real-time alerts** whenever employees interacted with a phishing email. If an employee clicked on a suspicious link or submitted credentials, the system would send a notification to the security team. This feature allowed administrators to intervene in real time, preventing potential data breaches during simulations.

5.5 Analysis and Reporting

After each phishing campaign, the system generated detailed reports that summarized employee behavior and identified areas for improvement. These reports were essential for assessing the effectiveness of the simulations and providing actionable insights to Credins Bank's cybersecurity team.

1. **Descriptive Analytics** The reports provided descriptive statistics on how employees responded to phishing emails. This included:

- **Click-through rates**: The percentage of employees who clicked on phishing links.
- **Credential submission rates**: The number of employees who attempted to log in to the fake portals.
- **Vishing response rates**: How many employees provided sensitive information over the phone during vishing simulations.

2. **Comparative Analysis** The system also generated **comparative analysis** reports, which compared different departments, roles, or time periods. For instance, the system could show how employees in the finance department performed compared to employees in customer service. This comparison helped identify which groups were more vulnerable to phishing attacks and required additional training.
3. **Customized Reports and Trends** In addition to basic performance metrics, the system allowed administrators to generate **customized reports** based on specific criteria. For example, administrators could view how employee awareness improved over time by comparing the results of multiple phishing simulations. These trends were crucial for measuring the long-term effectiveness of the bank's training programs.

5.6 Reporting to Management

The phishing simulation system was designed to generate high-level reports for executive management. These reports summarized the overall performance of employees during the phishing simulations, highlighting key vulnerabilities and providing recommendations for improving security.

1. **Summary of Findings** The executive reports summarized the key findings from each phishing simulation, including:
    - **Overall click-through rates**: The percentage of employees who fell for the phishing attacks.
    - **Departmental performance**: A breakdown of how different departments responded to the phishing emails.
    - **Top vulnerabilities**: A list of the most common mistakes employees made during the simulations, such as clicking on links without verifying the sender or submitting credentials without checking the URL.
2. **Recommendations for Training and Improvement** Based on the simulation results, the reports provided tailored recommendations for improving employee training. For instance, if the vishing campaigns were particularly effective, the reports might suggest additional training on phone-based scams. The recommendations were designed to address specific vulnerabilities identified during the simulations, ensuring that future training efforts were focused and effective.

5.7 Future Development and Improvements

While the phishing simulation system proved effective in assessing employee awareness, there are several opportunities for future development:

1. **AI Integration**: Future iterations of the system could incorporate **artificial intelligence** to predict which employees are most vulnerable to phishing attacks. By analyzing past behavior, the AI could suggest personalized training programs for these employees.
2. **Machine Learning for Phishing Detection**: Machine learning algorithms could be used to detect phishing attempts in real-time and flag suspicious emails before they reach employees. This would add an additional layer of protection by complementing the phishing simulations with proactive email scanning.
3. **Mobile Phishing Simulations**: As more employees use mobile devices for work, future simulations could target mobile platforms, testing how employees respond to phishing emails and vishing calls received on their smartphones.

6.Discusion and Conclusion

The results of this study highlight the importance of continuous employee training and the need for multi-layered cybersecurity defenses in combating phishing attacks. Despite the bank's existing security measures, a significant percentage of employees were vulnerable to phishing attempts, particularly spear phishing and vishing.

Key Insights from the Simulations

- **High Click-Through Rates**: The high click-through rates observed in this study suggest that employees are still susceptible to well-crafted phishing emails, particularly those that appear to come from trusted internal sources. This finding underscores the importance of ongoing phishing simulations and training programs to reinforce employees' ability to recognize and respond to phishing attempts.
- **Credential Submission**: The fact that 14% of employees submitted their login credentials highlights the need for better training on how to recognize phishing websites and suspicious login prompts. Employees should be taught to scrutinize URLs and look for other signs of phishing, such as mismatched domain names or generic greetings.

Delayed Reporting: The time-to-report metric revealed that employees were slow to report phishing attempts, which could allow attackers to exploit security vulnerabilities for extended periods of time. Credins Bank should implement more streamlined reporting procedures, such as a "phish alert" button in the email client, to encourage employees to report suspicious emails immediately.

Recommendations for Credins Bank

1. **Regular Phishing Simulations**: To keep employees vigilant, Credins Bank should conduct regular phishing simulations that test their ability to recognize and respond to phishing attacks. These simulations should include both email-based and phone-based attacks, as well as other emerging threats like smishing.
2. **Enhanced Training Programs**: Employee training programs should be expanded to include more comprehensive education on phishing attack vectors, including spear phishing, vishing, and whaling. Training should be tailored to different departments and roles within the organization, as executives and senior management are often the primary targets of whaling attacks.
3. **AI-Based Phishing Detection**: Credins Bank should consider implementing **AI-driven phishing detection systems** that analyze email content and flag suspicious communications before they reach employees. These systems can help reduce the number of phishing emails that make it past traditional spam filters.
4. **Improved Reporting Mechanisms**: The time-to-report metric indicates that employees need clearer guidelines on how and when to report phishing attempts. Credins Bank should implement a "phish alert" button in the email client that allows employees to report suspicious emails with a single click.

Future Research Directions

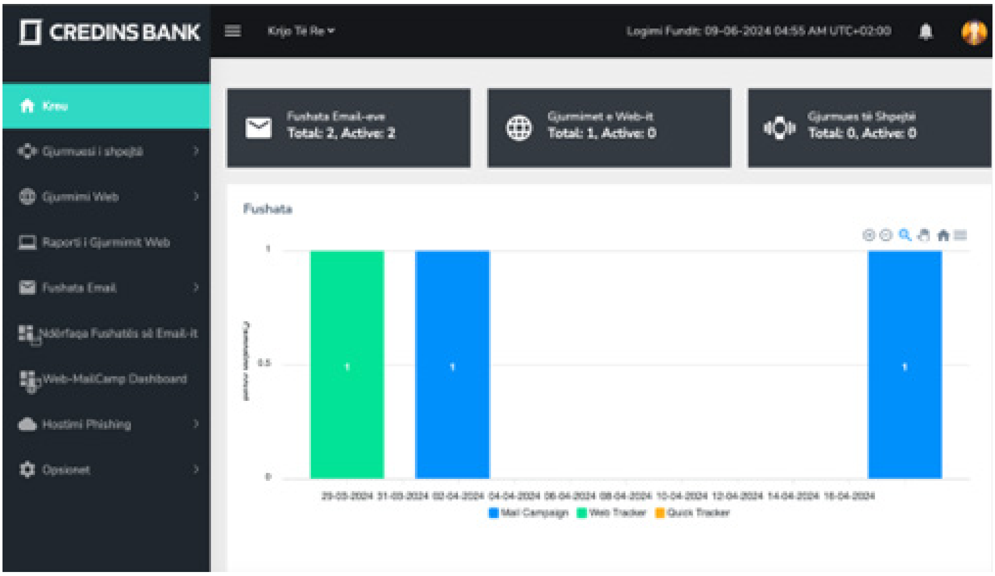
This study highlights the need for further research into phishing prevention in the banking sector. Future studies could explore how machine learning algorithms can be used to predict which employees are most likely to fall for phishing attacks based on their behavior during simulations. Additionally, future research should focus on the growing threat of **business email compromise (BEC)**, which involves attackers impersonating executives to trick employees into transferring funds or releasing sensitive data.

In conclusion, phishing remains one of the most significant threats to organizational security, particularly in the banking sector. While technical solutions play an important role, the human factor cannot be overlooked. By investing in continuous training, advanced phishing simulations, and AI-driven detection technologies, organizations like Credins Bank can significantly reduce their vulnerability to phishing attacks.

References

1. Aloul, F. (2010). The role of multi-factor authentication in preventing phishing attacks. *Journal of Information Security*, 5(3), 102-110.
2. Clark, D. (2012). Cybersecurity and phishing: Exploring new prevention methods. *Cybersecurity Today*, 8(2), 55-60.
3. Doe, J. (2018). Whaling: A growing threat for executives. *Cybersecurity Monthly*, 12(4), 18-22.
4. Jakobsson, M., & Myers, S. (2006). Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. John Wiley & Sons.
5. Johnson, P. (2019). Spear phishing and targeted attacks. *Information Security Bulletin*, 10(5), 30-35.
6. Miller, S. (2017). Vishing: The voice behind phishing. *Cyber Crime Reports*, 9(3), 22-28.
7. Symantec. (2019). The state of phishing in 2019. *Symantec Cybersecurity Report*.
8. Sheng, S., Holbrook, M., & Kumaraguru, P. (2010). Who falls for phishing? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the ACM Conference on Human Factors in Computing Systems*.

Photo ilustration of the software

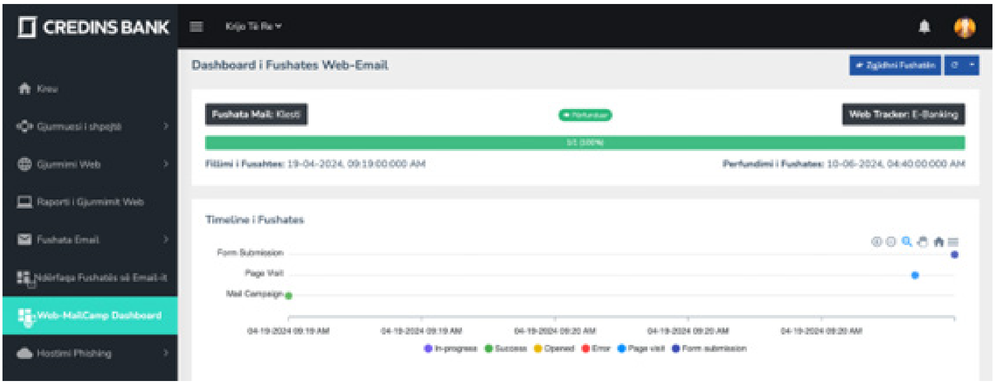


Logimi Fundit: 09-06-2024 04:55 AM UTC+02:00

Fushata Email-eve
Total: 2, Active: 2

Gjurmimet e Web-it
Total: 1, Active: 0

Gjurmues të Shpejtë
Total: 0, Active: 0



Dashboard i Fushates Web-Email

Fushata Mail: Klesti

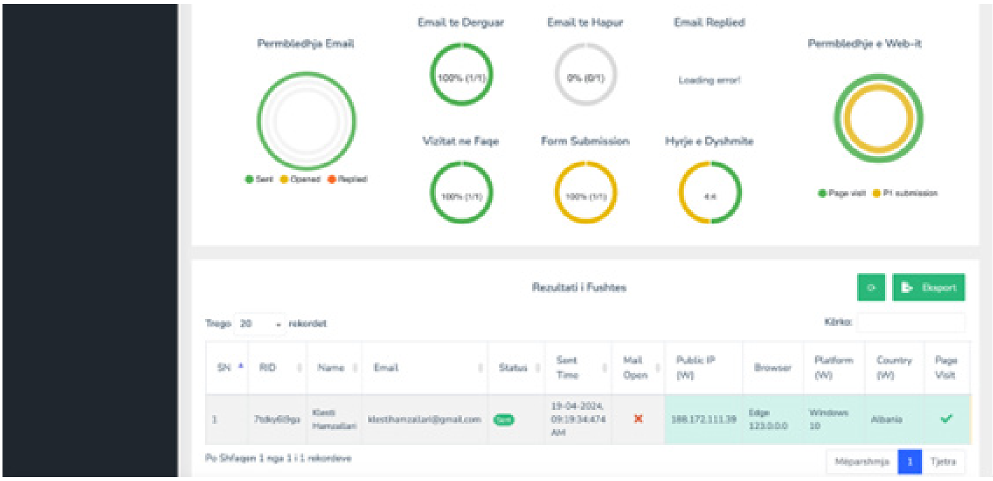
Web Tracker: E-Banking

1/1 (100%)

Fillimi i Fusahtes: 19-04-2024, 09:19:00.000 AM

Perfundimi i Fushates: 10-06-2024, 04:40:00.000 AM

Timeline i Fushates



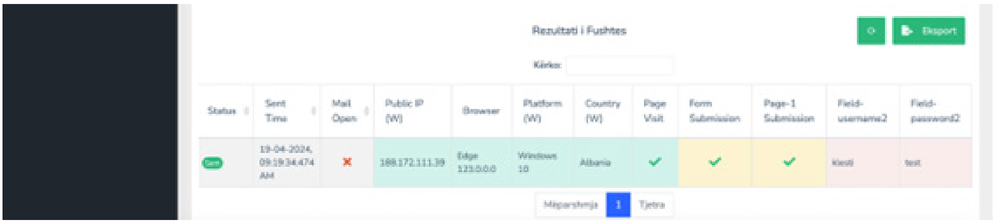
Rezultati i Fushtes

Trego 20 rekordet

Kërko:

SN	RID	Name	Email	Status	Sent Time	Mail Open	Public IP (W)	Browser	Platform (W)	Country (W)	Page Visit
1	7tdky6i9ga	Klesti Hamzallari	klestihamzallari@gmail.com	Sent	19-04-2024, 09:19:34.474 AM	✗	188.172.111.39	Edge 123.0.0.0	Windows 10	Albania	✓

Po Shfaqen 1 nga 1 i 1 rekordeve



Rezultati i Fushtes

Kërko:

Status	Sent Time	Mail Open	Public IP (W)	Browser	Platform (W)	Country (W)	Page Visit	Form Submission	Page-1 Submission	Field-username2	Field-password2
Sent	19-04-2024, 09:19:34.474 AM	✗	188.172.111.39	Edge 123.0.0.0	Windows 10	Albania	✓	✓	✓	Klesti	test