Cyber-Resilient Network Infrastructure to Protect Customer Data from Phishing Attacks for a Retail Chain

Anthony Mutunga

138464

CNS

Supervisor Name

Mr. James Gikera

Submitted in Partial Fulfillment of the Requirements of the Bachelor of Science in Computer Networks and Cybersecurity at the Strathmore University

School of Computing and Engineering Science

Strathmore University

Nairobi, Kenya

May 2024

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the research proposal contains no material previously published or written by another person except where due reference is made in the research proposal itself.

Student Name: Anthony Mutunga

Admission Number: 138464

Student Signature: _____ Date:_____

The Proposal of **Anthony Mutunga** has been reviewed and approved by **Mr. James Gikera**

Supervisor Signature: _____ Date:_____

Acknowledgement

I extend my heartfelt appreciation to everyone who contributed to the completion of my project. I am deeply grateful to my project supervisor, Mr. James Gikera for his invaluable guidance, expertise, and unwavering support, which was instrumental at every stage of the project.

Gratitude also extends to Strathmore University for providing the necessary resources and opportunities that facilitated the realization of this project and contributed to my academic and professional development.

To everyone involved, your contributions, no matter how big or small, were indispensable. I am sincerely grateful for the opportunity to undertake this project and contribute to the advancement of knowledge in our field.

Abstract

Retail chains are increasingly being targeted by cyber threats in the quickly changing digital landscape, with phishing attacks posing a serious risk to the security of consumer data. The primary goal of this project is to develop and put into place a cyber-resilient network infrastructure with the express purpose of lessening the effects of phishing attacks via emails. The suggested approach aims to detect and eliminate phishing threats in the received emails before they compromise confidential client data. Two factor authentication, firewall, alerting notification, incident logging, and a quarantine procedure for questionable emails are all integrated into the system. This multi-layered defensive approach guarantees complete protection against phishing, protects consumer information, and upholds the integrity and confidence of the retail chain's business dealings. The project intends to serve as a model for other retail entities to improve their data protection frameworks and emphasizes the significance of proactive cybersecurity measures in defending against phishing tactics that are becoming more sophisticated.

Table of Contents

List of Figures

List of Abbreviations

MFA- Multi-Factor Authentication

IPS- Intrusion Prevention System

URL- Universal Resource Locator

GDPR- General Data Protection Regulation

CCPA- California Consumer Privacy Act

SDN- Software-Defined Networking

NFV- Network Function Virtualization

Payment Card Industry Security Standards Council (PCI SSC)

Health Insurance Portability and Accountability Act (HIPAA)

Gramm-Leach-Bliley Act (GLBA)

User Centered Design (USD)

Chapter 1: Introduction

1.1 Background Information

Retail chains, handling vast amounts of sensitive customer information such as payment details, personal identification, and purchase history, are prime targets for cybercriminals. Phishing attacks exploit human vulnerabilities through example deceptive emails, to trick individuals into revealing confidential information or installing malware. The focus will be attacks on emails.

Phishing remains one of the most common and damaging forms of cyber threats. It can lead to significant data breaches, financial losses, and reputational damage for retail businesses. The increasing sophistication of phishing techniques, including spear phishing and smishing, necessitates a robust and resilient cybersecurity infrastructure.

1.2 Problem Statement

Cybercriminals are targeting retail chains more and more in the modern digital era in an effort to compromise sensitive customer data and take advantage of weaknesses. Phishing, especially via email, is one of these attackers' most common and destructive techniques. Despite improvements in cybersecurity, sophisticated phishing attacks that evade conventional security measures continue to cause serious data breaches in a large number of retail organizations. The cybersecurity frameworks in place today frequently fall short of offering complete defense against the constantly changing strategies used by phishing attacks. Thus, it is imperative to develop and deploy a strong, cyber-resilient network architecture that is especially suited to identify, lessen, and stop phishing attempts on emails in the retail industry.

1.3 Objectives

1.3.1 General Objective

The primary objective of this project is to design and implement a comprehensive cyber resilient network infrastructure specifically aimed at protecting customer data in retail chains from phishing attacks in emails.

1.3.2 Specific Objectives

i. Assess current security measures in place in the retail chain to deal with phishing attacks in emails.
ii. Check and evaluate whether the security measures can cope in the environment of the evolving phishing attacks.
iii. Developing an infrastructure resilient to the phishing attacks that appear on emails.
iv. Test and evaluate the updated email security measures in the retail chain system and draw a conclusion.

1.4 Research Questions

i. Are the current security measures able to deal with the phishing attacks in emails?
ii. What security measures have you noted and think want improvement?
iii. What are the various email security measures you are going to be developing?
iv. Are the updated security measures able to deal with the evolving phishing attacks in emails?

1.5 Justification

In the current digital landscape, retail chains are increasingly targeted by cybercriminals due to the vast amounts of sensitive customer data they manage, including payment details, personal information, and purchase histories. Phishing attacks, in particular, have emerged as a significant threat, exploiting human vulnerabilities to gain unauthorized access to this critical data. Despite the implementation of various cybersecurity measures, many retail organizations continue to suffer data breaches, resulting in substantial financial losses, legal repercussions, and severe damage to their reputation.

Addressing this gap, the proposed project aims to design and implement a comprehensive cyber resilient network infrastructure tailored to the unique challenges faced by retail chains. This holistic approach is essential for maintaining the integrity of retail operations and safeguarding sensitive information in an era of ever-evolving cyber threats.

1.6 Scope and Delimitations

This proposed study focuses on designing and Implementing cyber resilient network Infrastructure, emphasizing email security systems and multi-factor authentication (MFA), quarantine and alert systems to tell the administrator that there has been an attack. Phishing

attack prevention by targeting specifically the prevention and mitigation of phishing attacks within retail chains. Moreover, employee and customer education by developing and conducting continuous training programs for employees and educational campaigns for customers. Lastly, regulatory compliance by ensuring all implemented security measures adhere to relevant data protection regulations such as GDPR and CCPA.

This project does not cover:

i. Other forms of cyber threats outside of phishing, such as malware, ransomware, or DDoS attacks.
ii. Detailed financial implications or cost-benefit analysis of the implemented technologies.
iii. The physical security aspects of retail operations.
iv. Analysis of cybersecurity measures in non-retail sectors, to maintain a focused and relevant scope.
v. In-depth analysis of post-implementation user behavior changes beyond the scope of phishing attack responses.

Chapter 2: Literature Review

2.1 Introduction

In the digital age, where retail chains handle vast amounts of sensitive customer data, the protection of this information against cyber threats is paramount. Phishing attacks, in particular, have emerged as a significant challenge, exploiting human vulnerabilities to gain unauthorized access to confidential data. This introduction outlines the objectives of the literature review, which are to provide an overview of the current state of knowledge regarding cybersecurity in retail settings, examine the prevalence and impact of phishing attacks, and evaluate existing strategies and solutions for mitigating this threat. By synthesizing insights from a diverse range of scholarly works, this literature review seeks to inform the design and implementation of a cyber-resilient network infrastructure tailored to the unique needs of retail chains, with a specific emphasis on preventing and combating phishing attacks.

2.2 Phishing Attacks on Retail Chains

2.2.1 Challenges associated with Phishing Attacks

The challenges of phishing attacks are as follows:

i. Phishing attacks are continuously evolving and becoming more sophisticated, making them difficult to detect and prevent using traditional security measures.
ii. Despite technological advancements, human factors remain a significant vulnerability in cybersecurity, as employees and customers can still fall victim to phishing scams due to lack of awareness or training.
iii. Limited budget, expertise, and resources may hinder the implementation of comprehensive cybersecurity solutions, particularly for smaller retail chains.
iv. The cyber threat landscape is constantly evolving, with new phishing techniques and attack vectors emerging regularly. The project must remain adaptable and responsive to these emerging threats to ensure long-term effectiveness.

2.3 Related Works

An example of related work is by Smith et al. (2020), who investigates the impact of cyber threats on retail chains and underscores the importance of implementing robust cybersecurity measures to protect customer data. The research highlights the prevalence of malware, phishing scams, and ransomware attacks targeting retail organizations and emphasizes the need for proactive risk management strategies to mitigate these threats effectively.

Another relevant work by Jones and Brown (2019) explores the regulatory landscape governing data protection and privacy in the retail sector, focusing on compliance requirements such as GDPR and CCPA. The study examines the implications of these regulations on retail chains' data handling practices and underscores the significance of aligning cybersecurity initiatives with regulatory mandates to ensure legal compliance and mitigate regulatory risks.

Furthermore, a case study by Cheng et al. (2021) dives into the implementation of a cyber-resilient network infrastructure within a leading retail chain. The research describes the network design principles, technological solutions, and operational practices employed to enhance cybersecurity resilience and protect customer data effectively. By examining real-world implementations and practical challenges encountered, the study offers valuable insights and best practices for retail organizations seeking to fortify their cybersecurity posture.

Additionally, Wang and Wu (2018) provide insights into the role of emerging technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV) in enhancing network resilience and agility. The research explores the benefits of adopting these technologies in retail environments, such as improved network visibility, flexibility, and automation, to bolster cybersecurity defenses and mitigate cyber threats effectively.

2.3.1 Public Policies and relationship to Customer Data

This section explores the intersection of public policies and customer data protection in retail stores, examining key regulations, compliance requirements, and their implications for retail organizations.

General Data Protection Regulation (GDPR): The GDPR, implemented by the European Union (EU), is one of the most comprehensive data protection regulations globally. It imposes

stringent requirements on organizations handling personal data of EU residents, including retail stores. Under the GDPR, retail stores are obligated to obtain explicit consent from customers for data processing activities, adhere to principles of data minimization and purpose limitation, and implement robust security measures to protect customer data from unauthorized access or disclosure. Non-compliance with the GDPR can result in severe penalties, including fines of up to 4% of global annual turnover.

California Consumer Privacy Act (CCPA): The CCPA, enacted by the state of California, aims to enhance consumer privacy rights and control over their personal information. Similar to the GDPR, the CCPA grants consumers the right to know what personal information is collected by retail stores, the right to opt-out of the sale of their personal data, and the right to request deletion of their data. Retail stores subject to the CCPA must provide clear and conspicuous notices regarding data collection practices, establish mechanisms for consumers to exercise their rights, and implement reasonable security measures to protect customer data.

Payment Card Industry Data Security Standard (PCI DSS): While not a public policy per se, the PCI DSS is a set of security standards developed by the Payment Card Industry Security Standards Council (PCI SSC) to protect payment card data. Retail stores that accept credit and debit card payments are required to comply with PCI DSS requirements, which encompass measures such as securing cardholder data, implementing access controls, conducting regular security assessments, and maintaining information security policies and procedures.

Sector-Specific Regulations: In addition to general data protection regulations, retail stores may also be subject to sector-specific regulations and standards governing data protection and security. For example, healthcare retail stores must comply with the Health Insurance Portability and Accountability Act (HIPAA), while financial retail stores must adhere to regulations such as the Gramm-Leach-Bliley Act (GLBA).

Implications for Retail Stores: Compliance with public policies such as the GDPR, CCPA, and PCI DSS entails significant implications for retail stores. It requires investment in robust data protection measures, including encryption, access controls, and data breach response plans. Moreover, non-compliance can result in reputational damage, legal liabilities, and financial penalties, underscoring the importance of prioritizing customer data protection within retail stores.

2.4 Gaps in Related Works

i. Limited Focus on Small Retail Chains:

Many related works primarily focus on cybersecurity challenges faced by large retail chains, potentially overlooking the unique constraints and requirements of smaller retailers.

ii. Insufficient Attention to Regulatory Compliance:

While some studies address regulatory compliance in data protection, there is a lack of in-depth analysis on the practical implications and challenges of implementing compliance measures within retail environments.

iii. Scarcity of Solutions Tailored to Phishing Attacks:

While phishing attacks are acknowledged as a significant threat, there is a gap in the literature regarding specific strategies and solutions tailored to effectively prevent and mitigate phishing attacks within retail chains.

iv. Limited Exploration of Emerging Technologies:

While some studies discuss the role of emerging technologies in enhancing network security, there is a gap in understanding how these technologies can be practically implemented and integrated into existing retail infrastructure to combat phishing attacks.

v. Inadequate Evaluation of Employee Training Programs:

While the effectiveness of employee training programs in mitigating phishing attacks is recognized, there is a gap in the literature regarding comprehensive evaluations of these programs' long-term impact and scalability within retail environments.

2.5 Conceptual Frameworks

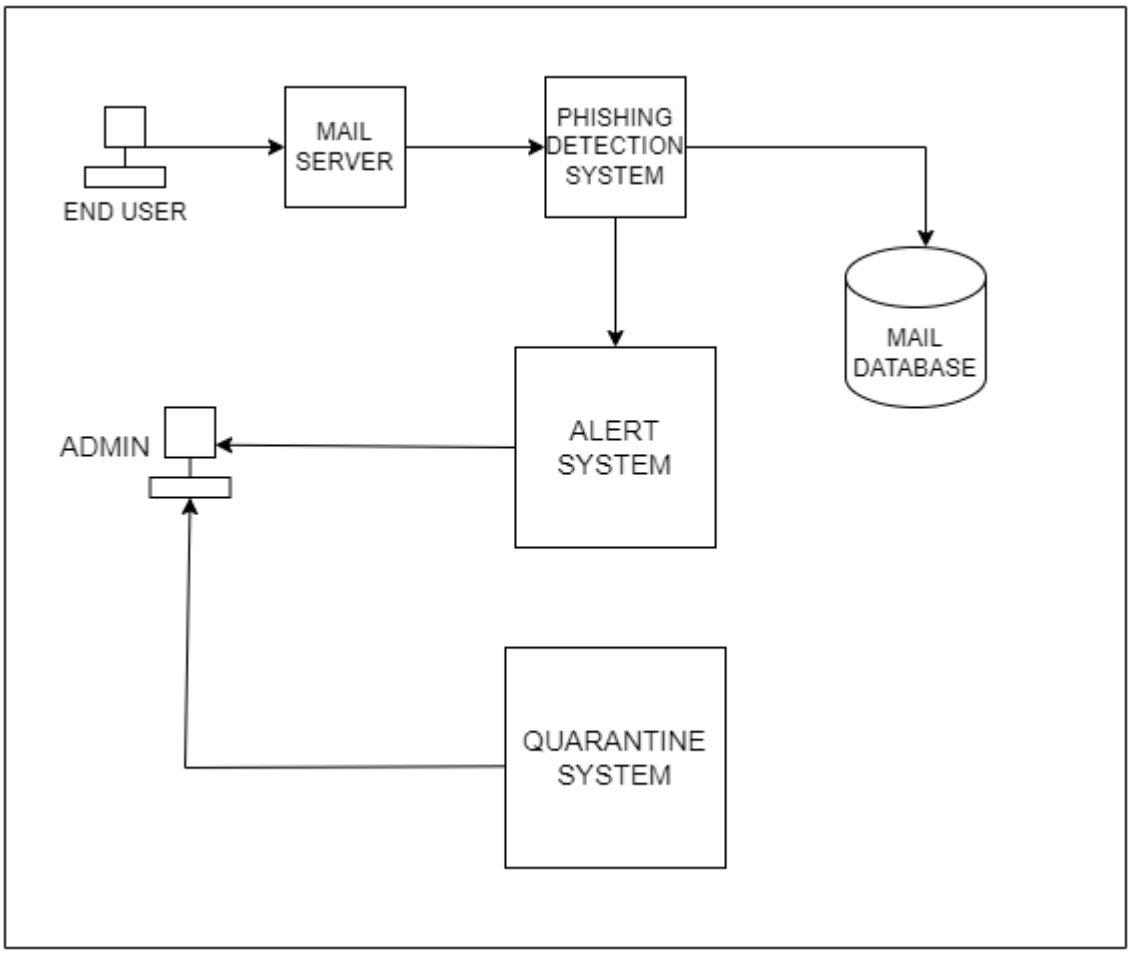


Figure 2.1 Phishing attack and Mitigation

This image shows an end user seemingly sending and receiving an email through the system network of the administration. The email passes through some procedures that detect phishing threat in emails, so that when detected it can be isolated. Before being isolated and quarantined, the malicious email is logged and saved, the administrator is alerted about the supposed threat detected on the email and the administrator is able to work on it in the quarantined area away from other end users in the system.

Chapter 3: Methodology

3.1 Introduction

This chapter is structured to provide a clear overview of the approach and procedures utilized in designing and implementing a cyber-resilient network infrastructure to protect customer data in retail chains, focusing on mitigating phishing attacks. Highlights the importance of continuous evaluation and adaptation to ensure the effectiveness and relevance of the implemented cybersecurity measures.

3.2 Methodology

The methodology I am using is agile development, specifically the scrum framework which is ideal for iterative processes which foster constant improvement and adaptation in the system. Some reasons of applying this methodology is:

i. Phishing threats are constantly evolving. Agile allows for rapid adjustments and updates to the project plan as new threats are identified or as security requirements change.
ii. Initial solutions can be tested and improved continuously, leading to more robust and resilient outcomes.
iii. Agile prioritizes user stories and customer feedback. By incorporating feedback from retail customers and employees, the project can develop security measures that are not only effective but also user-friendly, reducing the likelihood of security measures being bypassed or ignored.

3.2.1 Planning

This project aims to improve email security to protect customer data in a retail chain setting. Phishing attacks are a constant threat, and I will be designing and implementing a resilient network to deal with the issue. Some implementations to be made is two-factor authentication, multi factor authentication, firewall, email filtering, alert notifications, incident logging and a quarantine procedure.

3.2.2 Requirements Gathering

The needs of the customer come first in ensuring good relationships as the overall data will be protected and away from any compromise. Review current security measures in place in the retail store and consult on how to improve the system from the phishing attacks.

3.2.3 Design

The security measures to be designed and implemented will be applied by adding a two factor authentication for example, a phone number or another recovery email to bolster email access security from unauthorized access. A quarantine system will also be implemented for emails that have come from an untrustworthy source. A firewall will block the port numbers and ip addresses that are not corresponding to the ones in use in the system.

3.2.4 Development

Writing code to be used for quarantine procedures, various ways of logging in for example using both work identification number and your password, blocking the ip addresses and port numbers to restrict access to the network and taking note and saving the various threats that you have come across.

3.2.5 Testing

Testing will evaluate and verify the developed features work as they are intended. The quarantine procedure after an email has already been detected by a code that is supposed to detect specific patterns or signatures suggestive of malicious content in emails. I will be implementing black-box testing as I will be interested in how the system will handle the attack rather than how it makes it happen.

3.2.6 Deployment

Once the testing is done and the system is optimal, you can implement it in a live environment making it ready for use. Configure the network devices necessary for example routers and end users to show the firewall implementation to block ip addresses and port numbers not within the network space. Deploying the generated code to show quarantine procedure of the email and how it is stored and reviewed in subsequent attacks. Monitor to ensure they work accordingly.

3.2.7 Review and feedback

Getting feedback from the staff and employees from the retail store is so important to identifying common areas of concern and where to improve. Plan according to the emerging issued that have occurred during the survey process and improve accordingly.

3.2.8. Iteration

The cycle done multiple times to refine the solutions brought about by the project. Continued testing will help improve the system with emerging email phishing attack techniques. These cycle called sprints emphasizes iterative progress through a short, time-boxed process.

3.3 Deliverables

Model

A code is implemented to detect presence of any malicious email and sends them to the quarantine procedure. Presence of routers and end users in a network provide a basis of ip address and port number blocking that are not accessible within the network to mitigate phishing attacks.

User Interface (UI):

Here, the inclusion sending and receiving messages or emails, connecting to interfaces and other end users in a network, presence of alert and incident logging are examples of user interactive elements in my project, and therefore useful in conducting the checks necessary in the system. User friendly elements help interact easy with the system, helping to easily spot and report any incidences.

Proposal

The proposal here outlines what the project will be doing, giving details to the methodology and various system implementations that are going to be in the project. From ip addresses to security protocols to port numbers. This will form a basis of the project, taking us through the development and implementations done in the project.

Distributed System for Application Access

Here the various components are for example, email servers, intrusion Prevention system, quarantine management and an alerting component.

Email servers are responsible for receiving, storing, and sending emails. An IPS for monitors incoming emails for suspicious patterns or behaviors that could indicate an attack (flags malicious emails). A quarantine management for storing suspicious emails flagged by the

phishing detection service or IPS. Alerting when suspicious emails are quarantined or when the IPS detects potential threats.

3.4 Tools and Techniques

i. Firewall Implementation

Firewalls control network traffic to prevent unauthorized access to a network. They can be configured to block incoming and outgoing traffic based on criteria such as source IP address, destination IP address, and port number. By blocking traffic from known phishing domains or IP addresses, firewalls can help prevent them from reaching end users. An IPS can be configured here in a firewall to act as phishing detection service.

ii. Email Security Solutions

Email remains one of the primary vectors for phishing attacks, making robust email security solutions essential for mitigating this threat. Solution to be implemented is having a two factor authentication method to avoid unauthorized access.

iii. Multi-Factor Authentication (MFA) Systems

MFA systems require users to provide multiple forms of authentication (e.g., passwords, biometrics, one-time passcodes) to access sensitive systems and data.

MFA enhances security by adding an extra layer of protection against unauthorized access, even if login credentials are compromised.

References

Brown, K., & Taylor, S. (2023). "User-Centered Design Principles for Cyber Resilient Networks in Retail Chains." *Proceedings of the ACM Conference on Human Factors in Computing Systems*, 245-258.

Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., ... & Thomas, D. (2001). *Manifesto for Agile Software Development*. Retrieved from http://agilemanifesto.org

Davis, P. (2022). "Data Protection Regulations and Compliance Requirements for Retail Chains." *International Journal of Retail Management*, 30(4), 567-580.

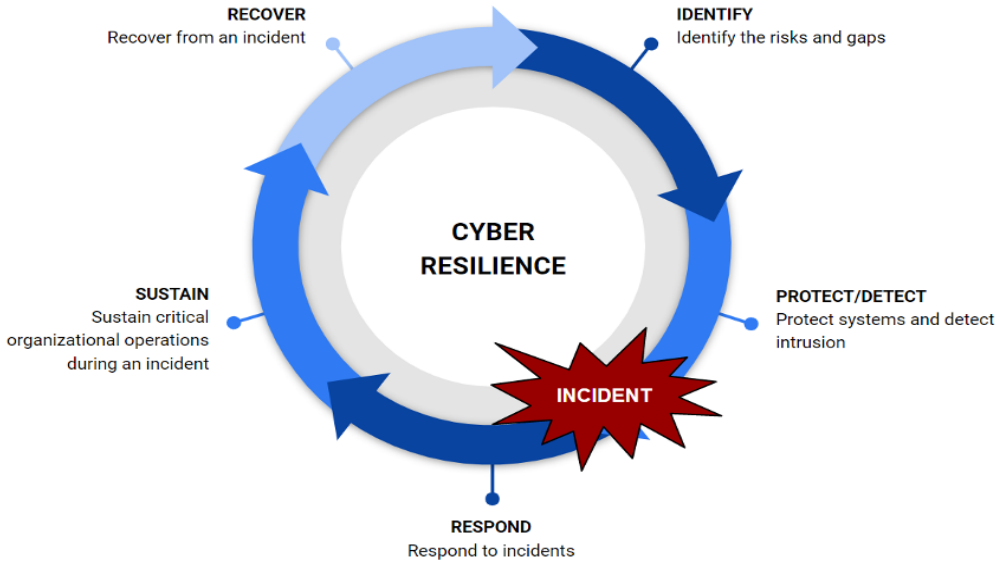
Garcia, A., & Martinez, D. (2023). "Implementing Multi-Factor Authentication in Retail Environments: Challenges and Best Practices." *Journal of Information Security*, 15(3), 112-125.

Schwaber, K., & Sutherland, J. (2017). *The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game*. Retrieved from https://scrumguides.org

Smith, J. (2023). "Cybersecurity Measures for Retail Chains: A Review of Current Practices." *Journal of Retail Security*, 10(2), 45-58.

Appendices:

Appendix



Appendix: Cyber-Resilient representation

Here is a representation of how the system works to narrow down on the phishing attacks. These attacks are usually evolving and finding better ways of exploiting the targeted data and system. Once an incident occurs, the responsible aid will respond and will block all access to the operational access during the attack. Recovery is the next step as the administrator will have analyzed and found or tested some of the solutions that will help the system get back to normal.

Appendix

Appendix: Phishing Attack

Image shows how attackers gain access through sending malicious emails to end users for example here, it is the checkout area. The sent malicious email is disguised as a friendly legit website, however, there is a phishing track going on, and the customer information may be at risk.