Interdisciplinary Approach towards Business Sustainability
Dr. S. Saileja & Dr. D. Mayuri
e-ISBN: 978-93-6252-974-9 | Year of Publication 2024
DOI: https://www.doi.org/10.58532/nbennuriach3

3

Impact of Phishing Attack on Business

Ms. Krishnaveni[*]

Abstract

Phishing attacks are a major threat to business, using tricks to manipulate employees into giving away sensitive information. This chapter explores how phishing attacks impact business operations, resulting in to financial losses, data breaches, and damage to reputation of business. Through case studies like Crelan Bank incident, it shows severe consequences of these attacks, including large amounts of financial loss and long-term harm to the company's reputation. This chapter explains different types of phishing attacks including email phishing, spear phishing, whaling, smashing, and gushing. Each type has its own methods but all aimed at stealing sensitive information. It describes the processes and techniques used in phishing attempts, such as fake emails, malicious links, attachments, and tricking people into giving. Sensitive information. This also emphasizes on the effects of phishing attacks on businesses such as financial loss to businesses, compromised data, and legal issues. The preventive measures include employee training, implementing

[*] *MBA Student, Department of Commerce and Business Management, Veeranari Chakali Ilamma Women's University (Formerly University College for Women), Koti, Hyderabad, Telangana, India.*

multi-factor authentication with robust security systems, and staying updated on the latest trends. This chapter also looks at future trends in phishing attacks, such as the use of artificial intelligence, targeting cloud platforms, and exploiting mobile devices. Overall, chapter focuses on the need for businesses to implement robust cyber security strategies to reduce the risks of phishing attacks, protecting their operations and maintaining trust with their stakeholders.

Keywords: *Phishing attack, Social engineering, Malicious link, Cybersecurity, credentials, Multi- factor authentication.*

Introduction

In a busy office, a finance manages once received an email that exactly looks like it’s from a regular supplier asking for an urgent payment update. The mail also includes an attachment of a link to click on it. The manager thinking that it’s a regular mail, clicks the link. This innocent action opens the door to a clever phishing attack. Cybercriminals then got an access to sensitive financial information, putting the company at risk of losing money and damaging its reputation. This cautionary incident nightlights the need for business to stay alert and secure against online threats and scams like Phishing attack.

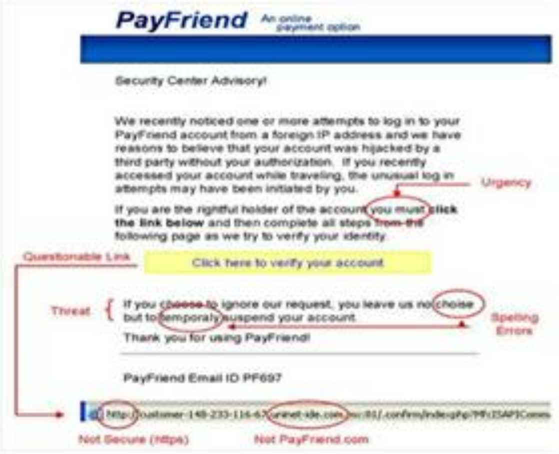
Phishing Attack

Phishing Attack is prevalent form of social engineering attack that mainly targets user’s information including login credentials like password, username and credit card details. It happens when an attacker, masquerading as a trustworthy entity, deceives a victim into opening an email, message or text. Then the victim is lured into clicking a harmful link, which can lead to malware installation, a ransomware attack, or the disclosure of sensitive information.

Phishing is also often used to gain access to corporate or government organizations as a part of larger attacks, including Advanced Persistent Threats (APTs). In such cases, employees are tricked to bypass security measures, spread malware within the secure environment. In addition to suffering large financial losses, a company snagged by a phishing scam can experience a domino effect, damaging its market share, reputation, and customer trust. Moreover the severity of the attack can trigger a full-blown security crisis, potentially leaving the organization with a long and difficult road to recovery.

Example for Phishing Attack

In 2019, there happened a cyber security incident at Crelan Bank in Belgium where phishing attackers gained an access to senior executive’s email account through which they sent deceptive emails to staff me members, posing as the senior executive. These fraudulent emails directed staff members to transfer funds to accounts which are under the control of attackers.



PayFriend An online payment option

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayFriend account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps ~~from the~~ following page as we try to verify your identity.

Click here to verify your account

If you ~~choose to~~ ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayFriend!

PayFriend Email ID PF697

http://customer-148-233-116-67.uninet-ide.com.mx:81/.confirm/index.php?Mfc ISAPICommand

Impact of this Incident: Crelan Bank lost a staggering $75.8 million due to this phishing attack.

Types of Phishing Attacks

1. **Email Phishing:** This is most common form of phishing, where attackers send fraudulent emails which contains malicious links or attachments, urging users to click or download that appear to be from authorized sources to steal sensitive information or install malware.

   Example: Fake account notifications, false security alerts and counterfeit invoice emails.

2. **Spear Phishing:** It is a more targeted form of phishing, where attackers customize emails to a specific individuals or organizations based on research about target, including their name, position and other details in order to steal their sensitive information.

Example: Emails that appear to be from a college or a business partner, requesting for sensitive information or asking recipient to click on a specific link.

3. **Whaling:** It is a highly targeted phishing attack that aims at senior executives and high profile individual like CEOs within the organization. Attackers use detailed information about the executive's role and responsibilities to craft convincing emails.

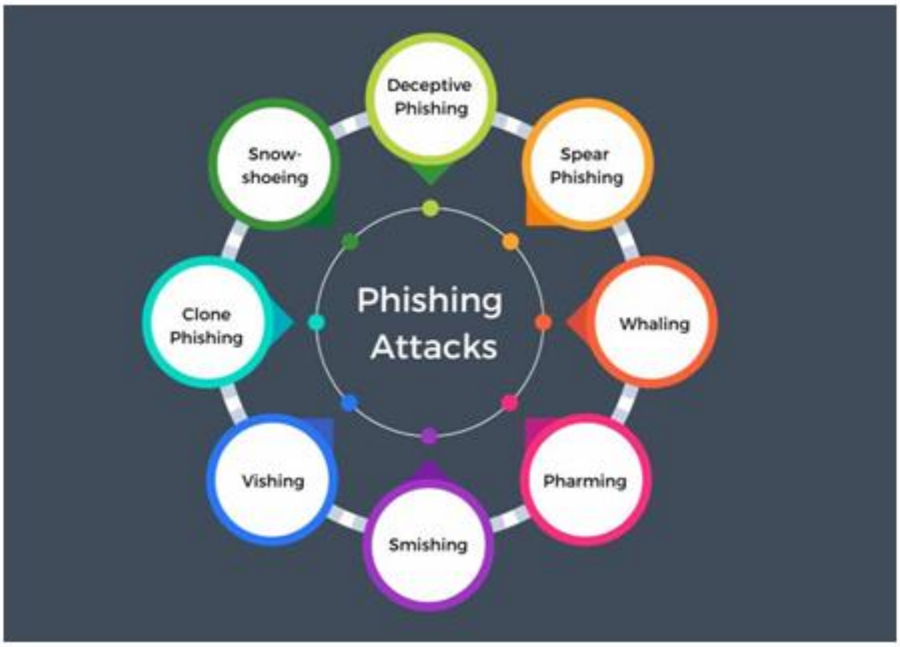
   Example: Emails posing as urgent requests from a CEO or CFO, often involving financial transactions or company's sensitive data.

4. **Smishing (SMS Phishing):** This is a type of phishing attack which is conducted through SMS messages rather than email. Attackers send text messages containing malicious links or phone numbers, urging recipients to respond or click.

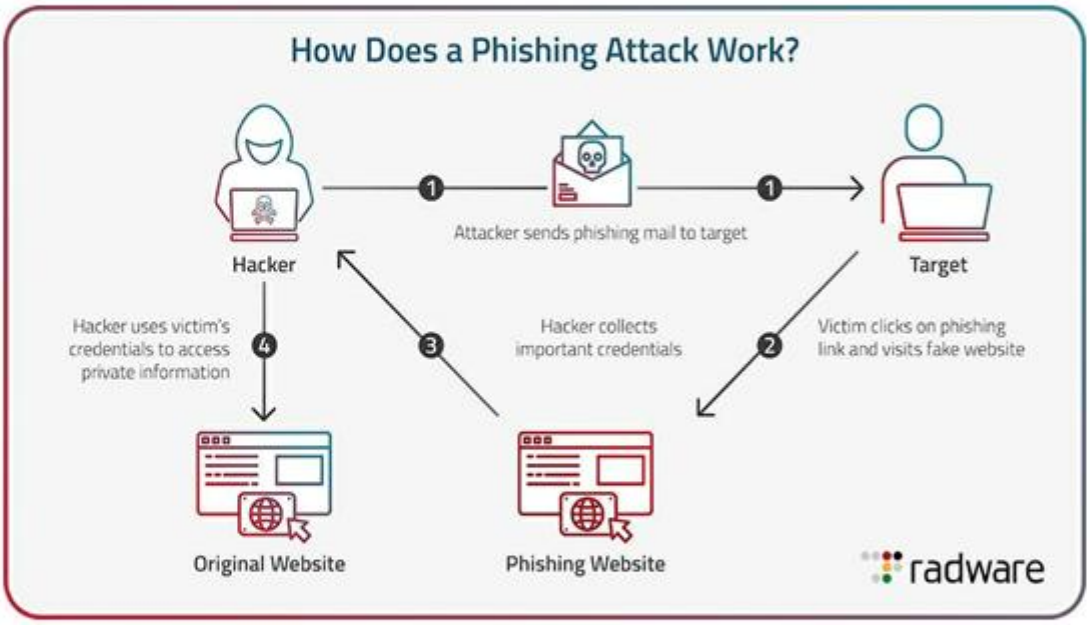
   Example: Fake messages from banks asking to verify account information or details, or fraudulent delivery notifications prompting the user to click on a link.

5. **Vishing (Voice Phishing):** Phishing attack carried out via phone calls, where attackers impersonate legitimate entities. It involves usage of social engineering to persuade victims to reveal personal information or transfer money.

Example: Calls pretending to be from a bank's fraud department, tax authorities, or tech support, claiming urgent action is needed.



Process of Phishing Attacks


How Does a Phishing Attack Work?
Hacker
1
Attacker sends phishing mail to target
1
Target
Hacker uses victim's credentials to access private information
4
3
Hacker collects important credentials
2
Victim clicks on phishing link and visits fake website
Original Website
Phishing Website
radware

Techniques of Phishing Attack in Business

1. **Deceptive Emails:** It a kind of phishing technique where emails that are sent to users appear to be from trusted sources, such as colleagues, executives, or well-known companies.

2. **Malicious Links:** These malicious links includes URLs that direct recipients to fraudulent websites designed to steal login credentials, personal information or install malware.

3. **Attachments:** These are files containing malware or ransomware that can infect the recipient's system upon opening.

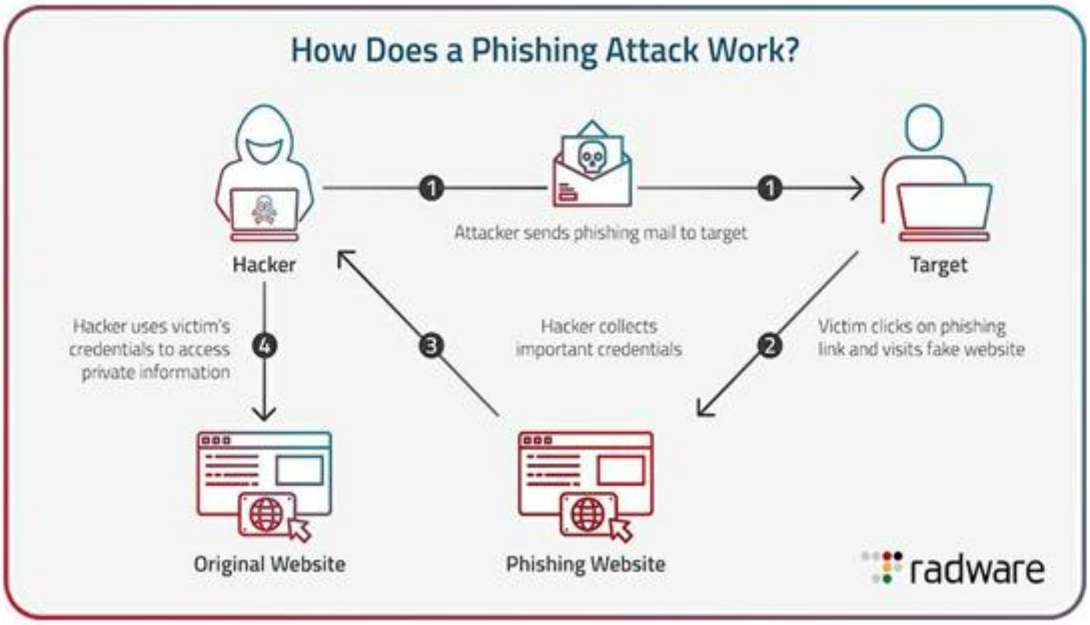
4. **Urgency and Fear Tactics:** It is a kind of phishing technique in which message are sent to users that create a sense of urgency or fear to prompt quick, unthinking action, such as claiming account suspension or requiring immediate verification.

5. **Impersonation of Trusted Entities:** In this technique familiar logos, emails address, and signature are used to appear legitimate to steal the users personal information either to steal money or identity damage of users.

6. **Spoofed Websites:** These are the fake websites mimicking legitimate business sites to collect sensitive information.

7. **Social Engineering:** Social engineering is a technique to manipulate individuals into divulging confidential information, often by pretending to be someone the recipient knows or trusts.

8. **Data Collection Forms:** These are the forms asking for sensitive information like passwords, credit details, or personal identification information.


How Does a Phishing Attack Work?
Hacker
1
1
Attacker sends phishing mail to target
Target
Hacker uses victim's credentials to access private information
4
3
Hacker collects important credentials
2
Victim clicks on phishing link and visits fake website
Original Website
Phishing Website
radware

Impact of Phishing Attacks on Business

Phishing attacks have a profound impact on business across several critical areas:

1. **Financial Losses:** Phishing attacks can lead to direct financial losses through fraudulent transactions, unauthorized access to financial accounts, or funds redirected to attacker-controlled accounts.

2. **Data Breaches and Loss of Sensitive Information:** Successful phishing attacks often result in compromise of sensitive company data, including customer information, intellectual property, and proprietary business data. This in turn lead to significant operational disruptions and potential legal liabilities.

3. **Damage to Brand Reputation and Customer Trust:** Publicized data breaches or instances of phishing can severely damage a company's reputation. Customers might lose trust in the organization's ability to protect their information, leading to decreased customer loyalty and potential loss of business.

4. **Legal and Regulatory Consequences:** Businesses may face legal consequences and regulatory fines if they fail to protect sensitive information adequately. Compliance failures with data protection laws such as GDPR or CCPA can result in substantial penalties and legal liabilities.

5. **Loss of Intellectual Property:** Phishing attacks targeting intellectual property can lead to unauthorized access and theft of valuable proprietary information, such as trade secrets, product designs, or strategic plans. This theft can severely impact a company's competitive advantage by giving competitors access to sensitive data. Moreover, it undermines future innovations as stolen intellectual property can be used to replicate products or services, and revenue earning potential.

6. **Employee Morale:** A sense of vulnerability and distrust within the workforce is created by phishing attacks which impact employee morale. Employees may feel stressed and anxious about the potential compromise of their potential information of financial data. This can result in decreased productivity as they may become hesitant to engage in digital communications, affecting overall workforce efficiency and morale.

7. **Operational Disruption:** Operational disruption from phishing attempts can cause significant downtime and reduced productivity as key systems or networks are compromised. Businesses may incur increased recovery costs associated with restoring systems, data integrity, and mitigating further security risks. Effective cyber security measures, including continuous monitoring and response protocols are essential to minimize these impacts and ensure operational resilience.

Case Studies of Phishing Attack on Business

Case Studies

Case Study 01-Upsher- Smith Laboratories – Loss of Nearly $39 Million

In 2014, Upsher-Smith Laboratories fell victim to CEO Fraud, a type of cyber- attack where malicious actors impersonate a company’s CEO via phishing emails. The attackers instructed the Accounts Payable Coordinator to transfer over $50 million to accounts they controlled, posing as the CEO and the company lawyer. Despite intercepting one transfer, Upsher-

Smith suffered a staggering loss of nearly $39 million. This incident underscores the severity of CEO Fraud, highlighting vulnerabilities inn corporate cyber security and the need for robust email security measures. It serves as a cautionary tale for organizations to enhance their defenses against sophisticated phishing attacks targeting financial transactions.

Case Study 02- Twitter Phishing Attack-2020

In July 202, a major Twitter phishing attack occurred when cyber criminals targeted Twitter employees with spear phishing tactics. Posing as Twitter IT administrators, the attackers convinces employees working from home to share their login credentials. With these compromised credentials, the attackers gained access to Twitter's administrator tools, allowing them to hijack high-profile accounts, including those of El on Musk, Barack Obama, Jeff Bezos, Apple, and Uber. They used these accounts to post scam messages requesting Bitcoin contributions. Due to the large followings of these accounts, the scam attracted significant attention, leading to over $180000 in Bit coin being transferred to the attackers. The incident was quickly noticed by the press, prompting Twitter to take immediate action to mitigate the damage.

Steps a Business Can take to Preventing these Phishing Attempts

Mitigating phishing attack impacts on business requires a proactive approach, including implementing robust cybersecurity measures, conducting regular security audits and employee training, and promptly responding to and reporting phishing incidents. By prioritizing cybersecurity and maintaining vigilance, businesses can mitigate the potential damages caused by phishing attacks and safeguard their operations and reputation.

1. **Regular Employee Training:** Regular Training sessions can educate employees on the latest phishing tactics in order prevent data breaches. These sessions helps in identifying suspicious messages.

2. **Multi-Factor Authentication (MFA):** Generally MFA adds an extra layer of privacy and security by requiring a second step besides a username and password. This may help in preventing financial and data loss.

3. **Robust Security Infrastructure:** Businesses should invest in advanced security solutions which can detect and block phishing attempts, including email filtering and endpoint security software. A strong security infrastructure has a capability to prevent phishing attacks by addressing the phishing emails.

4. **Staying Updated:** Staying informed about the latest phishing trends and updating security measures pro actively is crucial to stay ahead of cybercriminals and cyber security threats.

5. **Https Protocol:** Https helps prevent phishing by encrypting data between the user and the website, ensuring secure communication. It enables website authentication via SSL/TLS certificates, confirming the site’s legitimacy.

e-ISBN: 978-93-6252-974-9 | Year of Publication 2024
DOI: https://www.doi.org/10.58532/nbennuriach3

Borrowers display security indicators, like padlocks, to reassure users. Http reduces the risk of data interception and tampering by attackers. It also helps to maintain user trust and protect sensitive information..

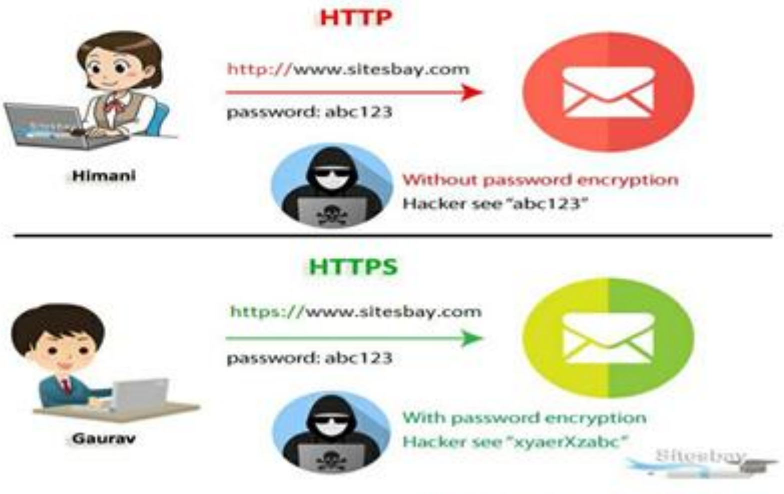


Fig: Difference Between http and https

Role of Phishing Prevention in Ensuring Sustainability of Business

1. **Highlighting Vulnerabilities:** phishing attacks expose security weakness within an organization, revealing areas that require immediate attention and improvement. By identifying these vulnerabilities, businesses can take steps to close gaps in their defenses.

2. **Investment in Security:** In response to phishing threats, organizations are motivated to invest in advanced cyber security measures. This includes upgrading software, employing specialized security teams, and implementing comprehensive security protocols to protect against future attacks.

3. **Employee Training:** Educating employees about phishing threats and how to recognize suspicious emails or activities is essential. Regular training sessions help employees to identify and avoid phishing attempts, reducing the likelihood of successful attacks and minimizing potential damage to the organization.

4. **Safeguarding Data:** With improved cyber security measures in place, businesses can better safeguard sensitive data. Protecting customer information, financial records, and proprietary data from unauthorized access ensures business continuity and compliance with data protection regulations.

5. **Maintaining Customer Trust:** Customers trust businesses to keep their personal and financial information secure. Effective prevention and mitigation of phishing attacks help to preserve this trust. When businesses demonstrate a commitment to protecting their customer's data, they strengthen their relationships and encourage customer loyalty.

6. **Resilience to Future Threats:** By addressing vulnerabilities and strengthening defenses, businesses become more resilient to future phishing attacks and other cyber security threats. This preparedness reduces the impact of potential breaches and ensures quick recovery.

7. **Long-Term Viability:** Proactive security measures contribute to the long-term sustainability and success of a business. By con tiny adopting to emerging threats and

maintaining robust defenses, business's can operate smoothly, avoiding disruptions and financial losses associated with cyberattacks.

8. **Fostering Growth and Innovation:** A secure business environment allows companies to focus on their core activities, such as growth and innovation, without being sidetracked by security concerns. By mitigating phishing risks, businesses can direct their resources and efforts towards developing new products, services, and strategies for long-term success.

9. **Preserving Corporate Reputation:** A business's reputation is one of its most valuable assets. Successfully addressing phishing threats helps avoid incidents that could damage public perception. When a company is known for its strong cyber security practices, it enhances its credibility and appeal to customers, partners, and investors.

10. **Advanced Security Technologies:** Employing cutting-edge security solutions such as email filters, multi-factor authentication, and threat detection systems enhance a business's ability to prevent and respond to phishing attacks. These act as a first line of defense, identifying and blocking phishing attempts before they can cause harm.

11. **Regulatory Compliance:** Adhering to industry regulations and standards related to cyber security helps businesses avoid legal and financial penalties. Compliance with regulations such as GDPR or HIPAA demonstrates a

commitment to safeguarding data and ensures that the business meets legal obligations, thereby maintaining its legitimacy.

Future Trends of Phishing Attack on Business

1. **AI- Powered Attacks:** Deep fakes and other Artificial Intelligence (AI) advancements could be used to create highly realistic phishing emails and messages, that mimicks the voices and appearances of executives or colleagues. This could make the emails even more believable and bypass traditional security measures.

2. **Cloud-Based Infiltration:** Phishing attacks might become more prevalent on cloud platforms such as collaboration tools and shared storage services which offer a wider reach for attackers and can potentially compromise a large number of users within an organization.

3. **Mobile Device Exploitation:** Phishing attempts might increase in number and attackers would focus on mobile users. As our reliance on mobile phones and tablets continues to grow, these phishing attempts will likely target these devices even more. These attacks have a capability to exploit social media platforms, messaging apps and even fake mobile application in order to steal sensitive information.

4. **Focus on Small Businesses:** Small businesses are increasingly becoming targets due to their typically weaker cyber security resources and lower employee awareness.

Attackers might leverage this vulnerability to gain access to critical DAT and financial resources.

5. **QR Code Phishing:** Malicious QR codes used in phishing messages are a recent trend. These QR codes can bypass security measures by hiding the true malicious URL behind the code.

6. **Social Engineering- a Major Weapon:** Social engineering would continue to increase in upcoming future and can be used as a major technique to steal sensitive information of users.

7. **Machine Learning Based Attacks:** Attackers will increasingly use machine learning to create more compromising phishing emails and messages. These technologies can help craft personalized and contextually relevant attacks that are harder to detect.

8. **Automated Phishing Kits:** The availability of automated phishing kits and services on the dark web would make it easier for less skilled attackers to launch sophisticated phishing campaigns.

Conclusion

Phishing attack represent a significant and evolving threat to business world. From the widespread email phishing to the highly targeted super phishing and executive-focused whaling, attackers continually adapt their tactics to exploit vulnerabilities. No single technology will completely stop phishing. However a combination of good organization and practice, proper application of current technologies and also improvements in security technologies has a potential to drastically reduce prevalence of phishing and losses suffered from it. It is crucial for organizations to maintain vigilance and implement proactive measures such as employee training, robust email filtering systems, multi-factor authentication, and regular security audits. These steps not only enhance awareness but also strengthen defenses against increasingly sophisticated phishing attempts. By prioritizing cyber security and fostering a culture of caution among employees, businesses can mitigate risks, safeguard sensitive DAT, and uphold trust with customers and stakeholders in an ever-challenging digital landscape. Everyone should be educated, updated according to technological improvements to reduce phishing attacks.

References

[1] en.m.wikipedia.org
[2] www.cybsafe.com
[3] www.ncsc.gov.uk
[4] www.stickmancyber.com
[5] fastercapital.com