Advanced Phishing Techniques: Analyzing Adversary-in-the-Middle and Browser-in-the-Browser Attacks in Modern Cybersecurity

Emerging Phishing Attacks: AiTM and BiTB Explored

JACOB O. DULDULAO

School of Information Technology, Mapúa University, joduldulao@mymail.mapua.edu.ph

JOHN VINCENT E. ESPEÑO

School of Information Technology, Mapúa University, jveespeno@mymail.mapua.edu.ph

DANIELLE B. MEER

School of Information Technology, Mapúa University, dbmeer@mymail.mapua.edu.ph

GEOFF STEPHEN M. PATAG

School of Information Technology, Mapúa University, gsmpatag@mymail.mapua.edu.ph

This paper focuses on two emerging and highly sophisticated phishing techniques: Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks, both of which have evolved to bypass traditional defenses like multi-factor authentication (MFA). These techniques represent the cutting edge of phishing tactics and are becoming increasingly common in targeted phishing campaigns against high-value entities, especially as attackers aim to undermine security protocols.

CCS CONCEPTS • Social engineering attacks • Authentication methods • Phishing defenses • Web-based interaction security • Online fraud detection

Additional Keywords and Phrases: Adversary-in-the-Middle (AiTM), Browser-in-the-Browser (BiTB), phishing, multi-factor authentication (MFA), social engineering, Zero Trust security, AI-driven threat detection

1 INTRODUCTION

Phishing attacks have been around for many years and remain one of the most common ways hackers trick people and steal sensitive information, like passwords or credit card details. However, as security technologies improve—such as the widespread use of Multi-Factor Authentication (MFA)—phishing techniques have also evolved to stay ahead. Attackers now use more advanced methods that go beyond simple emails or fake websites. This paper focuses on two of these new and dangerous methods: Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks.

In the past, phishing attacks often involved tricking someone into clicking a suspicious link or giving away personal information through fake websites. Today, techniques like AiTM and BiTB are more sophisticated. They allow attackers to bypass MFA, which was once considered a strong defense. These new phishing techniques make it harder to detect attacks, posing a serious risk to users and organizations alike.

An AiTM attack happens when a hacker puts themselves between the user and a trusted website, capturing login credentials and session tokens in real time. This makes it possible for the attacker to take control of a

user's session, even if MFA is in place. On the other hand, a BiTB attack tricks users by creating fake browser windows within real websites, making it look like they are logging into a legitimate service. Both methods are smart, dangerous, and can have serious consequences if not addressed properly.

The goal of this paper is to explore how these attacks work and why they are effective, using real-world examples from industries like finance, healthcare, and the public sector. These industries are prime targets because they store valuable data, and a successful attack can lead to financial loss or stolen personal information.

By analyzing these phishing techniques, we also aim to propose solutions that can help organizations prevent or minimize these threats. Some of the strategies discussed include Zero Trust security models, AI-based threat detection, and better user education. Understanding and addressing these new forms of phishing attacks is essential to keeping users safe in today's digital world.

1.1 Background on Phishing Attacks

Phishing is one of the oldest and most common cyberattacks used to steal sensitive information by tricking users into providing credentials or personal data. The word "phishing" comes from "fishing"—with attackers metaphorically casting a baited hook, hoping someone will "bite" by clicking a malicious link or sharing their information. Early phishing attacks date back to the 1990s, often involving emails pretending to come from trusted companies such as banks, requesting users to verify their accounts by clicking on a link.

Over time, phishing techniques evolved. Attackers shifted from basic email scams to more sophisticated campaigns, including fake websites, attachments laced with malware, and phone-based phishing (known as vishing). The reason phishing is still widely used today is its effectiveness—it takes advantage of human trust and carelessness, making it difficult for even tech-savvy users to always recognize it.

As cybersecurity defenses like anti-phishing filters improved, attackers began refining their methods. They now use personalized phishing attacks (spear phishing), which target specific individuals or organizations by using information gathered from public sources. This makes the scam appear more convincing. Phishing is not just about stealing passwords anymore; it is used to install malware, initiate financial fraud, or gain access to sensitive systems.

Despite advances in security technologies like firewalls and email filters, phishing remains one of the most successful attack methods because it exploits the human element—a weakness that technical solutions alone cannot completely fix. The rise of Multi-Factor Authentication (MFA) aimed to mitigate phishing attacks by requiring an additional step (like a code sent to your phone), but attackers have adapted again, leading to more advanced phishing techniques like Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks.

These modern phishing methods demonstrate that phishing is not only evolving but becoming more targeted and difficult to detect, forcing users and organizations to stay ahead of the curve by learning about new attack vectors and implementing stronger defenses.

1.2 The Role of Multi-Factor Authentication (MFA) in Security

Multi-Factor Authentication (MFA) is a security process that adds an extra layer of protection beyond just a password. It works by requiring users to provide two or more forms of authentication before they can access their accounts. These forms typically fall into three categories: something the user knows (like a password),

something they have (like a smartphone or hardware key), and something they are (like a fingerprint or facial recognition).

MFA has become widely adopted across various industries because passwords alone are often not enough to keep accounts secure. Many people reuse passwords or use weak ones, which makes them easy targets for hackers. Even if a password is stolen through a phishing attack or data breach, MFA can stop attackers from accessing an account unless they also have the second factor, such as a one-time code sent to the user's phone.

MFA significantly reduces the risk of unauthorized access, and it is now used by many organizations to secure systems and data. Banks, email providers, and online platforms encourage or even require users to enable MFA to protect their accounts from being hacked. The extra layer of authentication makes it harder for attackers to break in, even if they have compromised a user's password.

However, even with MFA in place, attackers have found ways to get around it. Advanced phishing attacks, like Adversary-in-the-Middle (AiTM) attacks, exploit the fact that MFA is based on real-time access. By intercepting both the password and the second factor in real time, attackers can log in to a system just as if they were the legitimate user. This bypass of MFA has become a serious concern in cybersecurity, as it shows that even modern security tools are not perfect.

As MFA becomes more common, attackers are developing new techniques like AiTM and Browser-in-the-Browser (BiTB) attacks to target users. These attacks demonstrate that while MFA is an important security tool, it is not a complete solution on its own. Organizations must combine MFA with other strategies, like Zero Trust models and AI-based threat detection, to better protect users from these evolving threats.

1.3 Introduction to AiTM and BiTB Attacks:

Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks are two advanced phishing techniques that have emerged to bypass traditional security measures, especially Multi-Factor Authentication (MFA). These attacks are becoming more popular because they are designed to trick users while avoiding detection by modern cybersecurity tools.

An AiTM attack works by placing the attacker between the user and the legitimate service, like an email provider or banking website. This allows the attacker to intercept the user's login credentials and session tokens in real-time. What makes this attack especially dangerous is that even if the service requires MFA, the attacker can forward the MFA code to the real service, gaining access as if they were the user. These attacks have been reported in several high-profile incidents, showing that they are becoming a common tool for hackers targeting companies and individuals.

The BiTB attack takes a different approach. Instead of intercepting a real connection, it creates a fake login pop-up within the user's browser. For example, if a website asks the user to log in through Google or Microsoft, the BiTB attack will generate a fake login window that looks exactly like the real one. This tricks users into entering their credentials and MFA codes into the fake window, giving the attacker everything they need to access the user's accounts.

Both AiTM and BiTB attacks demonstrate how phishing tactics are evolving to target not just passwords, but also MFA and other security measures. These attacks are difficult to detect because they rely on mimicking normal user behavior and processes. Understanding how these attacks work is crucial for developing better

defenses and staying ahead of attackers. This paper explores these two attack types in detail, providing case studies and recommendations to help organizations protect themselves from these growing threats.

1.4 Research Goals and Structure:

The primary goal of this paper is to explore two advanced phishing techniques—Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks—and to understand how they bypass modern security measures like Multi-Factor Authentication (MFA). By examining these attacks, this research aims to raise awareness of the growing sophistication of phishing campaigns and provide actionable solutions to combat them.

This paper also looks at the impact of these phishing techniques on different industries, such as finance, healthcare, and the public sector. These industries are often targeted because they store valuable data, and a successful attack can cause financial damage, data breaches, or disruptions in critical services. Through real-world case studies, this research provides insight into how these attacks unfold and how organizations have been affected by them.

In addition, the paper proposes defense strategies that organizations can use to detect and mitigate these threats. Techniques like the Zero Trust security model and AI-driven threat detection systems are explored as potential solutions to strengthen defenses. The role of user education is also emphasized, as awareness is a key factor in reducing the effectiveness of phishing attacks.

This paper is organized into six main sections. After the introduction, Section 2 provides a detailed analysis of AiTM attacks, explaining how they work and why they are effective. Section 3 focuses on BiTB attacks, showing how they mimic legitimate browser windows to steal credentials. Section 4 presents case studies from the finance, healthcare, and public sectors, highlighting the real-world consequences of these phishing techniques. Section 5 discusses defense mechanisms, offering practical recommendations for detecting and preventing these attacks. Finally, Section 6 provides a summary of key findings and suggestions for future research, along with concluding thoughts on the future of phishing.

This structure ensures a thorough exploration of both AiTM and BiTB attacks, making the research not only informative but also practical for those looking to improve their cybersecurity defenses.

2 ADVERSARY IN THE MIDDLE (AITM) ATTACKS

Adversary-in-the-Middle (AiTM) attacks represent a significant evolution in phishing techniques. Unlike traditional phishing, which focuses on tricking users into providing their credentials, AiTM attacks go a step further by intercepting login sessions in real time. These attacks are particularly dangerous because they can bypass Multi-Factor Authentication (MFA), a security measure designed to prevent unauthorized access. With attackers acting as an invisible middleman between the user and the legitimate service, AiTM attacks allow cybercriminals to steal session tokens and gain full control over accounts without raising suspicion. This section explores how AiTM attacks work, the techniques attackers use to carry them out, and the real-world impact these attacks have had on different industries.

2.1 Adversary in the Middle Attacks

The Man in the middle attack is a common type of network attack wherein an intruder is able to sit in between two communicating network endpoints, gaining access to data being transferred throughout the communication. MITM attacks come in forms (Mahapatra, et. al.) such as:

1. Passive MitM - eavesdropping on a conversation to access information being sent throughout
2. Tampering - editing information being shared between two endpoints
3. Delaying - delaying data being sent between two networks, causing an interruption in the network's processes
4. Dropping - completely deleting information being sent during communication, causing significant data loss within the network

Various approaches are also used to penetrate a connection and infiltrate a communication, such as spoofing and decryption. Anyone can fall as a target for man in the middle attacks, as communication between multiple devices are common in several types of system architectures and applications. Upon breach of communication, attackers can access information almost unnoticed, making MITM prevention a serious security priority and organization.

A prevalent type of man in the middle attack is the adversary in the middle attack. Adversary in the middle attacks can refer to the active versions of man in the middle attacks, wherein information is hijacked and stolen, or interacting with information while it is being sent throughout the network. Adversary in the middle attacks is a term normally related to multi-factor authentication bypassing, as more prevalent approaches have found ways to infiltrate these authentication processes.

2.2 Multi Factor Authentication

Adversary in the middle has been heavily prevalent against multi factor authentication (MFA). This is because MFA follows a decentralized, multi-device approach, which requires the user to login using more than one device to approve verification. As this may be a better approach to improve simpler authentication such as password-based authentication in preventing various attacks such as password hijacking and shoulder surfing, its decentralized nature makes it vulnerable to AITM. Based on the AITM model, attackers can intercept communication between two devices, allowing them to illegally phish for confidential information and real time authentication data, without being detected. With this, multi-factor authorization must be properly studied and implemented to ensure its overall security.

A study by Amft, et. al., aimed to assess account recovery loss using multi-factor authentication in terms of its security, implementation, and user experience. With the rapid growth of MFA as a main form of authentication to improve the simpler authentication methods such as password-based authentication, its drawbacks must also be assessed and require equal attention. In the study, 71 websites were assessed in its use of MFA to determine how insecure the use of MFA really is, along with determining steps to take to improve its implementation. The researchers conducted the study by creating accounts on websites that required MFA and utilizing the MFA to recover the account after a certain amount of time. Through this, the researchers were able to determine that mobile apps, SMS, emails, and hardware token were the most used methods of MFA. Not only this, but some websites have also been assessed as implemented poorly, as they were unable to gain access to 23 of the accounts.

As multi-factor authentication was developed to strengthen password-based authentication, according to Gavazzi, et. al., MFA has been recorded with low adoption rates. Because of this, risk-based authentication has become another highly recommended form of authentication. This type of authentication assesses the probability of account compromise, and if detected, prompts the user for more verifying action to gain access. The study by Gavazzi, et. al. aimed to measure the availability and usage of MFA and RBA on the web, along with additional authentication factors used, and the use of single sign on across various websites. 208 popular sites in the Tranco top 5K that support account creation were used to assess the study. Based on the study, only 43% of the websites audited offered any form of MFA. Upon further assessment, however, if each account that does not support MFA and/or RBA were to be made through an SSO provider that does, about 80% would have access to MFA and 72% of sites would block suspicious login attempts.

3 BROWSER-IN-THE-BROWSER (BITB) ATTACKS

Browser-in-the-Browser (BiTB) attacks are a new type of phishing technique that relies on tricking users through fake pop-up windows within their web browser. These attacks are particularly effective because they mimic the exact look and feel of legitimate login windows, such as Google, Microsoft, or social media platforms. Users often encounter such login windows when they need to sign in through third-party services, making the fake windows appear normal. What makes BiTB attacks so dangerous is that even careful users can fall for them, as the fake windows look authentic and include all the details people expect, like URLs and security icons. This section dives into how BiTB attacks work, the tricks attackers use to make them convincing, and real-world cases where these attacks have been used successfully.

3.1 What Are BiTB Attacks

Browser-in-the-Browser (BiTB) attacks are phishing attacks that trick users by creating fake login windows inside their web browser. These attacks are designed to look exactly like legitimate pop-ups from trusted services, such as Google or Microsoft, which users are often asked to log into when using single sign-on (SSO). The goal of a BiTB attack is to make the user believe they are entering their credentials into a secure login window, but instead, the information goes directly to the attacker.

A common scenario for a BiTB attack is when a user tries to access a service that asks them to log in using a third-party account, like "Sign in with Google." In a BiTB attack, the pop-up window asking for the login details is fake, even though it looks identical to the real one. Since users are used to seeing these kinds of login windows, they usually don't suspect anything unusual and enter their username, password, and MFA code. Once the user does this, the attacker collects all the information they need to access the victim's account.

3.2 Technical Aspects of BiTB Attacks

The effectiveness of Browser-in-the-Browser (BiTB) attacks lies in how accurately the attacker can mimic a legitimate login pop-up window. These fake windows are designed to look identical to real ones, including the same layout, fonts, colors, and buttons. Attackers can even replicate the address bar, showing what looks like a trusted URL (such as "accounts.google.com") to fool the user into thinking the pop-up is authentic. Some advanced attacks may also add lock icons and other visual cues associated with secure websites, making it difficult to notice anything suspicious.

Technically, these fake login windows are not separate browser windows but are embedded directly within the main browser page using HTML and JavaScript. Unlike real pop-ups, the fake ones cannot be dragged or resized, but this difference is subtle and often goes unnoticed by users. This method allows attackers to bypass certain security features, such as popup blockers, that would normally prevent a separate phishing window from appearing.

Another important feature is the single sign-on (SSO) mechanism, which is commonly targeted in BiTB attacks. SSO is meant to make logging in more convenient by allowing users to access multiple services with a single account (like Google or Microsoft). Since users are familiar with seeing login windows for these services, attackers can exploit this behavior, making the fake window feel natural.

Once the victim enters their credentials into the fake window, the attacker can collect everything in real-time, including the username, password, and MFA code if used. This allows the attacker to log into the victim's account immediately without raising any red flags.

3.3 Examples of BiTB Attacks in the Wild

BiTB attacks have been observed in several real-world scenarios, often targeting services that rely heavily on single sign-on (SSO) systems like Microsoft 365, Google Workspace, and social media platforms. These attacks are especially effective in environments where users are accustomed to seeing login pop-ups, making them more likely to fall for the scam.

One notable example involves attacks against Microsoft 365 accounts. In these cases, employees were tricked into entering their credentials into a fake Microsoft login window embedded in a phishing email's link. Since the pop-up looked identical to a legitimate Microsoft SSO login, employees unknowingly handed over their login credentials and MFA codes to attackers. Once inside, attackers had access to email accounts and sensitive company documents, leading to data breaches and financial fraud.

Another example occurred in the finance industry, where attackers used BiTB techniques to steal credentials from employees accessing online banking systems. A fake "Sign in with Google" window was created inside a phishing site, and the victims entered their Google account credentials, thinking they were performing a routine login. With access to these accounts, attackers were able to view and transfer funds, causing significant financial losses for the affected companies.

These examples show how BiTB attacks can have severe consequences, not only for individuals but also for organizations. They highlight the importance of being aware of these phishing tactics, especially in industries like finance, healthcare, and business, where the impact of a successful attack can be devastating.

4 CASE STUDIES

Examining real-world cases of Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks provides valuable insight into how these techniques are used by attackers and the damage they can cause. These case studies help us understand the specific methods used, the industries targeted, and the weaknesses that were exploited. By analyzing these incidents, we can identify patterns and develop strategies to prevent similar attacks in the future. This section focuses on notable examples from the finance, healthcare, and public sectors, where attackers have used AiTM and BiTB tactics to gain unauthorized access, steal sensitive data, or cause financial harm.

4.1 AiTM Attack in the Finance Industry

One real-world example of an Adversary-in-the-Middle (AiTM) attack occurred in the finance industry, targeting the online banking systems of high-profile institutions. Attackers used phishing emails to lure employees and customers into clicking on a link that led to a fake banking login page. The fake page looked identical to the legitimate one, tricking victims into entering their usernames, passwords, and MFA codes.

Once the victims entered their credentials, the attacker intercepted them in real-time and forwarded them to the real banking system. With the session token generated by the real site, the attacker gained full access to the user's account, bypassing MFA entirely. The attacker could then initiate transactions, change account settings, or extract personal data without raising suspicion, as everything seemed normal on the user's end.

In one reported case, a financial institution lost millions because attackers initiated fraudulent transfers after gaining access to several customer accounts. The breach was discovered only after customers reported suspicious activity. By that time, the stolen funds had already been transferred through multiple accounts, making it difficult to recover the money.

This example highlights how AiTM attacks can cause severe financial harm by bypassing security measures like MFA. It also emphasizes the need for stronger fraud detection systems and behavioral monitoring tools to identify unusual activities, even when a session appears legitimate.

4.2 BiTB Attack in the Healthcare Industry

A Browser-in-the-Browser (BiTB) attack was recently reported in the healthcare industry, where attackers targeted medical professionals accessing online patient management systems. Healthcare workers were sent phishing emails disguised as important notifications from their software provider. The email included a link that redirected them to a legitimate-looking login page with a pop-up window, prompting them to "Sign in with Google" to access their accounts.

The pop-up window was a fake, created using BiTB techniques. It looked identical to Google's usual login window, complete with the expected URL and security icons. Trusting the familiar interface, users entered their Google credentials and MFA codes, unknowingly providing attackers with access to their accounts.

With access to these Google accounts, the attackers were able to steal confidential patient information, including medical histories and personal identification. The breach disrupted hospital operations, as doctors and staff had to halt certain activities while investigating the compromise. Furthermore, the exposure of sensitive patient data created legal and financial risks for the healthcare provider, as they faced fines for violating data privacy regulations like HIPAA.

This case demonstrates how BiTB attacks can cause significant harm in industries that handle sensitive data. It also highlights the importance of employee training on identifying phishing attempts and the need for stronger authentication tools beyond MFA.

4.3 Other Relevant Case Studies

Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks have also been observed in the public sector and government agencies, where attackers sought access to classified or critical infrastructure systems. In one instance, government employees were targeted by a sophisticated phishing campaign using AiTM techniques. Phishing emails disguised as official government correspondence directed employees to a fake internal portal. Even though the portal required MFA, the attackers intercepted both login credentials and

MFA tokens in real-time, allowing them to access sensitive systems. This breach caused serious security concerns, as it exposed internal government communications and critical files to unauthorized individuals.

In the education sector, university faculty and students were targeted through BiTB attacks. Attackers sent emails that appeared to be from the school's IT department, requesting users to log into their Microsoft 365 accounts to resolve "account issues." A fake Microsoft login window was generated inside the phishing page using BiTB techniques. Several users entered their credentials and MFA codes, giving the attackers access to emails, assignments, and institutional data. The attack disrupted academic operations and forced the university to reset affected accounts and strengthen its login procedures.

These examples show that AiTM and BiTB attacks are not limited to the finance and healthcare sectors but pose a threat to any organization with valuable data. Whether targeting public institutions, educational systems, or businesses, these advanced phishing techniques demonstrate the need for robust cybersecurity measures across all sectors.

5 DEFENSE MECHANISMS

As phishing attacks like Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) become more advanced, it is essential for organizations to adopt stronger defenses. Traditional security measures such as Multi-Factor Authentication (MFA) are no longer enough, as these attacks are designed specifically to bypass them. Effective defense strategies require a combination of technology, policy, and user education. This section explores several practical ways to detect, prevent, and mitigate AiTM and BiTB attacks. These include the adoption of Zero Trust security models, AI-driven threat detection systems, and user awareness programs to reduce the chances of users falling victim to these phishing techniques.

5.1 Detecting and Preventing AiTM Attacks

Detecting and preventing Adversary-in-the-Middle (AiTM) attacks requires a combination of proactive security tools and strategies since these attacks are designed to bypass traditional defenses like MFA. One effective approach is implementing a Zero Trust security model, which assumes that every request—whether from inside or outside the network—must be verified before access is granted. With Zero Trust, even if an attacker hijacks a session, the system will continuously verify activities and detect unusual behavior, limiting the attacker's ability to do damage.

Another important defense mechanism is the use of AI-driven threat detection systems. These systems can analyze login patterns and detect abnormal behavior, such as multiple logins from different locations within a short period. AI models can also identify phishing patterns in real-time, blocking suspicious login attempts before attackers gain access to the system.

In addition, certificate-based authentication provides an extra layer of security. This method ensures that only devices with valid digital certificates can access sensitive systems, making it much harder for attackers to intercept communications. Session management tools are also essential, as they can detect and terminate compromised sessions if suspicious activity is detected during an active login.

Lastly, organizations should deploy network monitoring tools that can identify signs of a potential AiTM attack, such as unusual traffic patterns or multiple failed login attempts. By combining these technologies with strong security policies and user awareness, organizations can reduce the risk of falling victim to AiTM attacks.

5.2 Mitigating BiTB Attacks

Mitigating Browser-in-the-Browser (BiTB) attacks requires a combination of technical measures and user awareness training. Since BiTB attacks mimic legitimate login windows, the key defense lies in teaching users how to spot subtle differences between real and fake windows. For example, users should be trained to recognize that legitimate pop-ups can be dragged and resized, while fake BiTB windows usually cannot. Promoting a habit of manually entering URLs instead of clicking on login links also reduces the risk of falling for BiTB attacks.

On the technical side, anti-phishing browser extensions and web filters can block access to known phishing sites. These tools can detect suspicious behaviors on websites, such as embedded elements that resemble login windows, and alert users before they interact with them. AI-powered detection systems can also be used to analyze login requests and flag unusual login attempts that don't match the user's normal behavior.

Organizations can further protect users by adopting phishing-resistant authentication methods, such as hardware-based security keys like FIDO2. These keys verify both the user and the website during login, ensuring that credentials cannot be used on a fake site. Additionally, browser isolation technology can help by running risky websites in a separate, protected environment, preventing phishing content from interacting with the user's device.

Lastly, security policies that enforce frequent awareness training and phishing simulations can help users stay prepared for emerging threats. By using both technical tools and user education, organizations can better defend against BiTB attacks and minimize the risk of credential theft.

5.3 The Role of AI in Phishing Defense

Artificial Intelligence (AI) plays a crucial role in detecting and preventing advanced phishing attacks like AiTM and BiTB. Traditional security systems often rely on fixed rules and predefined patterns to identify threats, but modern phishing techniques are more dynamic and unpredictable. AI-powered tools can analyze large amounts of data in real-time, learning to recognize patterns and behaviors that might indicate a phishing attack, even if it is a new or unknown type of attack.

One way AI helps is by monitoring login behavior. AI models can flag unusual login attempts, such as logins from unfamiliar devices or locations, which could indicate an AiTM or BiTB attack. This gives security teams a chance to block the login or ask for additional verification before granting access. AI can also detect inconsistencies in session behavior, such as a user logging into multiple accounts from different locations within a short time, a common sign of AiTM attacks.

In the context of BiTB attacks, AI can identify fake login windows by examining how they behave compared to real ones. For example, an AI model might detect that a pop-up window behaves differently from a legitimate browser window or contains embedded elements designed to mimic a secure login page.

Another important role AI plays is in phishing email detection. Machine learning algorithms can analyze incoming emails for suspicious content, such as subtle changes in domain names or phrasing that might indicate a phishing attempt. These systems can block or quarantine phishing emails before they reach users, preventing attacks from being carried out in the first place.

Overall, AI-based tools provide an adaptive and proactive approach to phishing defense, evolving as threats change. By combining AI-driven detection systems with other security measures, organizations can respond more effectively to phishing attempts and reduce their risk of compromise.

6 CONCLUSION

The growing sophistication of phishing attacks, such as Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB), demonstrates that traditional security measures are no longer enough to protect users and organizations. These attacks exploit both technical vulnerabilities and human behavior, allowing attackers to bypass safeguards like Multi-Factor Authentication (MFA) and gain unauthorized access to sensitive information. As these threats become more common, it is critical to develop a deeper understanding of how they work and implement more effective defense strategies.

The case studies presented in this paper highlight the real-world impact of AiTM and BiTB attacks across industries such as finance, healthcare, and the public sector. These examples show that no organization is immune to phishing, and the consequences can be severe, ranging from financial losses to data breaches and operational disruptions.

Defending against AiTM and BiTB attacks requires multiple layers of protection. Organizations must adopt Zero Trust security models, which continuously verify both users and activities to limit the damage that a compromised session can cause. AI-driven threat detection systems are also essential, providing real-time analysis of login behaviors and identifying suspicious patterns before attackers can complete their goals. Additionally, user education remains a key component of defense, as many attacks rely on tricking users into sharing their credentials.

While no solution is foolproof, the combination of advanced technologies, strong security policies, and regular user training can significantly reduce the risk of falling victim to these phishing attacks. As phishing techniques continue to evolve, it is important for organizations to stay vigilant and proactive in their cybersecurity efforts, ensuring they are prepared to respond to emerging threats. Future research should focus on refining detection methods and exploring new ways to enhance phishing defense, as attackers will undoubtedly continue to find creative ways to bypass security measures.

6.1 Key Findings

This research highlights the evolving nature of phishing attacks and the challenges they pose to modern cybersecurity defenses. Adversary-in-the-Middle (AiTM) attacks show how attackers can intercept login sessions and bypass Multi-Factor Authentication (MFA) by acting as a middleman between users and legitimate services. Browser-in-the-Browser (BiTB) attacks demonstrate how attackers can exploit familiar user behaviors by creating convincing fake login pop-ups to steal credentials and MFA codes. Both attack types are effective because they rely on a combination of social engineering and technical mimicry, making them difficult to detect and prevent.

The case studies explored in this paper show the real-world consequences of AiTM and BiTB attacks across key industries, including finance, healthcare, and the public sector. These attacks have resulted in financial losses, data breaches, and service disruptions, proving that even organizations with strong security measures are at risk. This research underscores the need for proactive defense strategies to combat these evolving phishing threats.

6.2 Recommendations for Future Research

While this paper provides an in-depth analysis of Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) attacks, further research is needed to keep up with the evolving nature of these threats. Future

studies could explore more advanced detection methods, such as refining AI-based phishing detection tools to improve their ability to identify new attack vectors. Additionally, research on behavioral analysis algorithms could help develop systems that can better recognize unusual login patterns or suspicious session activity in real time.

Another area of research is the effectiveness of Zero Trust models when deployed at scale. While Zero Trust is gaining popularity, there is still limited data on how well it performs in preventing phishing attacks across different industries. Investigating how organizations can implement these models effectively, without disrupting operations, will be valuable in strengthening defenses.

There is also a need for user-focused studies that explore how people interact with phishing attempts. Understanding what makes users fall for attacks like BiTB or AiTM can lead to more effective training and awareness programs. Developing better ways to teach employees and users how to identify phishing attempts remains a crucial component in defense strategies.

Lastly, as new technologies like quantum computing and blockchain emerge, future research should investigate how these tools might both enhance phishing defenses and introduce new vulnerabilities. The dynamic nature of cybersecurity requires continuous research to ensure that defenses remain effective against the latest threats.

6.3 Final Thoughts on the Future of Phishing

As cybersecurity defenses improve, phishing attacks will continue to evolve, becoming more sophisticated and harder to detect. Techniques like Adversary-in-the-Middle (AiTM) and Browser-in-the-Browser (BiTB) represent just the beginning of a trend where attackers focus not only on stealing credentials but also on bypassing advanced protections like Multi-Factor Authentication (MFA). The use of real-time session hijacking and convincing fake browser elements suggests that future phishing attacks will increasingly target human behavior and trust.

Organizations must recognize that phishing is not just a technical problem but also a human challenge. While technologies like AI-driven threat detection and Zero Trust security will play an important role, user awareness and education will remain a critical line of defense. Attackers will likely continue to exploit single sign-on (SSO) platforms and browser interfaces, pushing organizations to adopt more phishing-resistant authentication methods, such as security keys.

Looking ahead, the rise of new technologies could bring both opportunities and challenges for cybersecurity. As AI becomes more accessible, attackers may use it to create more personalized phishing campaigns, making them even harder to detect. On the other hand, AI-powered defenses and emerging technologies like biometrics will provide new ways to strengthen security.

The battle against phishing is ongoing, and staying ahead of attackers will require continuous adaptation. Organizations must stay proactive, updating their security practices regularly and embracing new technologies to combat future threats. By fostering a culture of cybersecurity awareness and adopting advanced defense models, businesses and individuals can reduce the risks posed by evolving phishing techniques and build stronger, more resilient systems.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to Mapúa University for providing access to research resources and guidance throughout this project. We also extend our thanks to our instructor, sir Eric Blancaflor, whose insights and feedback we're sure will shape the direction of this research. Additionally, we appreciate the collaboration and teamwork of our group members: Jacob Duldulao, John Espeño, Danielle Meer, and Geoff Patag, who worked diligently on this project.

Finally, we would like to recognize the open-access tools, libraries, and online resources, such as research databases and technical reports, which contributed to our understanding of AiTM and BiTB attacks. This paper would not have been possible without these valuable sources of information and collective efforts.

REFERENCES

[1] Alessandro Ecclesie Agazzi. 2020. Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them. https://doi.org/10.48550/arXiv.2006.00577

[2] Mahmood A. Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H. Hasbullah. 2020. Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks. Retrieved October 14, 2024 from https://papers.ssrn.com/abstract=3662935

[3] Gokul Anand, Sahaya Beni Prathiba, Gunasekaran, and Ponmani. 2018. Detection of Man In The Middle Attacks in Wi-Fi networks by IP Spoofing. In *2018 Tenth International Conference on Advanced Computing (ICoAC)*, December 2018. 319–322. https://doi.org/10.1109/ICoAC44903.2018.8939063

[4] Gheorghe Romeo Andreica, Liviu Bozga, Daniel Zinca, and Virgil Dobrota. 2020. Denial of Service and Man-in-the-Middle Attacks Against IoT Devices in a GPS-Based Monitoring Software for Intelligent Transportation Systems. In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, December 2020. 1–4. https://doi.org/10.1109/RoEduNet51892.2020.9324865

[5] Sultan Asiri, Yang Xiao, and Saleh Alzahrani. 2024. Towards Improving Phishing Detection System Using Human in the Loop Deep Learning Model. In *Proceedings of the 2024 ACM Southeast Conference* (*ACMSE '24*), April 27, 2024. Association for Computing Machinery, New York, NY, USA, 77–85. https://doi.org/10.1145/3603287.3651193

[6] Sultan Asiri, Yang Xiao, and Tieshan Li. 2024. PhishTransformer: A Novel Approach to Detect Phishing Attacks Using URL Collection and Transformer. *Electronics* 13, 1 (January 2024), 30. https://doi.org/10.3390/electronics13010030

[7] Burak Aydın, Hakan Aydın, and Sedat Görmüş. 2024. A Security Mechanism Against Man in the Middle Attack in 6TiSCH Networks. In *2024 32nd Signal Processing and Communications Applications Conference (SIU)*, May 2024. 1–4. https://doi.org/10.1109/SIU61531.2024.10600741

[8] Jasmin Bharadiya. 2023. Machine Learning in Cybersecurity: Techniques and Challenges. *European Journal of Technology* 7, 2 (June 2023), 1–14. https://doi.org/10.47672/ejt.1486

[9] Andrea Chezzi, Christian Catalano, and Franco Tommasi. 2024. Bitm+ Attack: An Improved Bitm/Mitb-Based Phishing Attack Capable of Passing Through and Defeating the Fido/Ctap2 Protocol and the W3c Webauthn Api. https://doi.org/10.2139/ssrn.4711140

[10] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. 2016. A Survey of Man In The Middle

Attacks. *IEEE Communications Surveys & Tutorials* 18, 3 (2016), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426

[11] Vishalkumar Ravindrakumar Gajjar and Hamed Taherdoost. 2024. Examining Cyber Threats and Vulnerabilities: A Deep Dive into British Columbia's Cybersecurity Landscape. In *2024 International Conference on Expert Clouds and Applications (ICOECA)*, April 2024. 240–245. https://doi.org/10.1109/ICOECA62351.2024.00052

[12] Aaron Henricks and Houssain Kettani. 2020. On Data Protection Using Multi-Factor Authentication. In *Proceedings of the 2019 International Conference on Information System and System Management* (*ISSM 2019*), May 31, 2020. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3394788.3394789

[13] Nadim Ibrahim, N. R. Rajalakshmi, and Karam Hammadeh. 2024. Exploration of Defensive Strategies, Detection Mechanisms, and Response Tactics against Advanced Persistent Threats APTs. *Nanotechnology Perceptions* (May 2024), 439–455. https://doi.org/10.62441/nano-ntp.v20iS4.33

[14] Almaz Idiyatullin and Pavel E. Abdulkin. 2021. A Research of MITM Attacks in Wi-Fi Networks Using Single-board Computer. In *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, January 2021. 396–400. https://doi.org/10.1109/ElConRus51938.2021.9396241

[15] Ankit Kumar Jain and B.B. Gupta. 2022. A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems* 16, 4 (April 2022), 527–565. https://doi.org/10.1080/17517575.2021.1896786

[16] Sotonye Kalio. 2022. Phishing Attack: Raising Awareness and Protection Techniques. https://doi.org/10.31234/osf.io/uxeth

[17] Keshav Kaushik, Vanshika Singh, and V. Prabhu Manikandan. 2022. A Novel Approach for an Automated Advanced MITM Attack on IoT Networks. In *Advancements in Interdisciplinary Research*, 2022. Springer Nature Switzerland, Cham, 60–71. https://doi.org/10.1007/978-3-031-23724-9_6

[18] Brian Kondracki, Babak Amin Azad, Oleksii Starov, and Nick Nikiforakis. 2021. Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '21*), November 13, 2021. Association for Computing Machinery, New York, NY, USA, 36–50. https://doi.org/10.1145/3460120.3484765

[19] D.O. Lawal, D.W. Gresty, D.E. Gan, and T.C. Durojaiye. 2023. Forensic Implication of a Cyber-Enabled Fraud Taking Advantage of an Offline Adversary-in-the-Middle (AiTM) Attack. In *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, May 2023. 1258–1263. https://doi.org/10.23919/MIPRO57284.2023.10159879

[20] Avijit Mallik. 2019. MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. *Cyberspace: Jurnal Pendidikan Teknologi Informasi* 2, 2 (January 2019), 109–134. https://doi.org/10.22373/cj.v2i2.3453

[21] Sundaram Mishra, Shivam Mishra, Yan Chi Toh, Satyam Mishra, and Phung Thao Vi. 2024. Mitigating the Threat of Multi-Factor Authentication (MFA) Bypass Through Man-in-the-Middle Attacks Using EvilGinx2. In *Creative Approaches Towards Development of Computing and Multidisciplinary IT Solutions for Society*. John Wiley & Sons, Ltd, 59–78. https://doi.org/10.1002/9781394272303.ch5

[22] Ogugua Chimezie Obi, Onyinyechi Vivian Akagha, Samuel Onimisi Dawodu, Anthony Chigozie Anyanwu `, Shedrack Onwusinkwue, and Islam Ahmad Ibrahim Ahmad `. 2024. COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES. *Computer Science & IT Research Journal* 5, 2 (February 2024), 293–310. https://doi.org/10.51594/csitrj.v5i2.758

[23] Bhargav Pingle, Aakif Mairaj, and Ahmad Y. Javaid. 2018. Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use. In *2018 IEEE International Conference on Electro/Information Technology (EIT)*, May 2018. 0192–0197. https://doi.org/10.1109/EIT.2018.8500082

[24] Aya H. Salem, Safaa M. Azzam, O. E. Emam, and Amr A. Abohany. 2024. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *J Big Data* 11, 1 (August 2024), 105. https://doi.org/10.1186/s40537-024-00957-y

[25] Ahmet Nail Taştan, Serkan Gönen, Mehmet Ali Barışkan, Cemallettin Kubat, Derya Yıltaş Kaplan, and Elham Pashaei. 2024. Detection of Man-in-the-Middle Attack Through Artificial Intelligence Algorithm. In *Advances in Intelligent Manufacturing and Service System Informatics*, 2024. Springer Nature, Singapore, 450–458. https://doi.org/10.1007/978-981-99-6062-0_41

[26] Franco Tommasi, Christian Catalano, and Ivan Taurino. 2022. Browser-in-the-Middle (BitM) attack. *Int. J. Inf. Secur.* 21, 2 (April 2022), 179–189. https://doi.org/10.1007/s10207-021-00548-5

[27] Jonas Tzschoppe and Hans Löhr. 2023. Browser-in-the-Middle - Evaluation of a modern approach to phishing. In *Proceedings of the 16th European Workshop on System Security* (*EUROSEC '23*), May 08, 2023. Association for Computing Machinery, New York, NY, USA, 15–20. https://doi.org/10.1145/3578357.3589458

[28] M. Vijayalakshmi, S. Mercy Shalinie, Ming Hour Yang, and Raja Meenakshi U. 2020. Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions. *IET Networks* 9, 5 (2020), 235–246. https://doi.org/10.1049/iet-net.2020.0078

[29] Examination of Phishing Attempts on Web-Based Business Applications and Their Preventions | IEEE Conference Publication | IEEE Xplore. Retrieved October 14, 2024 from https://ieeexplore.ieee.org/abstract/document/10593139

[30] NIS04-4: Man in the Middle Intrusion Detection | IEEE Conference Publication | IEEE Xplore. Retrieved October 14, 2024 from https://ieeexplore.ieee.org/abstract/document/4150912