INTELLIGENT TECHNICAL SOLUTIONS

A COMPREHENSIVE GUIDE TO EMAIL-BASED CYBER ATTACKS

Table of Contents

I. Introduction

Despite the proliferation of new messaging apps and video chat platforms, email still remains the preferred method of communication for many people. That's because it's one of the most effective tools for businesses to communicate with customers and colleagues while requiring minimal resources.

Unfortunately, it's also one of the most likely attack vectors used by cybercriminals. In fact, the number of email-based cyber attacks has surged 464% in the first half of 2023 alone. And because of how much people use emails for business communications, that makes securing email accounts a tough challenge for IT and office managers.

Intelligent Technical Solutions (ITS) has helped hundreds of businesses secure their IT environment, including email accounts. In this eBook, we'll help you understand the threats so you can prepare against them, as well as provide you with the best ways to secure your email systems.

II. Understanding the Threat: Email-Based Cyber Attacks

Email-based cyber attacks refer to any malicious activities that exploit email systems to compromise individuals, organizations, or systems. Such attacks attempt to infiltrate a victim's device by utilizing your email as a conduit for disseminating malware, stealing confidential data, or disrupting your operations.

Some of the most common email-based cyber attacks include:

1. Phishing

Phishing is a cyber attack where cybercriminals craft seemingly legitimate emails, messages, or websites to trick recipients into divulging sensitive information, such as passwords, credit card details, or personal data. Cyber criminals will often impersonate legitimate entities like banks, businesses or government agencies as part of their deceptive strategy. They will then leverage social engineering tactics to induce a sense of urgency or fear to manipulate you into clicking malicious links that download harmful attachments or urge you to provide sensitive information.

2. Spear Phishing

Similar to phishing, but highly targeted, spear phishing is often tailored to specific individuals or organizations. Attackers research their targets to craft convincing and personalized messages that seem trustworthy, often mimicking sources the targets know. That personalization makes it much harder for you to spot the scam, increasing the likelihood that you will click on a malicious link.

3. Whaling

As opposed to phishing which targets employees, whaling aims for the top executives. It involves attackers meticulously crafting deceptive emails or messages posing as trusted contacts or entities familiar to high-profile targets like CEOs. It's a dangerous attack as it can potentially grant scammers critical company data, financial information, or confidential systems. With that level of access, the fallout can be severe, potentially leading to financial losses, reputation damage, or even broader security breaches within the organization.

4. Email Spoofing

Email spoofing is a form of cyber attack in which a scammer sends an email with a manipulated sender address that makes it seem as if it originated from a trusted source. It's a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a known sender.

RELATED: How to Protect Your Business from Email Spoofing

5. Business Email Compromise (BEC)

Business Email Compromise (BEC) is an attack that involves impersonating high-ranking company officials to trick employees into performing unauthorized money transfers or sharing sensitive information. These types of attacks have doubled over the past year—comprising nearly 60% of social engineering incidents. Furthermore, according to the FBI, BEC attacks led to $2.7 billion in losses in 2022 alone.

RELATED: 7 Tips to Prevent Business Email Compromise (BEC) Scams

6. Credential Harvesting

In credential harvesting, cybercriminals create emails that redirect recipients to fake login pages in an attempt to steal usernames and passwords when entered. They will often mimic legitimate login pages (like Microsoft Office 365) in order to trick you into typing in your login credentials. That is dangerous especially when you consider that around 65% of people reuse the same password for multiple accounts. It means that a single stolen password can potentially give access to more than one account.

7. Social Engineering

Social engineering is a manipulation technique that exploits human psychology to gain access to private information, passwords, or account numbers. These scams are built around how people think and act. Once a scammer understands what motivates your actions, they can deceive and manipulate you or members of your team more effectively.

III. Key Components of Email-Based Cybersecurity

Unfortunately, there's no single way to combat email-based attacks. It requires a multi-faceted approach that involves user education, robust security solutions and fostering a security-conscious culture within your organization.

Take a look below at some of the things you need to do to keep your email secure:

A. Email Security Best Practices

- **Employee Training and Awareness** - Training employees to recognize phishing attempts, suspicious emails, and risky behaviors significantly reduces the chances of successful attacks.

- **Patch Management** - Keeping email systems, software, and security solutions updated helps protect against known vulnerabilities.

- **Multi-Factor Authentication (MFA)** - Requiring multiple forms of verification adds an extra layer of security, making it harder for attackers to access accounts even if they obtain passwords.

- **Email Encryption** - Encrypting sensitive information in emails and using secure communication channels help safeguard data from interception or unauthorized access.

- **Implement Robust Email Security Measures** - Implementing advanced spam filters, antivirus software, and email authentication protocols (like DMARC, SPF, and DKIM) can prevent malicious emails from reaching inboxes.

B. Risk Mitigation Strategies

- **Incident Response Plans** - Establishing protocols to detect, respond to, and recover from email-based attacks is crucial. Having a well-defined incident response plan can mitigate the impact of successful breaches.

- **Regular Security Audits and Updates** - Conducting periodic audits and assessments of email systems and security measures ensures that defenses are up-to-date and effective against evolving threats.

- **Vendor and Third-Party Risk Management** - Managing vendor and third-party relationships in terms of email-based cybersecurity helps prevent potential vulnerabilities originating from external sources.

- **Data Backup and Recovery Measures** - Implementing data backup and recovery provides a safety net against data loss and cyber attacks, and ensuring quick restoration of email services in case of disruptions or security incidents.

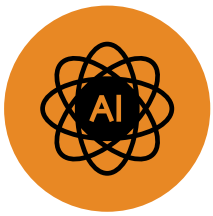
IV. The Future of Email-Based Cybersecurity

Email is here to stay. Organizations will continue using it in the foreseeable future. However, that doesn't mean that the way businesses use it will stay the same. That's why it's vital to stay up-to-date about the future of email-based threats and security. It will allow your organization to adopt a proactive and adaptive approach to cybersecurity, enhancing your resilience against evolving cyber threats.

In this section, we'll discuss:

- Emerging Email-Based Threats and Trends
- Trends and Innovations in Email Security

A. Emerging Email-Based Threats and Trends

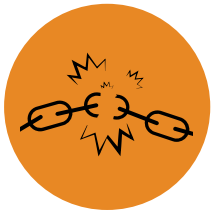


1. AI-Powered Phishing

Just as businesses are leveraging artificial intelligence for efficiency, so are cybercriminals. Many scammers are turning to AI to create more convincing and targeted phishing emails. They usually use AI to generate more highly personalized and sophisticated phishing messages that are harder to detect.

2. Deepfake Audio/Video in Emails

Some scammers can also use deepfake technology to create realistic audio or video content embedded within emails. These could trick recipients into believing they're interacting with trusted individuals or organizations, leading to more convincing social engineering attacks or spreading misinformation.



3. Supply Chain Attacks via Email

There has been an increase of scams targeting supply chains and third-party vendors through email-based attacks. Cybercriminals might exploit weaknesses in email communications between businesses and their suppliers, using spear phishing or business email compromise tactics to gain access to sensitive data.

RELATED: How a Third-Party Vendor's Ransomware Crisis Became Our Own

4. Ransomware Targeting Email Servers

Ransomware attacks targeting email servers or cloud-based email platforms have grown more sophisticated in recent years. These attacks could encrypt entire email databases, leading to significant disruptions and data loss.

5. Misuse of IoT Devices for Email Attacks

New scams are utilizing Internet of Things (IoT) devices to facilitate email-based attacks. IoT devices with email capabilities can be exploited to send malicious emails or serve as entry points into corporate networks.

B. Trends and Innovations in Email Security

1. AI-Powered Threat Detection

Using AI and machine learning can help you detect and prevent email threats in real time, making it easier to defend against sophisticated attacks. They can analyze patterns and learn from them, improving their threat detection capabilities over time.

2. Zero Trust Email Security

While the Zero Trust model isn't new, its use has extended to email security, focusing on continuous authentication and verification of users and devices accessing email systems. This approach helps prevent unauthorized access, even from compromised accounts or devices.

3. Domain-based Message Authentication, Reporting, and Conformance (DMARC) Enhancements

DMARC has gained prominence in preventing email spoofing and domain impersonation. Recent innovations in DMARC implementation and reporting tools provide better visibility and control over email authentication.

4. Cloud-Native Email Security

With the increasing migration of email services to the cloud, there's a focus on developing and enhancing cloud-native email security solutions. These solutions provide real-time threat intelligence, data loss prevention, and advanced encryption within cloud-based email platforms.

Need Help Securing Your Email?

While email remains a cornerstone for business communication, it's a prime target for cyber threats. The surge of email-based attacks in recent years highlights how urgently you need to fortify your email system's defenses. You can do that by employing the best practices we've listed above.

These practices can help you create a robust defense against multifaceted email-based threats. If you need help securing your email systems, our team at ITS have helped hundreds of businesses do the same. Find out how we can help you by scheduling a meeting with one of our experts.

Intelligent Technical Solutions
(885) 204-8823
www.itsasap.com

INTELLIGENT TECHNICAL SOLUTIONS