mimecast

PART TWO

Future-proofing your cybersecurity strategy

Defending Against PHISHING

Barraged by Phishing Fraud

This past year was the worst year on record for cybersecurity[1], and phishing was the biggest culprit. More than a third **(36%)** of all data breaches in 2021 were due, at least in part, to employee credentials stolen through a phishing attack[2], **91%** of which occur through email.[3]

Phishing occurs when an attacker masquerades as a trusted entity, duping the victim into opening a malware-laden email, instant message, or text message. The cybercriminal's aim may be to obtain credit card or other financial information, but often phishing emails are sent to seduce employees into revealing their passwords and logins so the attacker can access their company's network.

According to recent reports:

- A staggering **84% of U.S. organizations** have reported phishing or ransomware attacks in the past 12 months.[4]
- The FBI warns that phishing is the most common type of cybercrime, with publicly reported incidents nearly doubling **from 114,702 in 2019 to 241,324 in 2020**.[5]
- In 2021, phishing was the second most expensive type of cyberattack, surpassed only by business email compromise (BEC). Breaches due to phishing cost organizations an **average of $4.65 million**.[6]
- Per a 2020 study, nearly one-out-of-five employees will likely click on a phishing email link. Of those, more than two-thirds **(67.5%)** will then enter their credentials on the attacker's website.[7]

The Different Types of Phishing Ploys

Malefactors can be extremely sophisticated and use different types of phishing ploys to achieve different aims and against different targets. These include:

- **Email phishing**, which is the most common and most basic type of cyberattack. A fraudster will mimic an organization's email domain and then send out thousands of generic requests. To panic the recipient, a common tactic is to claim that one of the person's accounts has been compromised and to urge the individual to respond immediately. Or the attacker may take the opposite approach, claiming that someone has won a prize to lure the person into clicking on a malicious link. The aim in both cases is to induce the victims to provide personal information or enter their credentials on a site controlled by the hacker.

- **Spear phishing**, which is a more directed form of attack against specific people. Instead of sending out mass emails to numerous recipients, the perpetrator targets individuals within a company with high levels of network access or the authority to approve financial transactions. Such attacks are often more personalized to dupe the intended victim.

- **Whaling**, is quite similar to spear phishing but aimed against senior executives with a great deal of authority — and the tactics employed are even subtler. Emails may appear to come from a client or business partner whom the target knows and make requests for proprietary information that appear innocuous.

- **Smishing and vishing** replace email with text and telephone scams. A smisher will send out thousands of malicious text messages in the same way that a phisher will send out emails. A visher will use the phone to engage their target in a conversation. One common ploy is for the scammer to pose as a fraud investigator from a bank or credit card company. The fraudster will then ask the intended victim to provide personal information in order to verify his or her identity.

Who Gets Phished?

Some of the world's most prominent businesses have been phishing victims. These three incidents were among the most costly:

- Between 2013 and 2015, an extended phishing email campaign deceived **Facebook** and **Google** into paying more than $100 million. Both companies used the same computer supplier out of Taiwan. The phisher issued a series of fake invoices from the vendor, which both Facebook and Google paid.[8]

- **Crelan Bank**, in Belgium, was the victim of a phishing email scam that cost the company approximately $75.8 million. The perpetrator successfully compromised the account of a high-level executive and then instructed bank employees to transfer money to an account controlled by the hacker. Crelan Bank discovered the fraud during an internal audit.[9]

- **FACC**, an Austrian manufacturer of aerospace parts, was another high-profile phishing victim. Posing as the company's CEO, the phisher instructed an employee in the accounting department to send $61 million to a bank account that the fraudster controlled.

Alarmingly, these type of incidents are becoming much more common. In Mimecast's most recent State of Email Security report, more than half **(55%)** of the 1,400 information technology and cybersecurity professionals that participated in the study reported that during the past year the number of phishing attacks like those cited above rose significantly.

84% of U.S. organizations were phished in the past 12 months.

Phishing is the most common type of cyber fraud, with the number of incidents nearly doubling between 2019 and 2020, according to the FBI.

How to Thwart Phishing

Given the prevalence of phishing attacks and the degree of damage they can cause, companies have no choice but to strengthen their defenses. Here are the main vulnerabilities companies need to address and the key defensive measures they need to take:

Given the prevalence of phishing attacks and the degree of damage they can cause, companies have no choice but to strengthen their defenses. Here are the main vulnerabilities companies need to address and the key defensive measures they need to take.

Phishing attacks that rely on brand impersonation are difficult to spot but very easy for a cybercriminal to instigate. To defend against these attacks, organizations need security systems and third-party monitoring services that provide them with complete visibility into all uses of their email domains.

Most successful phishing attempts succeed due to human error. But companies can significantly reduce this risk by providing regular cybersecurity awareness training to their workforce, including instruction that teaches employees how to spot and sidestep a phishing attack.

When work from home became the norm during the COVID-19 pandemic, email usage rose dramatically and it continues to rise. The volume is now so great at most companies that it is difficult or impossible for humans to discern which emails are safe and which are malware-laden without the aid of technology. To help support their efforts to identify, block, and remediate suspicious emails, companies are well advised to incorporate the latest advances in artificial intelligence and machine learning into their cybersecurity defenses.

How Does Mimecast Defend Against Phishing?

With best-in-class email security, brand protection, and award-winning employee security awareness training, Mimecast provides the strongest possible defense against phishing:

- ***Mimecast Email Security defends against all forms of email-based threats***, including phishing attacks that rely on tactics like malicious attachments, URLs, and impersonation. Choose the best deployment option for your needs – with or without a gateway.
- ***Many phishing attacks occur through brand spoofing***. Mimecast protects your brand and safeguards against this type of attack with its innovative brand protection solution. Using machine learning to proactively find and take down phishing attacks before they cause damage, Mimecast's technology can instantly block malicious URLs or domains across email and web.
- ***Mimecast's DMARC Analyzer can protect your business' email domains from being used in a phishing attack.*** This Mimecast solution allows you to better protect your own organization and brand, as well as your customers, partners, and suppliers by providing complete visibility into and control over who is sending email on your behalf.
- ***Mimecast security awareness training was developed by leaders from the military, law enforcement and intelligence communities, and will prepare an organization's employees to detect and evade phishing threats***. Utilizing humor and other engaging techniques, Mimecast training arms your troops with an understanding of the many ways that attackers attempt to deceive them and how they can evade their attacks. For more on this, see our paper, Teaching Good Security Behaviors with Seinfeld: Overcoming the employee engagement challenge in security awareness training.
- ***As phishing attacks become ever-more deceptive, AI-based defensive measures become ever more important.*** Mimecast's AI-powered cybersecurity solutions safeguard businesses from even the most stealthy and hard-to-detect email-based threats. Mimecast's CyberGraph toolset, for example, helps detect highly evasive threats – like social engineering and malware-less attacks – by using AI and Social Graphing to map communication patterns, identify anomalies, alert employees of potentially suspicious emails with contextual warning banner and prevents data leakage by warning employees from sending emails to the incorrect recipient. This solution also removes embedded email tracks to limit attackers' ability to access information that can be used to craft highly personalized attacks.
- ***Mimecast also offers other resources that help mitigate the consequences of a successful phishing attack.*** These include an all-in-one subscription service for business continuity that enables employees to continue to send and receive email — even in the midst of a computer breach. Other services include email backup and recovery, which rapidly restores mailboxes, calendar items and contacts lost through malicious deletion or file corruption, helping to minimize downtime and ensure a swift return to normal business operations.

Conclusion:
Don't Succumb to the Barrage

Cybercriminals engage in a constant barrage of phishing attacks that rely on clever ruses to lure their targets into taking the bait. Mimecast's email security arsenal ferrets out these ploys, neutralizing them and making them easier to spot. When deployed in tandem with Mimecast's security awareness training, these solutions put employees in a much stronger position to identify and safeguard themselves from a phishing attempt.

The fight against phishing will only intensify. But the defensive measures described here will arm companies to effectively fight and defeat this threat.

[1] "Q3 First-Half Data Breach Analysis," Identity Theft Resource Center

[2] "2021 Data Breach Investigations Report," Verizon

[3] "91% of all cyber attacks begin with a phishing email to an unsuspecting victim," Deloitte

[4] "Osterman Research: How to Reduce the Risk of Phishing and Ransomware," Mimecast

[5] "Internet Crime Report 2020," FBI

[6] "How much does a data breach cost?" IBM

[7] "Gone Phishing Tournament," Terranova Security

[8] "How this scammer used phishing emails to steal over $100 million from Google and Facebook," CNBC

[9] "Belgian bank Crelan loses €70 to BEC scammers," Help Net Security

[10] "Throwback Attack: How a single whaling email cost $61 million," Industrial Cybersecurity Pulse

Work Protected.

Advanced Email & Collaboration Security

mimecast

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.