PHISHME
COFENSE
EMAIL SECURITY

Email Security in an AI-Driven World

Insights and Trends You Need to Know in 2025

INTRODUCTION

Even though email is the #1 communication tool for most businesses, it's also one of the greatest vulnerabilities in organizational cybersecurity. Each year, threat actors innovate new ways to exploit email systems, and artificial intelligence is making it easier than ever for them to create highly sophisticated and targeted attacks. Looking ahead in 2025, the stakes are higher than ever for cybersecurity professionals working to keep their organizations safe.

To help enhance your security posture, we've gathered predictions from Marc Olesen, CEO and other Cofense experts to highlight the trends shaping email security and the key vulnerabilities organizations will face in the coming year. Whether you're a seasoned professional or managing cybersecurity for your organization for the first time, these insights will help you prepare for what's ahead.

A strong email security posture built for the "Golden Age of AI" will require cybersecurity leaders to think and plan strategically to stay one step ahead of threat actors. Cofense experts have identified some of the top email security challenges organizations need to consider and prepare for to stay secure in 2025.

MARC OLESEN
Chief Executive Officer

2025: The Year of Measuring What Matters in Cybersecurity—Focusing on Human Resilience

Human risk management will take center stage, with an emphasis on measuring employee resilience through security awareness programs trained on real, current threats targeting employees' inboxes. This approach will assess how effectively employees identify and mitigate vulnerabilities, as well as how they respond to emerging threats. Employees generate valuable data that can help protect organizations from cyber risks, including their susceptibility to attacks and their ability to detect and avoid them, key factors that will be integral to measuring the success of an organization's security program.

Additionally, as threat actors continue to leverage AI for their exploits, utilizing AI to counter these efforts will become essential for organizations. While fighting AI with AI will be necessary, human resilience will remain the foundation of cybersecurity. By continuously assessing and improving how humans interact with security systems, organizations can ensure they are prepared for evolving threats and empowered to effectively defend against them.

WHAT CAN YOU DO TO PREPARE?

- **Enhance Security Awareness Programs with Real-World Threats:** Develop comprehensive training programs that simulate real, current threats targeting your employees. Regularly assess your employees' ability to identify and respond to email security threats. Use these insights to measure resilience and adapt strategies to strengthen your organization's human defenses against cyber risks.
- **Leverage AI and Strengthen Human Resilience:** Incorporate AI-driven tools to detect and mitigate email security threats. Complement these technologies with continuous evaluation and improvement of how employees interact with security systems, ensuring human resilience remains the core of your cybersecurity strategy.

JOSH BARTOLOMIE
VP, Global Threat Service

The cybersecurity industry's lack of focus will be its main vulnerability in 2025.

Despite the increasing sophistication of threats and record profits, many businesses are still cutting costs in cybersecurity. While there have been advancements, the focus generally remains on short-term cost-cutting objectives and profit expansion. This is a dangerous trend, especially cyber threats continue to escalate in both volume and impact. Boardroom conversations about cybersecurity have been ongoing for years, yet the industry remains fixated on "shiny" new technologies. We need to return to the basics and address the fundamental issues that continue to plague our defenses.

WHAT CAN YOU DO TO PREPARE?

- **Refocus on Cybersecurity Fundamentals:** Prioritize addressing core issues such as employee training and baseline threat detection, instead of chasing flashy technologies that may overlook critical vulnerabilities.
- **Commit to Long-Term Investment in Security:** Shift from short-term cost-cutting measures to sustainable strategies that strengthen foundational defenses and ensure resilience against evolving threats.

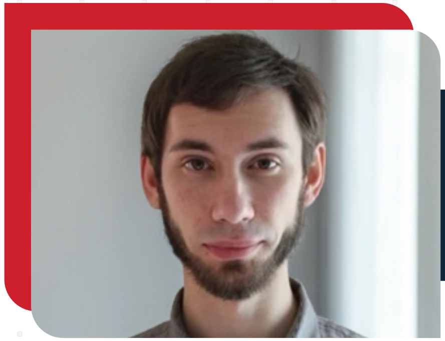
JOSH BARTOLOMIE
VP, Global Threat Service

Data analysts will be in high demand in the coming years and key to developing cybersecurity strategies.

Data analysts with a deep understanding of cybersecurity will be in high demand in the coming years. As businesses grapple with increasing cyber threats and the need to protect sensitive data, skilled professionals who can analyze and interpret security data will be invaluable. A "unicorn" in this field would possess not only strong data management and correlation analysis skills, but also a comprehensive understanding of cybersecurity principles, threat vectors, and mitigation techniques. This combination of technical expertise and cybersecurity knowledge will enable data analysts to identify vulnerabilities, detect threats, correlate potential risks, and help provide the insight that will help drive data-driven and significantly more effective and impactful security strategies.

WHAT CAN YOU DO TO PREPARE?

- **Upskill in Data Analysis and Cybersecurity:** Encourage professionals to gain expertise in both data management and cybersecurity through targeted training programs, certifications, and hands-on experience with threat detection and mitigation tools.
- **Integrate Data-Driven Practices into Security Strategies:** Adopt frameworks that utilize data analytics to identify vulnerabilities, assess risks, and enhance decision-making to create more effective and proactive cybersecurity measures.



MAX GANNON

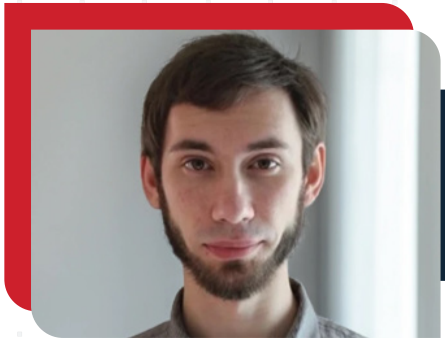
Manager, Intelligence Analysis

AI-powered phishing campaigns will become more convincing at a larger scale.

AI-powered phishing campaigns will become increasingly sophisticated and tailored on a wider scale. While speed has been a primary benefit of AI in phishing campaigns, the rapid advancement of AI technology suggests we can expect to see even more sophisticated campaigns in the coming year that include convincing logos, names, and context.

WHAT CAN YOU DO TO PREPARE?

- **Leverage AI for Advanced Threat Detection:** Implement AI-driven security solutions that can identify and respond to the subtle patterns of AI-powered phishing attacks in real-time, enhancing overall defense capabilities.
- **Conduct Regular Employee Training:** Equip users with the knowledge to recognize highly convincing phishing attempts through ongoing education using real and relevant threats, focusing on identifying suspicious emails, links, and requests for sensitive information.



MAX GANNON
Manager, Intelligence Analysis

Threat actors will increasingly leverage social platforms to spread malware and steal personal data.

We can expect generic credential phishing campaigns to decrease, and threat actors may shift their focus to using legitimate links to social platforms like TikTok and Meta more frequently. We have recently observed phishing attempts leveraging popular social media platforms, such as YouTube or Facebook, to spread malicious links. In the coming year, we can anticipate threat actors increasing their use of this tactic, exploiting user trust in these platforms.

WHAT CAN YOU DO TO PREPARE?

- **Enhance User Education on Social Media Threats:** Conduct regular training to raise awareness about malicious links, phishing tactics, and the risks of trusting unsolicited messages or content on social platforms.
- **Strengthen Security Measures for Social Media Use:** Implement advanced security tools, such as URL filtering and multi-factor authentication, while closely monitoring interactions on social platforms to detect and block suspicious activities.

CHANCE CALDWELL
Sr. Director, Phishing Defense Center

In the coming year, the growing trend of offshoring security teams is set to significantly undermine organizations' cybersecurity.

The loss of in-house expertise will create critical gaps in understanding and addressing security risks, while outsourced teams may face communication and coordination challenges, leading to delays and missed vulnerabilities. Offshoring may also weaken oversight, reduce the customization of security practices, and create compliance issues.

While short-term cost savings may appear attractive, the long-term consequences, such as heightened exposure to cyberattacks, third-party breaches, and a misalignment between security and business objectives, are likely to outweigh the immediate financial benefits.

WHAT CAN YOU DO TO PREPARE?

- **Maintain a Core In-House Security Team:** Retain critical cybersecurity expertise internally to ensure thorough understanding of organizational risks, enable rapid response to threats, and provide oversight for outsourced teams.
- **Establish Strong Collaboration and Oversight:** Develop clear communication protocols, regular coordination practices, and accountability measures for offshored teams to ensure alignment with business goals and effective handling of security operations.

CHANCE CALDWELL
Sr. Director, Phishing Defense Center

Healthcare will remain a target for threat actors with teaching hospitals being especially susceptible.

Given the high-profile healthcare breaches in recent years, healthcare remains a prime target for cyberattacks. Teaching hospitals, with their frequent turnover of temporary staff, are particularly vulnerable. These temporary employees may not prioritize security as much as permanent staff, creating significant vulnerabilities for these institutions. These vulnerabilities can be likened to technical debt, where neglecting security best practices can accumulate over time, leading to more significant risks and potential breaches.

WHAT CAN YOU DO TO PREPARE?

- **Implement Rigorous Access Controls:** Use role-based access measures and regularly update permissions to ensure temporary staff only have access to the information needed for their duties, reducing exposure to sensitive data.
- **Provide Continuous Security Training:** Conduct mandatory, recurring security training tailored to both permanent and temporary staff to instill best practices and minimize risks linked to human error.

CONCLUSION

The predictions outlined by our experts make one thing clear—2025 will not only see the evolution of cyber threats but also the transformation of cybersecurity roles and practices. From AI-driven phishing campaigns to changing organizational structures, the risks businesses face are growing more complex and sophisticated.

To stay ahead, cybersecurity professionals must remain vigilant, focusing on both emerging technologies and tried-and-true fundamentals. The insights in this ebook aim to guide your approach, ensuring your security strategies are proactive, adaptable, and robust.

About Cofense

Cofense® provides the world's most effective business email threat detection and remediation solutions. The Cofense PhishMe® Email Security Awareness Training (SAT) Platform with Risk Validation and the Cofense Phishing Threat Detection and Response (PDR) Platform are powered by over 35 million Cofense-trained employees who report phishing and other dangerous email threats in real time. Exclusive to Cofense, our network detects and eradicates threats other email security systems miss and removes them from our customers' inboxes. For more information, visit cofense.com or connect with Cofense on X and LinkedIn.

PHISHME® COFENSE EMAIL SECURITY