Abnormal

CISO Guide to Phishing

How to Stop 74% of All Advanced Attacks

/ By Mike Britton

The Rising Threat of Phishing Attacks

Phishing is the most common advanced email threat that organizations face, accounting for 74% of attacks seen by Abnormal in 2023. Phishing emails can lure victims into trusting the sender with their login credentials, other sensitive information, and even company funds. Successful phishing campaigns can also lead to business email compromise (BEC)—one of the most costly cybercrimes.

Perhaps due to its versatility as the first step in a variety of crimes, phishing far outpaces other types of attacks. The FBI's Internet Crime Complaint Center (IC3) documented 298,878 phishing incidents in 2023—five times as many as the second most common cybercrime.

Because phishing emails target human behavior, create a sense of urgency, and appear to come from trusted senders, stopping them before they reach employee inboxes is the key to staying safe. Secure email gateways can stop simple phishing attacks that contain obviously malicious links or attachments. But more sophisticated phishing messages often sail through, putting organizations at risk for credential theft, business email compromise, financial losses, data breaches, and ransomware attacks—all of which can have costly consequences for the business.

$417M

Total losses attributable to phishing attacks since 2019

FBI IC3 Internet Crime Report

Types of Email Phishing Attacks

Phishing comes in many forms and can be used for various goals depending on the attacker and the target. Some examples are harvesting credentials for account takeover, capturing sensitive internal information for resale or espionage, diverting funds to attackers' accounts, and infecting computers or networks with ransomware. The common thread among all types of phishing is a message that tricks victims into taking the bait.

Credential Phishing

The simplest, widest-scale phishing campaigns dupe users into entering their login credentials and personal information for banks, email clients, employer networks, social networks, and other sensitive accounts. For example, a phishing campaign designed to harvest Microsoft 365 passwords might include a link to a malicious website that looks like the Outlook login portal but captures credentials as victims key them in.

Spear Phishing

Spear phishing criminals research and target specific employees within an organization, often in payroll and accounting. These emails often appear to come from other employees who want to switch their direct deposit to a new bank account or from vendors asking the recipient to log in to fix a problem. Spear phishing emails may include malicious links or rely on written instructions, such as for payroll changes. They can come from spoofed emails outside the organization but are especially difficult to catch when they come from compromised accounts.

Whaling or CEO Fraud

Named for the biggest "phish," whaling attacks impersonate the target company's CEO or another executive. These emails pressure specific employees—again, typically in accounting or payroll—to immediately pay a fake invoice, share protected information, or even buy gift cards for a "last-minute event" and give them the card numbers.

It's worth noting that phishing attacks can be executed in a variety of ways, and phishing tactics are always evolving. These attacks can be part of large-scale credential harvesting or account takeover schemes that can have dire consequences for organizations and their executives, employees, customers, and investors. And while email is the most popular delivery mechanism, phishing also occurs over text (smishing) and the phone (vishing) as cybercriminals constantly innovate.

How Phishing Works

Phishing attacks use social engineering—a predatory blend of identity deception, manipulation of trust, and deadline pressure—to push email recipients to take actions they wouldn't do if a stranger made the request.

Impersonation of Trusted People and Brands

The initial phishing email may seem to come from the victim's boss, a company executive, a known vendor, or a trusted brand. If the attackers have taken over a company email account or exploited website vulnerabilities to send emails from a trusted domain, the phishing message may look entirely credible—even upon closer inspection.

Abuse of Trusted Relationships

By hiding behind a trusted persona—a boss or brand, for example—phishing emails can make requests that would otherwise raise red flags right away. For example, a common phishing scheme targets employees with a fake email from their CFO, claiming to need them to pay an invoice immediately to avoid a deal falling apart. The email might direct the victim to a fake payment website or simply give them the account and routing numbers to use. While an employee wouldn't take this action for a stranger, they may do so for a high-powered financial executive.

Pressure on Recipients to Act

Phishing attackers know they have to keep recipients from spending too long evaluating their requests, so they turn up the pressure. For example, the CFO needs that invoice paid within an hour, before a big meeting. Few employees want to let the CFO down, so they may act instead of flagging the email for review. The result? Drained funds and a place on the "suckers list" for future attacks from that same threat actor.

Because most phishing emails are carefully researched and well-designed, it can sometimes be difficult for employees to see them for what they are, even with security awareness training. For that reason, the safest approach is to make sure these messages never reach employees' inboxes.

#1

Cybercrime by attack volume for the past five consecutive years

FBI IC3 Internet Crime Report

Impact of Phishing Attacks

The FBI Internet Crime Complaint Center actively tracks successful phishing incidents and their financial impact. In 2023, there were a reported 298,878 successful phishing attacks. Phishing has been the most common type of cybercrime since 2019, leading to victim losses of more than $417 million over the past five years.

Of all attacks stopped by Abnormal, 74% of them are classified as credential phishing, most of which can be used to launch more advanced attacks from compromised email accounts. And even if the cybercriminal isn't that sophisticated, the fact that they have credentials means they can do as they please within the account, and perhaps access additional (potentially more valuable) services if those same credentials are used across multiple sites.

11x

Increase in successful phishing attacks since 2018

FBI IC3 Internet Crime Report

$417M

Total losses attributable to phishing attacks since 2019

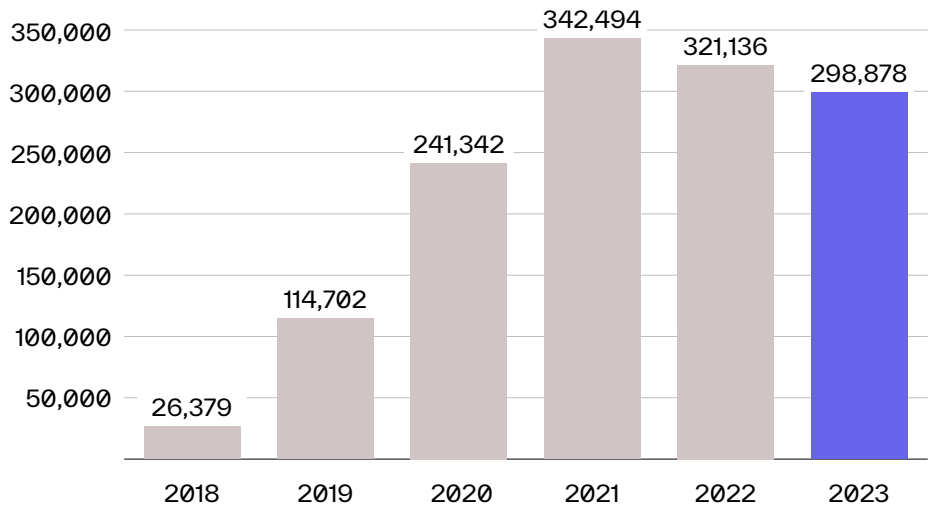
FBI IC3 Internet Crime Report

74%

of all advanced attacks are credential phishing attempts

Abnormal Security

Number of Phishing Attacks Reported to FBI IC3



Abnormal

Why Phishing Attacks Are Successful

While the number of successful phishing attacks reported to the FBI IC3 has somewhat plateaued recently, it's important to consider that the volume of this attack has skyrocketed just in the past five years.

In 2018, the FBI IC3 documented only 26,379 phishing incidents. In 2023, that number jumped to 298,878—11 times the 2018 figure. That massive growth is evidence of how effective phishing is at getting victims to do what email attackers want.

Phishing attacks will likely continue to grow in number, not only because they work but also because legacy solutions are increasingly ineffective against advanced socially engineered threats.

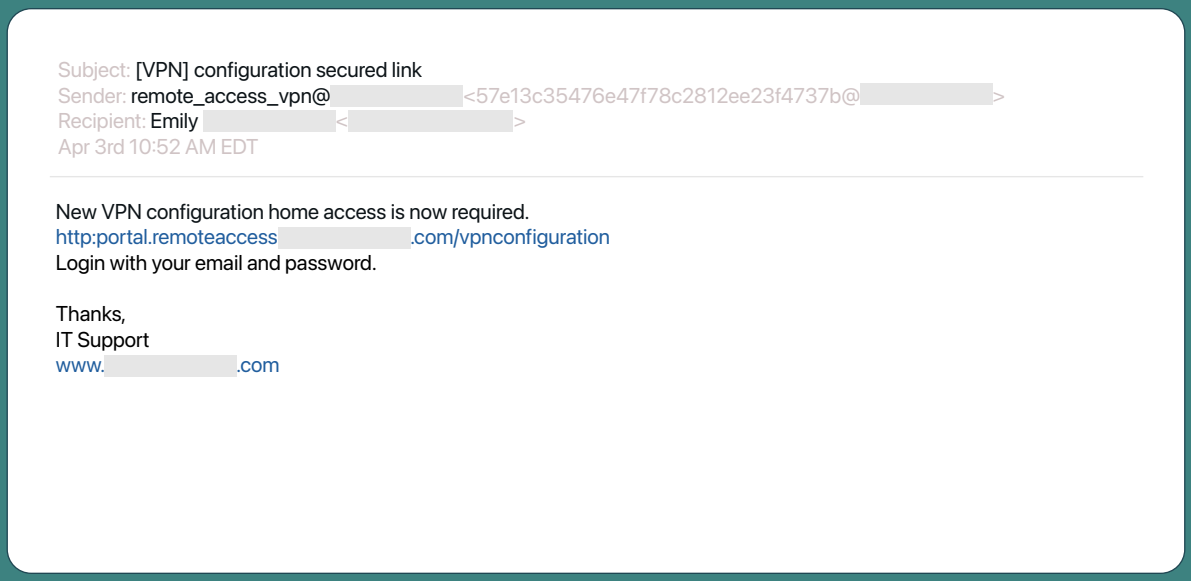
Today's Phishing Attacks Are Designed to Bypass SEGs

Secure email gateways look for known bad or indicators of compromise, like a bad sender reputation, suspicious links, and malicious attachments. But phishing messages are increasingly sophisticated, leveraging trusted identities, detailed text instructions, and deadline pressure to compel recipients to complete actions they would otherwise probably not do.

Security Awareness Training Is One Layer in Comprehensive Email Security

Security awareness training aims to teach employees to spot clues that indicate risky emails so they don't click on malicious links or attachments or rush to make suspicious transactions. However, phishing clues are harder than ever for people to identify. This is especially true for people who are working quickly under time pressure and who may trust that the realistic-looking message in their inbox is safe. That's why it's critical to back up security awareness training with technology that reduces the number of emails employees have to assess or report.

If you look at a real-world example of a phishing attack that bypassed the secure email gateway, you can see why traditional defenses fail.



Subject: [VPN] configuration secured link
Sender: remote_access_vpn@ <57e13c35476e47f78c2812ee23f4737b@ >
Recipient: Emily <>
Apr 3rd 10:52 AM EDT

New VPN configuration home access is now required.
http:portal.remoteaccess .com/vpnconfiguration
Login with your email and password.

Thanks,
IT Support
www. .com

A quick scan of this message might not raise flags for remote worker Emily. The email comes from her employer's domain, but the disparity between the sender's identity and the actual email address indicates domain hijacking or spoofing. The URL provided is also formatted incorrectly, raising more flags. If Emily doesn't look closely and clicks on the link and logs in, the site will collect her credentials. The attackers can then compromise her account and gain access to her employer's VPN, putting the company at risk of a data breach or ransomware attack.

This kind of attack is hard to identify with traditional email defenses and has a high potential to slip by humans—especially in the middle of a busy workday. The best defense is to stop these carefully crafted attacks before they reach your employees.

How to Stop Phishing Attacks

To counter increasingly sophisticated phishing attacks, large enterprise organizations need the right email security platform. The next generation of email security includes:

API Architecture

A solution that connects to Microsoft 365 and Google Workspace via an API and, in doing so, provides access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more.

Behavioral Data Science Approach

The solution should use a fundamentally different approach that leverages behavioral data science to profile and baseline good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that include suspicious attachments or links, or unusual download requests.

Organizational Insights

The solution should understand both formal and informal organizational hierarchies. It should map internal as well as cross-organizational relationships to understand typical communication patterns and behavior, and then detect, log, and remediate all email threats.

Without each of these capabilities, phishing attacks will continue to be delivered through email, outpacing security measures and making it more difficult to prevent these attacks from reaching employees. When they do, they can cause financial losses and lead to data breaches—neither of which a CISO wants to endure.

Conclusion

It's clear that phishing-related risks will continue to increase, as data from both the FBI IC3 and Abnormal shows it's the most common type of cybercrime.

Unfortunately, there doesn't seem to be a ceiling on phishing growth, as criminals find new ways to leverage email to phish for victims. For example, QR code attacks, the newest iteration of phishing, are a type of social engineering attack in which a threat actor attempts to trick a target into interacting with a malicious QR code. The QR code is linked to what appears to be a legitimate website with a prompt to enter login credentials or other sensitive details. Unfortunately, any information provided can then be used by the perpetrator to compromise the target's account and launch additional attacks.

Stopping phishing emails requires a solution that can detect and interpret thousands of signals to block the emails that appear suspicious, even when they don't contain traditional indicators of compromise. Unlike legacy email security tools, an API-based security solution uses AI-native detection engines to ingest, analyze, and cross-correlate behavioral signals to spot anomalies in email patterns that indicate a potential attack. It then automatically remediates malicious emails to prevent end-user engagement. Implementing modern email security technology that pairs advanced behavioral science with risk-adaptive detection is the only surefire way to safeguard your organization from advanced attacks.

/ Mike Britton

CISO, Abnormal Security

Mike Britton is the CISO of Abnormal Security, where he leads information security and privacy programs. Prior to Abnormal, Mike spent six years as the CSO and Chief Privacy Officer for Alliance Data. He brings 25 years of information security, privacy, compliance, and IT experience from a variety of Fortune 500 global companies. He holds an MBA with a concentration in Information Assurance from the University of Dallas.

Abnormal

Abnormal Security is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, Salesforce, ServiceNow, Zoom, Amazon Web Services and multiple other cloud applications.

Ready to Stop Phishing Attacks?

Request a Demo →

See Your ROI →