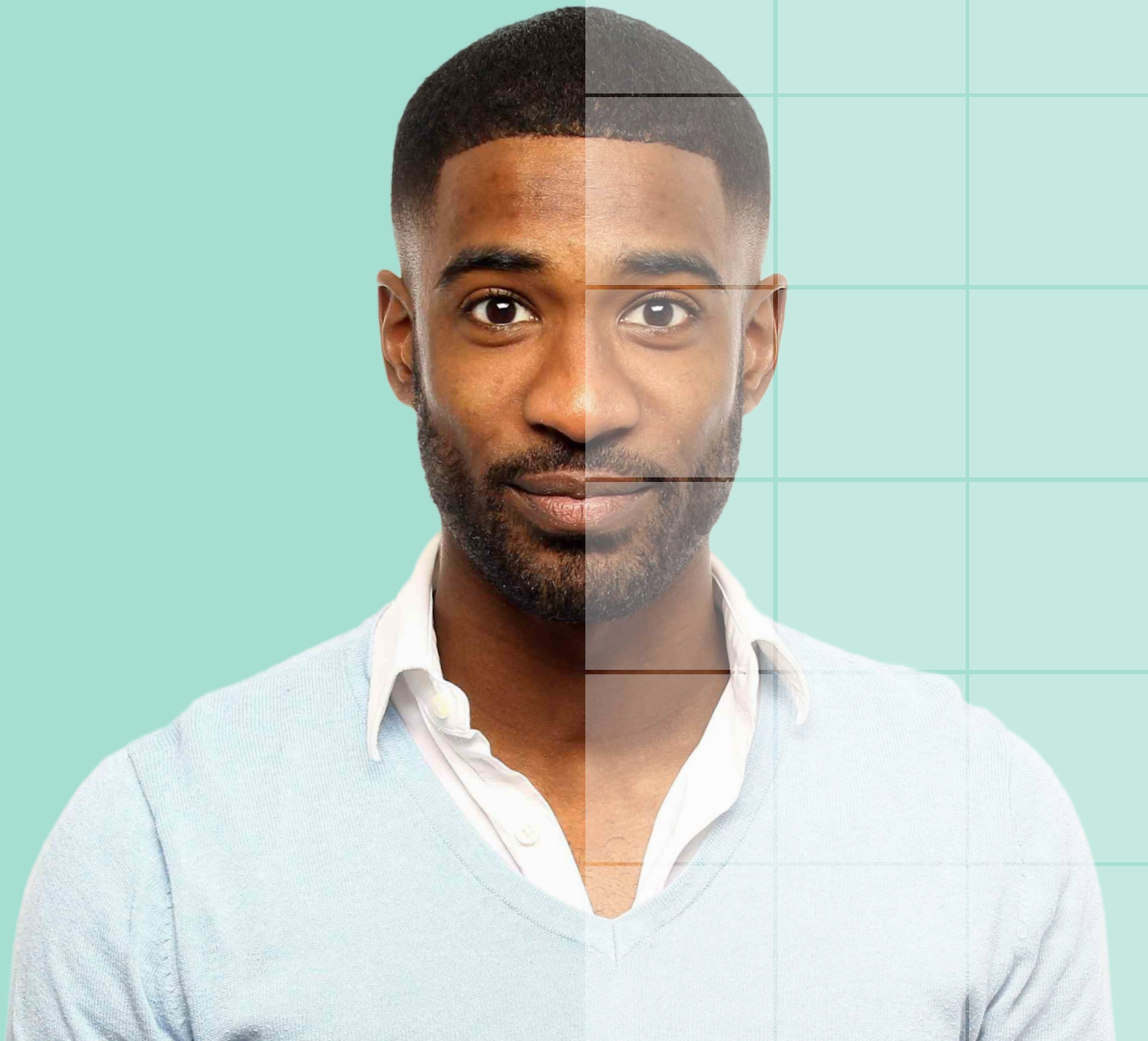
Abnormal

CISO Guide to Phishing

How to Stop 77% 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 nearly 77% of attacks seen by Abnormal in 2021. 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), and Deloitte reports that phishing is the number one delivery vehicle for ransomware.

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 323,972 organizational and individual phishing victims in 2021, nearly four 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.

$44M

$44 million lost to phishing attacks in 2021.

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 three consecutive years.

FBI IC3 Internet Crime Report 2021

Impact of Phishing Attacks

The FBI Internet Crime Complaint Center actively tracks successful phishing incidents and their financial impact. In 2021, successful phishing attacks increased by 34.2%, rising from 241,342 in 2020 to 323,972 in 2021. Phishing has been the most common type of cybercrime since 2019, leading to victim losses of more than $44 million in 2021 alone.

Of all attacks stopped by Abnormal, 77% 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.

34.2%

increase in successful phishing attacks since 2020.

FBI IC3 Internet Crime Report 2021

20

average number of phishing attacks received each week per 1,000 mailboxes.

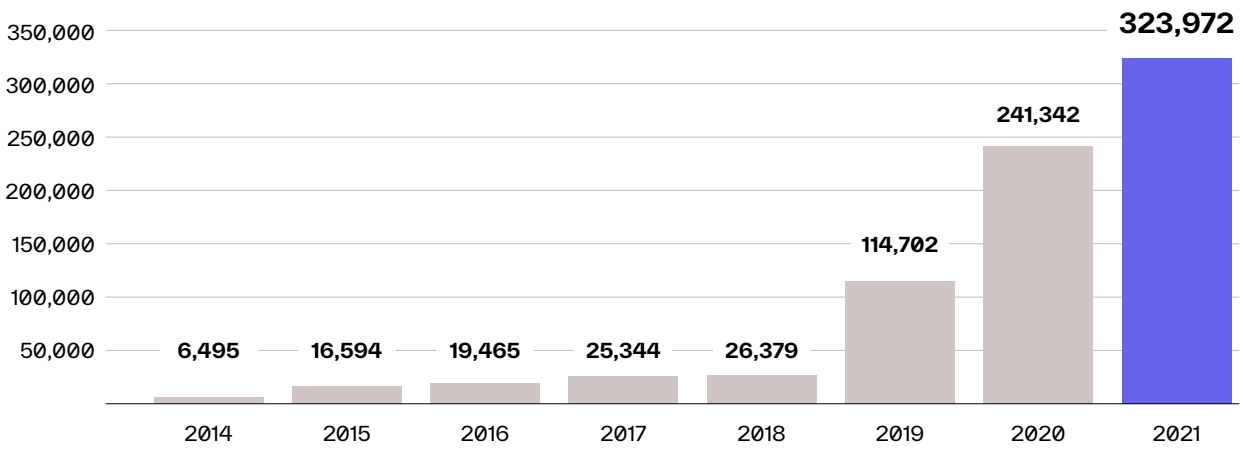
Abnormal Security

77%

of all advanced attacks are credential phishing attempts.

Abnormal Security

FBI's Reported Complaints of Phishing/Vishing/Smishing Attacks



Abnormal™

Why Phishing Attacks Are Successful

The number of successful phishing attacks has exploded by 1,178% since 2017, when the FBI IC3 documented just 25,344 such incidents. 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.

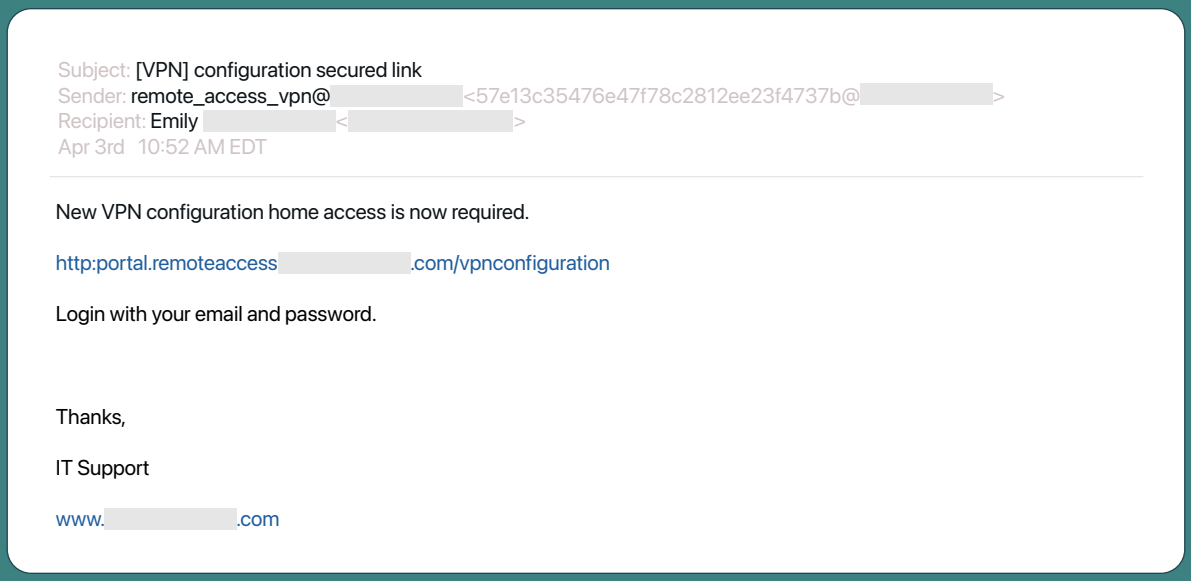
Today's Phishing Attacks Are Designed to Bypass SEGs

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 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.

Abnormal™

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-based 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 are increasing, as successful attacks jumped 34% over the past year. The increase is unsurprising, considering that phishing comprised more than three-quarters of all attacks seen by Abnormal in 2021.

Unfortunately, there doesn't seem to be a ceiling on phishing growth, as criminals find new ways to leverage email to phish for victims. One trend Abnormal is monitoring closely is phone fraud attacks that start with a phishing email impersonating a brand, urging the victim to call a number to solve a problem. In Q3 2021, 31.4% of organizations were hit with email-initiated phone fraud attacks, and the rate leaped to 59.2% in December 2021.

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. It's only by stopping these attacks from reaching inboxes that we can truly protect our organizations from phishing and other email-based 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

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Interested in Stopping Phishing Attacks?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@abnormalsec