White Paper

Ultimate Guide to Email Security

IRONSCALES
SAFER TOGETHER

A Brief History of Email Phishing

As the email phishing threat landscape continues to rapidly evolve, understanding the totality of the email security and anti-phishing universe can be difficult for even the savviest of enterprise buyers. That's because for many years, organizations believed that they could adequately reduce cyber risk by simply deploying Secure mail gateway (SEG) technology along with anti-spam filters and basic employee security awareness training.

Up until 2014 or so, this sentiment was more accurate than not. But then the landscape started to change. Phishing transformed into spear-phishing, followed closely by the introduction of malware and ransomware into the mainstream. The emergence of social engineering, including Business Email Compromise (BEC), added additional complexity, now overburdening both human and gateway controls.

In response to the rising threats, email security solutions and anti-phishing tools began to evolve. Legacy signature-based tools built on YARA rules began to have their value propositions challenged by smart, self-learning technology built on artificial intelligence (AI), machine learning (ML) and automated incident response. This new generation of email security technology promised to accelerate the time from incident discovery to organization-wide remediation.

This convergence of more frequent and sophisticated phishing threats with more advanced cybersecurity solutions and services significantly increased the complexity of the anti-phishing ecosystem, making it increasingly difficult for security specialists to quantify and qualify email risks and emerging solutions versus legacy controls.

Contents

The 10 Most Common Tactics Deployed To Defeat Email Security Controls

In an attempt to declutter the ambiguity around domain vernacular and to bring clarity to the buying process, we've developed this whitepaper to help readers better understand and make sense of the tactics, techniques, standards, protocols, technology and solutions that comprise the email phishing threat landscape.

To begin, here are the ten most common phishing tactics:

Account takeover

Most commonly deployed by financially motivated attackers, account takeover occurs when an adversary obtains - either through legal or illegal actions - a person's legitimate login credentials to a website, server or application, enabling them to commit various types of financial fraud.

Advanced Persistent Threat (APT)

An APT refers to a sophisticated hacker, cybercrime outfit or nation state exploiting multiple threat vectors, including email, for both reconnaissance and exploitation purposes. The method is commonly used as a means to gain unauthorized access to networks, servers or devices.

Credential Harvesting

A highly common phishing tactic where attackers will attempt to lure a recipient into entering their password or other compromising log-in information, usually via a web page. This is most often deployed via spear phishing.

Financial Fraud

Similar to credential harvesting, except that instead of trying to get someone to enter their password, the attacker's goal is to get the recipient of the phishing email to enter compromising info that can later be used to steal money. This can include bank account information, credit card numbers, social security numbers and more.

Malware

Otherwise known as malicious coded software, malware is commonly deployed via email and is used to disrupt or destroy networks, servers and devices. Examples of malware include Trojan horses, spyware, adware and viruses.

Phishing

Delivered via phone, text, email or social media, phishing is the oldest yet most prominent tactic in which criminals attempt to trick an unsuspecting recipient into taking an action, such as wiring money. It is estimated that phishing accounts for nearly 90% of all cyberattacks worldwide.

Ransomware

An increasingly popular malware strain, ransomware encrypts the victim's data and then demands a sum of money (to be paid in bitcoin) in order to receive the decryption key. The criminal typically makes a threat to release the victim's data to the internet and/or dark web if payment isn't made. The Justice Department reports more than 4,000 ransomware attacks per day in the U.S. alone.

Social Engineering

Growing in popularity, social engineering occurs when an attacker uses psychological manipulation to trick a person or company into taking an action, such as providing login credentials, paying a fraudulent invoice or sharing personally identifiable information (PII), such as a social security number. According to Verizon, social engineering now occurs in almost 60% of phishing attacks.

Spam

These junk and unsolicited email messages have historically been more annoying than risky. However, spam is increasingly viewed as a cybersecurity threat due to inattentional blindness, which occurs when individuals fail to perceive an unexpected change in plain sight.

Spear-phishing

The main difference between phishing and spear-phishing is that spear-phishing targets specific people and/or organizations with an ask to complete a specific task, such as downloading an attachment or clicking on a link, while phishing is often distributed at random to widespread audiences. Oftentimes, engaging with the payload enables adversaries to access the information needed to institute a major cyberattack.

Let's switch gears a bit and explain the difference between an email phishing tactic and an email phishing technique as we see it. In truth, tactics and techniques are often talked about interchangeably, as the distinction between them is small and rather unimportant most of the time. But for the purposes of this analysis, we consider techniques as extensions or variations of a tactic.

For example, business email compromise (which we will talk more about later in this article) is ultimately a spear-phishing technique. BEC attacks fit within the definition of spear-phishing, but have distinctive elements, such as the absence of a malicious payload, that make it unalike from what is commonly recognized as a traditional spear-phishing attack.

While the number of phishing tactics can be counted on both hands, the number of phishing techniques is quite vast, and growing on a regular basis. That's because attackers are always seeking out new methods to defeat both human and technical anti-phishing controls. This game of cat and mouse has been ongoing for nearly two decades, and adversaries' relative success in bypassing email security protocols suggests that the evolution of phishing techniques is here to stay.

The 13 Most Common Email Phishing Techniques

Business Email Compromise (BEC)

One of the most common and successful types of cybercrime, BEC attacks leverage socially engineered messages as a means to commit financial fraud. The goal is to trick email recipients into taking an action, such as wiring money, paying a bill or providing confidential credentials that can then be exploited for financial gain. Since BEC attacks typically do not leverage malicious URLs or malware attachments, they easily bypass signature-based prevention mechanisms, such as secure email gateways, and human controls. BEC attacks cost organizations nearly $1.8 billion in 2019, according to the FBI.

Domain Phishing

A type of spoofing email in which an attacker sends a malicious message from a fraudulent domain that is an exact match to the spoofed brand's domain (Example: TimCook@apple.com). These messages are detectable by many anti-phishing technologies since the sender domain can be easily identified as false.

Extortion

Extortion phishing scams leverage scare tactics, including blackmail, threats or coercion, to intimidate victims into paying a ransom or providing them with a specific service. These types of scams, which are increasing in frequency, often threaten to spread sensitive information such as private photos and videos (whether or not the attackers actually have this compromising info).

Fake login pages

These nefarious, yet often highly realistic looking website pages, are an increasingly common technique deployed by attackers seeking to obtain a person's login credentials to a legitimate website in order to harvest personal or company information and commence with illegal activity, such as credit card fraud, identity theft and more. Adversaries are able to bypass both human and technical controls by exploiting inattentional blindness. Last year we identified more than 200 major brands significantly impacted by fake login pages in the first half of the year.

Hidden Text/Zero font

This technique implements hidden text with a font size of zero within a phishing email. Since a human reader cannot detect the zero-width characters, these malicious emails often appear legitimate to unsuspecting users. Invisible characters are also capable of bypassing legacy email security defenses, which is why the best way to defend against this type of attack is to turn to AI-powered email security tools that use natural language processing and computer vision to detect anomalies.

Impersonation

A type of spoofing attack, with or without a payload, in which adversaries take on the persona of a colleague, vendor, partner, friend or family member in order to achieve a specific objective. Such attacks can be used for quick financial gains, or deployed as part of an advanced persistent threat (APT) in which reconnaissance is the main objective.

Polymorphism

This phishing technique occurs when a malicious actor implements slight but significant changes to an email's artifacts, such as its content, copy, subject line, sender name or template in conjunction with or after an initial attack has deployed. This strategic approach enables attackers to quickly develop phishing attacks that trick signature-based email security tools that were not built to recognize such modifications to threats. With the ease associated with the development and delivery of polymorphic attacks, it is no surprise that 42% of all phishing attacks are polymorphic.

Smishing

Delivered via SMS, smishing text messages are phishing attack techniques containing malicious URLs that attempt to lure recipients into visiting risky websites, downloading malware onto their mobile devices or sharing login credentials. These text messages can sometimes appear to be from trusted senders, such as banks and online retailers, making them a real threat to people who are only accustomed to look for phishing attempts via email attacks.

Spoofing

Email spoofing occurs when an attacker sends a malicious message with false sender address in an effort to steal personal information, infect computers with malware or leverage extortion to steal money. There are four primary types of spoofing attacks, including exact sender name impersonations (the most common), similar sender name impersonations, look alike/cousin domain spoofing and exact domain spoofs.

Typosquatting

Also known as URL hijacking, typosquatting preys on inattentional blindness by leveraging small deviations in domain names to lure them into visiting malicious websites. These deviations include scrambled letters, wrong domain endings and other typographical errors that can easily lure victims to fake websites and fake login pages. Once lured, typosquatters have an easy opportunity to harvest personal and financial information to make quick money.

Unicode Domain Phishing

As a result of the internationalization of the World Wide Web and the rise of internationalized domain names (IDNs), cybercriminals have the opportunity to exploit Unicode domains to make dangerous websites appear as safe and authentic. Unicode domain phishing replaces characters in the domain with similar characters from a foreign language, allowing the fraudulent website to bypass web browser protections and legacy email security tools.

Vishing

This type of phishing attack technique tricks victims into giving up sensitive personal information over the phone, such as credit card numbers and passwords. By relying on social engineering to prey on human emotions such as greed or fear, unsuspecting victims can easily be duped into giving attackers exactly what they're looking for. The FBI has reported that the vishing technique is increasing with great frequency.

Whaling/VIP Impersonation

Directed at senior executives at mostly large corporations, Whaling/VIP Impersonation attacks are targeted spear-phishing campaigns aimed at tricking high-level executives and organizational leaders into sharing confidential or proprietary information that can be used for financial fraud and other forms of exploitation. According to our research, VIP impersonations penetrate SEGs about 20% of the time.

Phishing Techniques Add To The Complexity of Email Security

If we revisit this whitepaper 12-18 months from now, it's likely that we would be able to add another 2-3 trending techniques to the list, if not more. The reality is that phishing remains the number one driver of cyberattacks and so, as defenses ramp up, cybercriminals are already scheming their next moves.

Email authentication isn't only about protecting the integrity of messaging. Rather, it is about how brands can ensure deliverability with bulk email distribution. But as phishing and spam have evolved from an occasional annoyance to a never-ending threat, email authentication has emerged as a popular means of reducing the risk of malicious messages.

There is a common misunderstanding though as to how much of a role authentication protocols and standards play in email security. While some vendors and email clients will have you believe that compliance will significantly reduce risk, the truth is that these safeguards represent just a small piece of the ever-growing anti-phishing puzzle.

The Opportunity Cost of Email Authentication

It's important to know that each standard and protocol was designed to solve one very specific problem. As such, these technical defenses often struggle against mitigating complex phishing attacks, especially those not spoofing domains. Further, many are difficult to implement and require intensive and costly maintenance over time.

Nonetheless, email authentication standards and protocols can be helpful as a part of a robust email security strategy. Here's a list that every security analyst and IT professional be aware of:

Brand Indicators for Message Identification (BIMI)

As the newest and least utilized email authentication standard, BIMI intends to reduce fraudulent brand spoofing emails by visualizing a logo as a measure of authenticity. Compliance requires DMARC configuration with active "quarantine" or "reject" policies, a positive sender reputation and a BIMI Assertion Record.

Domain Keys Identified Mail (DKIM)

This is an email security standard that uses cryptography to ensure that messages aren't manipulated between sender and receiver. DKIM helps improve email deliverability rates, while also reducing the frequency of domain spoofing. Learn how to setup DKIM here.

Sender Policy Framework (SPF)

This is a policy that protects against domain spoofing by hardening DNS servers and restricting access to senders. SPF enables Internet Service Providers (ISPs) to verify that a mail server is authorized to send an email from a specific domain. Learn how to setup SPF here.

Simple Mail Transfer Protocol (SMTP)

The purpose of SMTP is to help organizations send and receive emails. While helpful for deliverability, this protocol remains highly vulnerable because it does not encrypt or authenticate messages.

Domain Message Authentication Reporting & Conformance Protocol (DMARC)

At a high level, the Domain Message Authentication Reporting & Conformance (DMARC) protocol is a way to determine email authenticity and empowers senders to determine the fate of an email should the email fail SPF and/or DKIM verification. As such, DMARC helps reduce risk associated with only one very specific type of spoofing: domain spoofing.

While DMARC has been around for over a decade, it boomed in popularity in recent years thanks to vendor promotions and public sector adoption. While overall usage is trending upwards, only about 20% of the Fortune 500 have implemented this protocol.

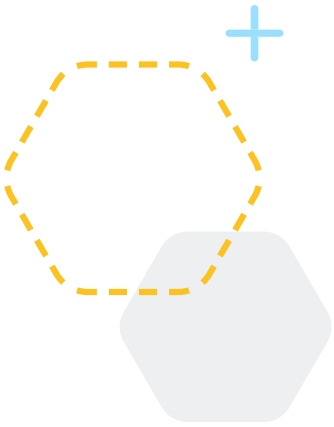
In 2018, the Department of Homeland Security threw DMARC into the mainstream when it mandated that the entire agency become compliant. This direction, while well-intended, inadvertently gave off the perception that DMARC solved more email security challenges than it actually does.

In response to the mandate, we wrote an op-ed in NextGov about how DMARC was not the email security silver bullet that so many were making it out to be. Here's an excerpt from our article, Attention Federal Agencies: DMARC is Not a Silver Bullet for Email Security:

DMARC was first launched in 2012 to better detect and prevent email spoofing. It is built on the DomainKeys Identified Mail and Sender Policy Framework and offers linkage to the sender's domain name, reporting, and policies on how to handle authentication failures. When implemented by both sender and receiver, DMARC can help foil domain spoofing and enables organizations to filter out and reduce the number of fraudulent emails.

For DMARC to work as intended, both the sender and the receiver need to implement it correctly. But even if they have, exact domain spoofing attacks can exploit vulnerabilities in email clients to mislead end users on the validity of a message. In a direct spoofing attack, an adversary can exploit a vulnerability in a web browser or in a code to change the return path details. Mailsploit, one of the latest and most dangerous phishing techniques, can easily render DMARC obsolete by exploiting how mail servers handle text data differently than operating systems. In other words, government agencies could remain at risk of exact domain spoofing whether or not they have implemented DMARC appropriately.

Even when it is effective, DMARC can be cumbersome. It often leaves some organizations accidentally rejecting legitimate messages, and it can also break a company's mail flow by creating a backlog of messages. DMARC is also very complicated to configure with many cloud-based solutions and can require significant maintenance beyond authorization.



DMARC, like the other email authentication protocols and standards, is only effective for solving one particular challenge. But therein lies the problem: such technical controls are only meant to solve specific problems.

We have reached the point where security teams and IT leaders are spending far too much time analyzing and responding to phishing threats, and part of that is due to an over-reliance on point solutions (which is essentially what email standards and protocols are).

So now that we better understand the robust and ever-shifting email security threat landscape, one question remains: how can you protect your organization?

A Comprehensive Guide to Anti-Phishing Solutions

Anti-phishing behavioral conditioning (APBC)

A specific type of anti-phishing employee training with the goal of educating employees about common types of phishing threats and reducing the number of incidents where an employee takes the bait left out by a threat actor.

Common Vulnerabilities and Exposures (CVE)

A list of security vulnerabilities and exposures records allowing companies to better classify, identify and organize phishing threats with the goal of accelerated remediation.

Content Disarm & Reconstruction (CDR)

A computer security technology that removes malware from code. It is commonly offered as part of a larger email security solution as a bolt-on focused on cloud-based email endpoints.

Cloud Email Security Supplement (CESS)

This type of solution first gained mainstream attention as a result of Gartner's 2019 Market Guide for Email Security. CESS solutions target a very narrow subset of advanced threats, unlike Integrated Email Security Solution (IESS) vendors (see below for more).

Data Leak Prevention (DLP)

A capability of some email security solutions that prevents sensitive information or data from leaving an organization via email. This is a common add-on service offered by email providers such as Microsoft.

Extended Detection and Response (XDR)

Similar to SIEM, XDR solutions aggregate data across endpoints, including antivirus, firewall, and more. Security analysts leverage XDR to provide a full picture of an organization's threat landscape, which, of course, includes email.

Indicator of Compromise (IoC)

IoC-focused email defenses are commonly found in SEGs, which rely on technology to identify phishing threats that contain a malicious payload (URL, attachment). However, this technology is ineffective in remediating the rise of social engineering attacks.

Integrated Email Security Solution (IESS)

This is where many modern email security solutions sit, including IRONSCALES. While the efficacy and integrated advanced technologies vary, most email security companies claim to offer robust advanced threat capabilities to prevent all types of phishing techniques that would normally breach Secure Email Gateways.

Email Security Orchestration, Automation and Response (M-SOAR)

This solution is commonly deployed by email security companies, including IRONSCALES, with end-to-end security to identify and remediate threats while continuously learning to better improve the process.

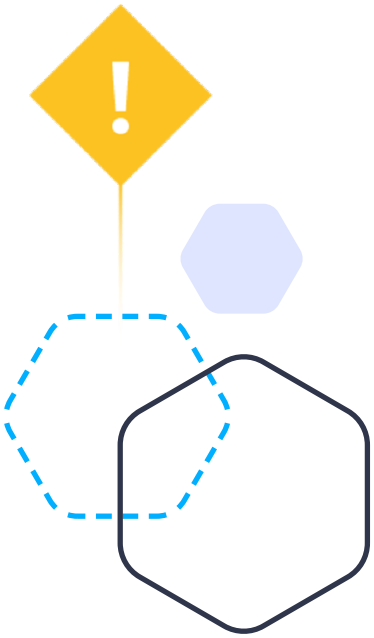
Phishing Button

This is a common feature found across many email security products. The button empowers users who receive a suspicious email to quickly click "spam alert" or "phishing" so that the email is then routed to a phishing mailbox for further investigation.

Phishing Mailbox/Spam Mailbox/Abuse Mailbox

These terms often get used interchangeably but the distinctions are important.

- Phishing Mailboxes: these mailboxes received user/employee-reported email threats.



- Spam Mailbox: these mailboxes are commonly found in most email clients as “spam” folders where junk and/or spam email is automatically routed.
- Abuse Mailbox: these mailboxes are where emails are automatically sent in organizations that have M-SOAR solutions (i.e. suspicious emails are automatically quarantined here rather than requiring any action by users).

Phishing Simulation and Training

While phishing training is a commonplace solution, many businesses are not investing in the use of advanced phishing protection education to help employees identify and mitigate more complex threats like socially engineered attacks and business email compromise (BEC).

Sandbox

An extremely common solution for a variety of technologies used by engineers and other users can safely test new technologies before they are widely deployed into production. However, sandboxes differ in email security, referring to the isolation of a suspicious URL or attachment in a phishing email. This is particularly useful for zero-day attacks that bypass existing technical defenses.

Secure Email Gateway (SEG)

Some of the most commonly deployed email security solutions, SEGs as identified by Gartner, “provide basic message transfer agent functions; inbound filtering of spam, phishing, malicious and marketing emails; and outbound data loss prevention (DLP) and email encryption.” So what is the problem with SEGs? IRONSCALES research shows advanced phishing attacks bypass leading SEGs at a nearly 50% clip.

Security Information and Event Management (SIEM)

Email security solutions often integrate with SIEM tools. The email security tools send logs to the SIEM, which then consolidates logs from all connected security technologies, analyzes the data and then generates alerts for analysis and reporting. Some IRONSCALES SIEM integrations include Micro Focus ArcSight, IBM QRadar and Splunk.

Breaking Down The Advanced Technology That Powers Modern Email Security

The lifeblood of the solutions described above is the advanced technology that powers the software and keeps organizations secure. While almost every company will claim to use "advanced technologies", it is important to understand the basic mechanics of what these technologies entail to discern when companies are full of hot air.

For example, SEGs may claim to use AI and machine learning, but without emerging technologies to automatically understand both the content and intent ("what") of suspicious messages, and at the same time validating sender identity and domain authenticity ("who"), they're unable to stop the rise of social engineering threats.

Artificial Intelligence (AI)

Big picture, AI utilizes machine learning algorithms to conduct tasks in smart ways. When many people are asked to define AI, there's a wide range of reactions from fully autonomous futuristic humanoid robots seen in movies to smart technologies like Alexa, Siri and Roombas. For the purposes of this blog, AI enables decisions to be made on trending and zero-day phishing attacks without human intervention. In fact, it's the basis of how we founded the IRONSCALES self-learning email security platform.

Computer Vision

An advanced technology that helps to prevent credential harvesting and PII leaks by looking at visual deviations from the norm common with fake web pages. By comparing the visual similarity of legitimate landing pages to spoofed ones, computer vision provides a critical additional layer of defense since they do not rely on simple pattern matching technologies.

Machine Learning

Fundamentally, machine learning is the ability for machines to become smarter through experience. Machine learning makes AI possible and uses algorithms to query vast amounts of data, discover patterns and generate insights. In email security, machine learning can automate the task of phishing attack discovery via scanning messages and other proprietary analytics.

Natural Language Understanding (NLU)

An emerging advanced technology used in many technology sectors. In email security, it leverages advanced machine learning and neural networks to automatically detect and respond to the most common types of BEC attacks. Importantly, NLU is what allows IRONSCALES to understand both the "what" and the "who" of suspicious messages.

Now that you've had time to read, absorb and better understand the email security landscape, you're probably wondering how and where IRONSCALES fits in. Schedule a free demo today to learn how we use a combination of email security solutions and advanced technology to protect organizations around the world from phishing threats.

To learn more about how to get started please request a demo today at https://ironscales.com/get-a-demo/

IRONSCALES
SAFER TOGETHER

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

To learn more, please visit **www.ironscales.com** today!