FORTRA

WHITEPAPER (Email Security)

A Window on Email Security

Protecting Your Business From Hidden Email Threats

Cybercriminals frequently employ email as a means of launching attacks. Email is widely used and trusted in the workplace, increasing the likelihood that your message will reach its intended recipient. Phishing and other email-based attacks are simple to execute, can be deployed at scale, and can yield substantial benefits to the attacker.

Email Phishing Is Here To Stay

Phishing and Business Email Compromise (BEC) scams remain the primary attack vectors used to gain access to organizations, frequently providing the foothold needed by threat actors to wreak havoc on businesses and their customers despite billions of dollars being invested in perimeter and endpoint security over the past two years. The losses from phishing and other forms of sophisticated email fraud in 2021 alone totaled over $44 million[1].

The volume of phishing and email spoofing attacks doubled in 2021[2]. Malicious data breaches are caused by stolen credentials rather than the installation of malware, and the average number of BEC attempts received in 2020 increased dramatically by 15% between Q2 and Q3[3].

IBM found that in 2021, lost or stolen credentials accounted for 19% of malicious data breach infiltrations, while phishing attacks accounted for 16%[4]. According to information gathered by Atlas VPN, Google has identified 2.02 million phishing websites since the beginning of 2020[5]. In 2020, Google found an average of 46,000 new phishing websites every week, as reported in the company's Transparency Report[6].

Lack of Phishing Awareness

Although phishing is a serious problem for modern enterprises, over 20% of companies only provide phishing awareness training once a year[7]. To a significant extent, this ignorance is to blame for the fact that phishing is still the most common form of cyberattack that leads to stolen information. Nearly 20% of all employees are likely to click on phishing email links, and of those, an astounding 67.5% go on to enter their credentials on a phishing website, as shown by data from Fortra's Terranova Security's 2020 Gone Phishing Tournament. That indicates that nearly one in seven workers (13.4%) are susceptible to giving up their passwords on a malicious phishing site.

Insider Threats Are Possible

A shocking 34% of business owners stated that employee "collusion" was involved in the fraudulent actions, according to research from the accountancy firm BDO[8]. Roughly half of the scams revealed by respondents originated from external sources. What's more alarming is that 21% believe one of their own employees is responsible for the scam.

Technology Defenses Against Email Spoofing

These reasons highlight the importance of email security in an organization's overall cybersecurity plan. Fortunately, technological defenses against spoofing, such as Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Brand Indicators for Message Identification (BIMI), are free and widely available. By adopting them, you may greatly increase the safety of your company's outgoing and receiving email communications.

Considering how effective email-based exploits are, criminals are unlikely to stop using them anytime soon. Companies may only safeguard themselves against the email threat if they implement extensive, tailored email security.

Types of Email Risk

There are many different threats to email security, all closely related to social engineering techniques. One of the reasons social engineering is so effective is that it will manipulate our emotions to cloud our judgment. How we process information is crucial.

The field of behavioral economics postulates that people have two distinct processing speeds: fast and slow[9]. When we take our time processing information, we become calm, deliberate, and logical in our decisions. Cybercriminals would prefer we not think in this way. While we are still vulnerable, emotional, and easily manipulated, they want to test our ability to think fast under pressure. So, fraudsters use psychological tricks to get us to open suspicious emails, download malicious attachments, and reveal confidential information.

Some of the most common email attacks leveraging social engineering include:

Business Email Compromise

BEC is a scam in which the recipient is tricked into responding to an email appearing to be originated by an executive at the company. Email compromise in business is a widespread and increasing threat to companies of all sizes and in all sectors around the world.

The potential losses from BEC scams to businesses are in the billions of dollars. Social engineering is a primary tactic used by BEC fraudsters to deceive unwary personnel. Many times, they will pose as the CEO or another high-ranking executive to conduct wire transfers. Fraudsters also do extensive background checks on, and surveillance of, the businesses and individuals they hope to defraud.

According to the FBI, there are 5 types of BEC scams[10]:

1. With the "Supplier Swindle" scam, fraudsters pose as legitimate businesses asking for money to be wired to their account by posing as the suppliers sending the invoices.
2. "CEO fraud" occurs when scammers send an email to the company's finance department pretending to be the CEO or another high-ranking executive and asking them to wire funds to an account they control.
3. The email account of a company's CEO or employee is hijacked and then used to send payment requests to the suppliers who are saved as contacts in the compromised account. Following this, funds are wired to fictitious financial institutions.
4. The term "Attorney Check Scam" refers to attacks in which the perpetrator poses as a lawyer or a member of the legal firm who is in charge of sensitive and vital topics. Emails or phone calls made at the end of the business day tend to be fraudulent.
5. Employees in the human resources and accounting departments are often the targets of data theft attempts to gain access to confidential information such as tax returns or other sensitive financial documents belonging to other employees or executives. Such information is useful for planning future operations.

Spear Phishing

Spear phishing refers to a form of phishing that is designed to trick certain people or departments into giving over sensitive information. A particularly dangerous form of phishing, this fraudulent practice of communicating with victims via electronic means (email, social media, instant messaging, etc.) is an advanced tactic employed to obtain sensitive information or to coerce them into taking some action that will compromise a network, steal data, or otherwise cause monetary harm. While traditional phishing techniques may include sending out bulk emails to a wide range of potential victims, spear phishing is more targeted and requires much preparation.

An email with a malicious attachment is a common component in spear phishing campaigns. The recipient's name and position in the firm are among the details included in highly personalized emails to increase the chances of opening the email and downloading the infected attachment.

Account Takeover (ATO)

Account Takeover is when an unauthorized third party obtains a user's login information and takes over their online account. Cybercriminals can compromise a company by impersonating employees and making unauthorized changes to accounts, sending phishing emails, stealing sensitive data, or moving laterally within the corporate network. As a result, it is crucial that groups like IT, HR, and management understand the threats they face in their respective roles.

Cybercriminals also routinely use deceptive emails to persuade online account holders to enter usernames, passwords, and other sensitive data into phishing websites. With this information, scammers can access real customer accounts and commit fraud.

Spam

Even though many people have heard the term "spam," everyone has their own unique understanding of what it means. In the eyes of some, spam is any form of advertising communication that was not specifically requested by the recipient. This type of email can be quite bothersome and intrusive, so legal businesses should never send it unless the recipient has explicitly requested to receive it. It's important to note that this particular form of spam is completely safe.

But spam sent with ill intent can be devastating. Spyware and ransomware are two prevalent forms of this spam. This is becoming increasingly sophisticated and can have far-reaching consequences for businesses.

Advance-fee scams, which bear similarities to the "Nigerian Prince" email scams, are still very common types of fraud, although people are now more suspicious and knowledgeable in spotting and reporting them. At the same time, more realistic and sophisticated (and therefore dangerous) emails attempt to get recipients to click on a link and damage or hijack that user's system.

The Four Goals of Email Security

When we are discussing email security, one important factor to consider is what we are trying to achieve by protecting corporate email.

Keep your organization **safe**

Defend your employees' inboxes

Ensure your data is **protected**

Safeguard your brand's reputation

1. Keep the Organization Safe

At a high level, email security solutions give you the ability to keep the organization safe from external threats like malware, spam, or increasingly sophisticated ransomware and spyware attacks coming into the organization.

There is also a lot of focus from organizations on stopping phishing attacks coming into the business as well. However, the difficulty is that when you look at those types of attacks, there is no malicious content in the message. It is literally just some words where somebody is trying to socially engineer, for example, the finance department, into paying a false invoice into the attacker's bank accounts.

2. Ensure Data Is Protected

Email security solutions also can look at both the outbound and the internal data flows and ensure data is protected. Using integrated data loss prevention (DLP) controls, organizations can make sure that only the right people get access to sensitive data, or they can automatically encrypt this data to keep it secure while in transit.

3. Defend Employees' Inboxes

The crucial part of protecting data flows is to defend your employees' inboxes by having in place flexible policies that will enable frictionless data exchange without placing unnecessary barriers on day-to-day communications. This is important if you want to avoid any pushbacks because of security controls that harm employee experience and business productivity.

4. Safeguard Brand Reputation

Criminals are launching email phishing campaigns because they are trying to lure the customers of an organization, like a bank, into voluntarily giving their login credentials or clicking a link, or opening a file because it looks like it is coming from a trusted source.

Besides the obvious implications of violating regulatory compliance, more and more organizations understand the impact a phishing campaign has on their brand reputation. If an organization is being used aggressively by social engineers, then people will be less likely to interact with legitimate messages, and engagement rates will start going down.

Making Sense of Email Security Risks: The Johari Window of Email Security

Johari's Window is a notion developed in 1955 by two American psychologists named Joseph Luft and Harrington Ingham and has been widely employed by analysts in the United States intelligence community[11].

Johari's Window popularized the concept of known knowns, known unknowns, and unknown unknowns and was adopted by the U.S. intelligence services to identify blind spots in what we know and don't know when analyzing data.

It can also be used in identifying the risks pertinent to email security, as shown in the image below.

	Known to you	Not known to you
Known to others	Known email security risks	Blind spots
Not known to others	Hidden email security risks	The unknown factor

The Four Quadrants of Email Security

Let us delve into these four quadrants and understand what the real email security risks are.

Known Email Security Risks

As more and more companies move their infrastructure to the cloud, using native email systems becomes the norm for official communications. Protecting against common email threats like phishing, dangerous links, and infected attachments is a breeze with Microsoft 365 and Gmail's built-in email security features.

However, it is important to understand that the built-in security features are not sufficient to mitigate the sophisticated email security threats modern organizations face today – the known unknowns. For instance, third-party research has found that Microsoft Office 365 isn't very good at preventing phishing emails. Further, Office 365 cloud-based enterprise email has its own unique challenges that cannot be addressed by using standalone third-party point solutions for on-premises email.

Hidden Email Security Risks

While Microsoft 365 and Google will provide you the protection you need from everyday email security risks, they leave certain gaps exposing businesses to emerging email security threats. Even if these tools can protect against 80% of known attacks and risks, there is still another 20% of "hidden" risks that can cripple your infrastructure. For example, targeted ransomware and spyware attacks can bypass traditional defenses and wreak havoc within your organization.

Using an email security solution like Fortra's Clearswift can close these gaps. Clearswift's Deep Content Inspection goes further with scanning content in a multi-stage process far exceeding any other structural level of verification on the market. Through sandboxing, you can detect otherwise hidden mechanisms that can infect your system. Not only can you detect zero-hour threats that could initiate an attack, but you can also mitigate these threats.

With optical character recognition, you can even uncover malicious files that seem legitimate on the surface and sanitize them. Moreover, through anti-steganography, Clearswift can remove data hidden in images whether they are images coming into or out of the organization.

In addition, the solution can remove links to malicious websites hidden in the email body or in the attachments. Finally, you can redact sensitive data from your documents, such as account numbers or national insurance numbers, to be compliant with privacy and security regulations.

All these can be done without placing any barrier to legitimate business communication, in a less intrusive manner on the day-to-day operations, and without any delay.

Blind Spots

Besides the hidden risks, there are also email risks that are blind spots. These are sophisticated phishing attacks where the message looks perfectly legitimate. They use the exact wording that the finance department or the HR team sees and reads every single day. However, they are crafted in such a way as to trick your employees into voluntarily disclosing sensitive information about the organization or even sharing their access credentials.

These types of messages require a different use of threat intelligence and insight. This is where solutions like Fortra's Agari can become helpful. Agari can look at more advanced forms of phishing and social engineering that may not get picked up elsewhere. It can also secure outbound email content, protecting your employees from inadvertently causing problems to business clients, partners, and brand reputation.

Agari uses the most advanced ML and AI techniques to model the patterns of legitimate communication and content to preemptively detect untrusted email communications and automatically keep them out of the employees' inboxes. Agari leverages threat intelligence from various sources to enforce corporate policies and build defenses around the employees' communications.

The Unknown Factor

Despite all the defenses we build around corporate mailboxes, new email threats and social engineering tactics emerge every day. This is where empowering your employees is essential to form a provisional line of defense. An organization's end users can be the strongest ally and spot abnormalities using human intelligence.

What you need is a training and awareness-raising solution that integrates with your technology in place. Terranova is your strongest ally. Terranova offers you a library of training material that you can use to create customized courses for your employees. The solution integrates with your corporate directory, whether this is on-premises or in the cloud, and generates both generic training content (i.e., GDPR requirements) and role-specific material, for example, for the finance department, to help them identify financial fraud emails.

The modularity of Terranova allows you to build an awareness program that is both digestible and comprehensive. For example, you can supplement annual training events with bite-size monthly modules targeted on a specific topic to empower your people without getting in the way of their daily tasks. What is more, you can also easily create simulated phishing attacks using predefined templates to help them become more effective at spotting malicious content.

Generating Insight for Strong Protection

If actionable threat intelligence were not used as a framework, all these technological instruments would be useless. Brand misuse, account takeover, social media frauds, data leakage, and advanced email attacks are just some of the many online risks that can compromise a company's most valuable digital assets and information.

Fortra's PhishLabs analyzes and continuously monitors vast amounts of data from the open and dark web, client feeds, social media, mobile devices, and emails to produce actionable intelligence. Combining cutting-edge automatic analysis with human curation, we can eliminate irrelevant data and reliably identify threats. By feeding this compiled knowledge into Fortra's Clearswift, Agari, and Terranova, your company may lessen its vulnerability to email attacks without increasing the effort of its security personnel.

Final Thoughts

Microsoft 365 and other providers may help protect users' inboxes from spam and malware, but they fall short when it comes to supplying the robust data loss prevention capabilities and threat intel that are now essential for businesses of every size. This may discourage businesses from really contemplating a Microsoft 365 implementation, but the limits can be addressed with the help of an enterprise-strength solution.

Fortra offers a wide range of granular email security tools that can help you keep your organization safe, protect your employees' mailboxes, and safeguard your brand reputation.

TAKE ASSESSMENT

Sources

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[2] https://glockapps.com/blog/email-spoofing/
[3] https://info.abnormalsecurity.com/rs/231-IDP-139/images/AS_Qtrly_BEC_Report_Q3_2020.pdf
[4] https://www.ibm.com/reports/data-breach
[5] https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/?sh=66f129bf1662
[6] https://transparencyreport.google.com/
[7] https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/
[8] https://www.bdo.co.uk/en-gb/rethink/business-issues/strategy-operations/has-covid-19-made-your-business-more-vulnerable-to-corporate-fraud
[9] https://www.youtube.com/watch?v=YN6pijC-Kec
[10] https://www.ic3.gov/media/2015/150122.aspx
[11] https://www.communicationtheory.org/the-johari-window-model/

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.