GreatHorn

January 2023

2023 STATE OF EMAIL SECURITY:

KEY TRENDS AND INSIGHTS FROM 2022

INTRODUCTION

For the past five years, the GreatHorn Threat Intelligence team has been surveying thousands of information security professionals across various businesses and industries who manage email security within their organizations. This survey allowed us to gather new insights and research into new and emerging email security threat vectors.

For this 2023 report, the GreatHorn Threat Intelligence Team has shifted from surveying and benchmarking data to focusing on perceptions by email security professionals and aggregated real-world data seen in today's Microsoft and Google email environments. This report provides those insights into new threats and risk vectors being delivered to organizations via email – bypassing the native controls within Google and Microsoft. In 2022, the GreatHorn Threat Intelligence Team analyzed billions of emails, aggregating and anonymizing the data to provide primary trends and key emerging threats. The data was analyzed between January 1, 2022 through December 31, 2022.

KEY TRENDS AND LESSONS LEARNED IN 2022

The cyber landscape continued to be treacherous in 2022. Attacks using email not only remained common but became more sophisticated. The following are key trends and lessons learned from 2022.

Emails has never been secure. Now the attacks are much more targeted	On average, 0.21%, or 1 out of every 500 emails, has anomalous characteristics that bypass both native email security systems and secure email gateways (SEGs).
Phishing attacks are moving in the direction of quality over quantity	Spear phishing increased 127% between Q1 2022 and Q4 2022, using highly targeted and personalized attacks to a specific recipient.
Brand impersonations that result in Business Email Compromise (BEC) remains a perennial favorite	Within 2022, 43% of emails carrying potential risk each month are brand impersonation attacks.
Attackers are focusing on ways to increase both effectiveness and impact	Executive impersonations saw a 344% increase between Q1 2022 and Q3 2022 representing 6.7% of all risk associated with emails.
Personal email use in business continues to complicate both compliance and security	The use of personal email addresses within organizations represents 1.2% of all emails received, increasing the attack surface for attackers and the security risks for organizations.
Attachment-based attacks may be the new SPAM	Microsoft and Google have both improved their attachment scanning, resulting in a dramatic decline in attachment-based attacks reaching users.
URL-based attacks using compromised domains evade detection	Of the Top 20 malicious links analyzed in 2022, by quantity, 100% were compromised domains with positive reputation scores to bypass native scanning controls.
The use of file sharing links by bad actors is increasing risk to organizations	File sharing links via storage.googlesapis.com, storage.cloud.google.com, docs.google.com or page.link had the greatest quantity of potentially malicious links at 38%.

With an onslaught of new cyberattacks and cybercrime concerns at an all-time high, organizations are increasingly trying to limit exposure to risk. Key takeaways from our 2022 data continue to validate the sentiment from the 2021 report that revealed email was the leading security concern for security and IT professionals. Email security remains a leading cause of organizational breaches, with email-based attacks providing an effective way to trick employees inside a company to provide unauthorized access to corporate systems or to perform illegitimate action(s), such as financial fraud.

82% **of breaches involved the human element**

The Verizon 2022 Data Breach Investigations Report states that, "[t]he human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike."

These breaches have the potential to compromise organizational integrity, result in financial loss, and/or trigger disruption well beyond the initial intrusion. The Verizon 2022 Data Breach Investigations Report validates the multiplicative effect of a single email attack, "...one key supply chain incident can lead to wide-ranging consequences. Compromising the right partner is a force multiplier for threat actors."

True dollar cost estimates as provided by the US Federal Bureau Investigations illustrate that in 2021, the cost of nearly 20,000 Business Email Compromise (BEC)/Email Account Compromise (EAC) complaints had adjusted losses at nearly $2.4 billion.

Further analysis of cost and frequency produced by IBM Security in the Cost of a Data Breach Report 2022 demonstrates that security threats exist across multiple attack vectors.

Recognizing this, organizations are seeking to address potential security risks ahead of them landing in a user's inbox. And, because no detection technology is 100% accurate, if there is a threat in the user's inbox, how to prevent them from taking action and interacting with the email.

HOW AT-RISK IS YOUR ORGANIZATION?

For nearly every organization, email is at the heart of their internal and external communication. Our 2022 analysis reveals that 1 out of 500 or 0.21% of emails possess characteristics that make them suspicious or potentially malicious. Using an extremely conservative estimate of 1 million monthly emails being received by an organization, this translates to over 2000 messages per month that have the potential to be nefarious.

The impact can be significant.

"An estimated **40%** of ransomware attacks start through email."

- Gartner

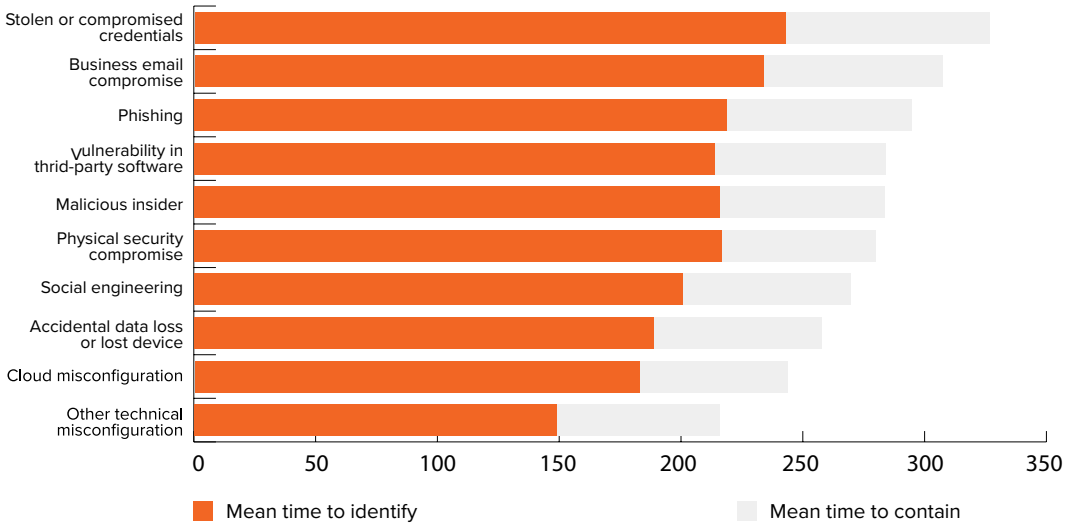
0.21% **suspicious or potentially malicious emails**

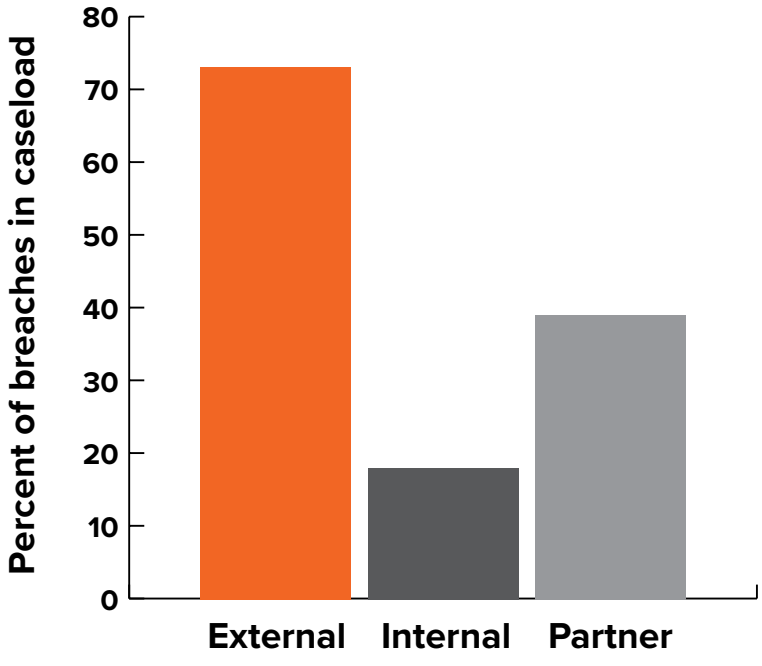
Our 2022 analysis reveals that 1 out of 500 or 0.21% of emails possess characteristics that make them suspicious or potentially malicious.

The threat assessment from the Verizon 2022 Data Breach Investigations Report reveals that nearly 75% of all data breaches come from outside of an organization, contributing to the significant need for organizations to invest in additional analysis, detection and application of security layers to protect against potentially malicious emails. Yet, as these threats frequently evade native email platform detection by simulating trusted or internal sources, as the emails reach user's inboxes, there is a greater risk of employees engaging with them.

Average time to identify and contain a data breach by initial attack vector

The time spent on data breach, as demonstrated by IBM.





Detection has evolved to incorporate sophisticated techniques such as natural language understanding and processing and image recognition. These capabilities include assessments for anomalous characteristics surrounding atypical data structures and their associated semantics.

Significant Numbers of Potentially Malicious Emails are Being Delivered to Inboxes...

Increases in the use of sophisticated, targeted attacks are revealing that using static analysis in email security techniques cannot be relied on as the sole detection methodology. These detection methodologies that use 'known bad' analysis to examine source code for common threats offer limited effectiveness at achieving the level of risk analysis required in 2022 and beyond. **Attacks are extending well outside the scope of these limited strategies, with a broad range of risks identifiable.**

... Despite Effective Out of Box Controls from Cloud Email Providers

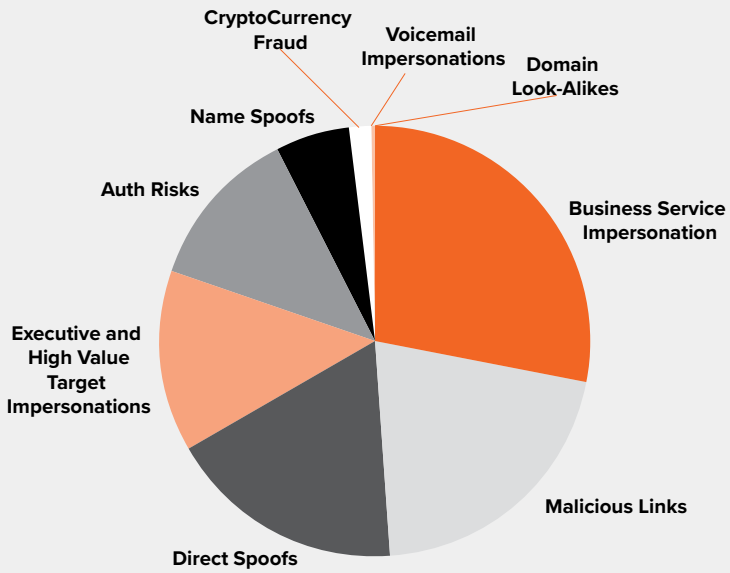
There was a continued movement away from secure email gateways in 2022, with organizations increasingly utilizing built-in protection from cloud-native email providers. Gartner estimated that by 2023, **at least 40% of all organizations will use built-in protection capabilities from cloud email providers rather than a secure email gateway (SEG), up from 27% in 2020.**

Our data concludes that this movement is attributed to cloud-native platform providers doing an excellent job with out-of-the-box capabilities. As a result, our 2022 data reveals that the total emails protected using native email controls account for ~43% of all emails that get delivered into an organization's environment.

Types of key, out-of-the-box protection include:

- Blocking emails from known bad senders
- Scanning attachments with AV
- Blocking emails with known bad URLs
- Content analysis to identify SPAM

Out of the Box Risk Types Identified



Source: https://www.greathorn.com/blog/native-seg-ices-what-you-need-to-know-about-email-security/

~43% **total emails protected**

Our 2022 data reveals that the total emails protected using native email controls account for ~43% of all emails that get delivered into an organization's environment.

Attacks Succeed Even for Security-Conscious Organizations

Despite increasing attention and security budgets, email attacks continued to succeed in 2022. In large part, this is attributed to a movement away from traditional broad-based attacks to a targeted approach involving social engineering. Using language which invokes a sense of urgency (a reason why to respond) or because of a known relationship, these increasingly sophisticated attacks all target a psychological response to improve their effectiveness.

Spear phishing is On the Rise

127% **increase in spear phishing attacks**

Our aggregate data reflects a 127% increase in spear phishing attacks between Q1 and Q4 2022.

>9.9% **potential risk in all emails**

Significant not only due to its growth pattern, spear phishing now accounts for a consequential > 9.9% of potential risk in all emails.

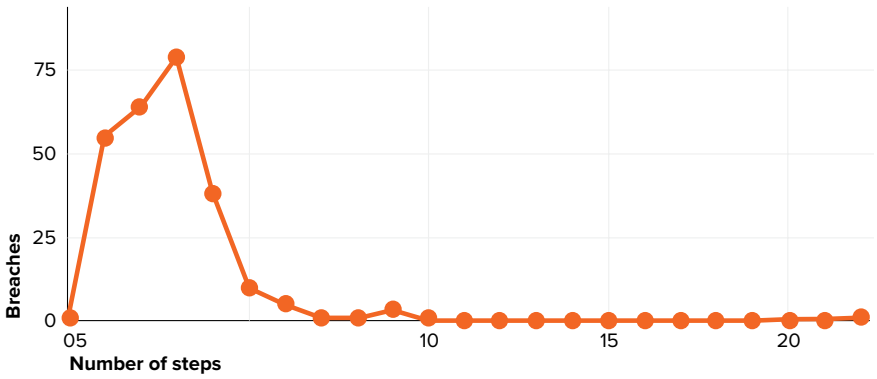
These incredibly targeted attacks go after a single user, whom the attacker knows will have access to do something or have a highly privileged account. Typically, these spear phishing attacks appear to come from someone the recipient knows (impersonating a trusted person or brand). But what makes these spear phishing emails so dangerous is the layer of social engineering used to craft highly sophisticated emails from the widely available data from open web sources to appear legitimate.

Common Features of a Spear Phishing Email:

- Sent to a single recipient
- Incorporates data available on social media or websites
- No misspellings or odd grammar
- Often contains a hyperlink

BOTH FREQUENT AND SOPHISTICATED - IMPERSONATION ATTACKS CONTINUE

Impersonation attacks carry particular risks as they are frequently multi-stage. They begin with an attacker compromising a website, sometimes referred to as a legitimate link. Once this has been done and someone clicks on this link, they are brought to this malicious destination site. During this time, the attack executes its payload giving credentials or deploying malware. The payload is then deployed by impersonating a brand or an executive using manipulation techniques that exploit human error to gain access to information.



Brand impersonation attacks using commonly known and used applications tend to be most common and represent 43% of all emails that represent risk to an organization.

By impersonating a trusted company or brand, attackers more effectively trick users into responding or clicking on a link. Because these brands are so common, email recipients are more likely to take requested action without close scrutiny. The sophistication of these attacks means that even the vendor's native controls may miss these phishing attacks, as is evidenced in the following blog, "Google Workspace Missing Google Brand Impersonation Attack."

The top 7 brands for attackers to spoof are:

Google Microsoft amazon Dropbox wetransfer FedEx zoom

These represent 72% of all brand impersonations.

A Movement Toward Higher Effectiveness and Higher Reward

Our analysis revealed that in 2022, executive impersonation attacks have increased rapidly, with a 344% spike from Q1 2022 to Q3 2022, representing 6.7% of all risk associated with emails in 2022.

These executive impersonations consist of attackers using Display Names and Sender email addresses that appear to come from senior-level officers, such as a CEO or CFO. And, by targeting lower-level employees, implying or outright stating the urgency behind the request within the attack, success rates for the attackers increase.

These attacks present a higher risk for two reasons:

1. The attacks appear to come from a trusted, high-level individuals and make requests that are consistent with general business practices. As a result, these attacks are much more likely to get an employee to take action on the email.
2. These attacks can be particularly difficult for most email security vendors to detect. This is largely due to the language signals needed to detect these types of attacks. Typically brief, with direct messages being delivered to the recipient, detection of these attacks require the analysis of all email event data and symantecs (including, but not limited to Display Name, Sender Address, and body copy).

DEFINING RISK - THE TRUTH ABOUT LINKS

Data supports that there has been a significant improvement in third-party attachment scanning. Native controls in both cloud email providers, specifically Microsoft and Google, have resulted in a dramatic decline in attachment-based malware reaching users.

Attackers are not conceding, however, with suspicious links now replacing attachment-based attacks. Created with the intent of having a user click on a malicious URL, these dangerous links can be used to download malware, credential harvesting that leads to Account Takeovers and Business Email Compromise, financial losses and/or create beachheads to allow for additional forms of cybercrime.

Evaluation of the top 20 malicious links identified in 2022 further characterized the danger in hyperlinks.

One hundred percent (100%) of the top 20 malicious links were domains that were compromised and subsequently used to either capture credentials, deliver malware and/or capture financial/PII.

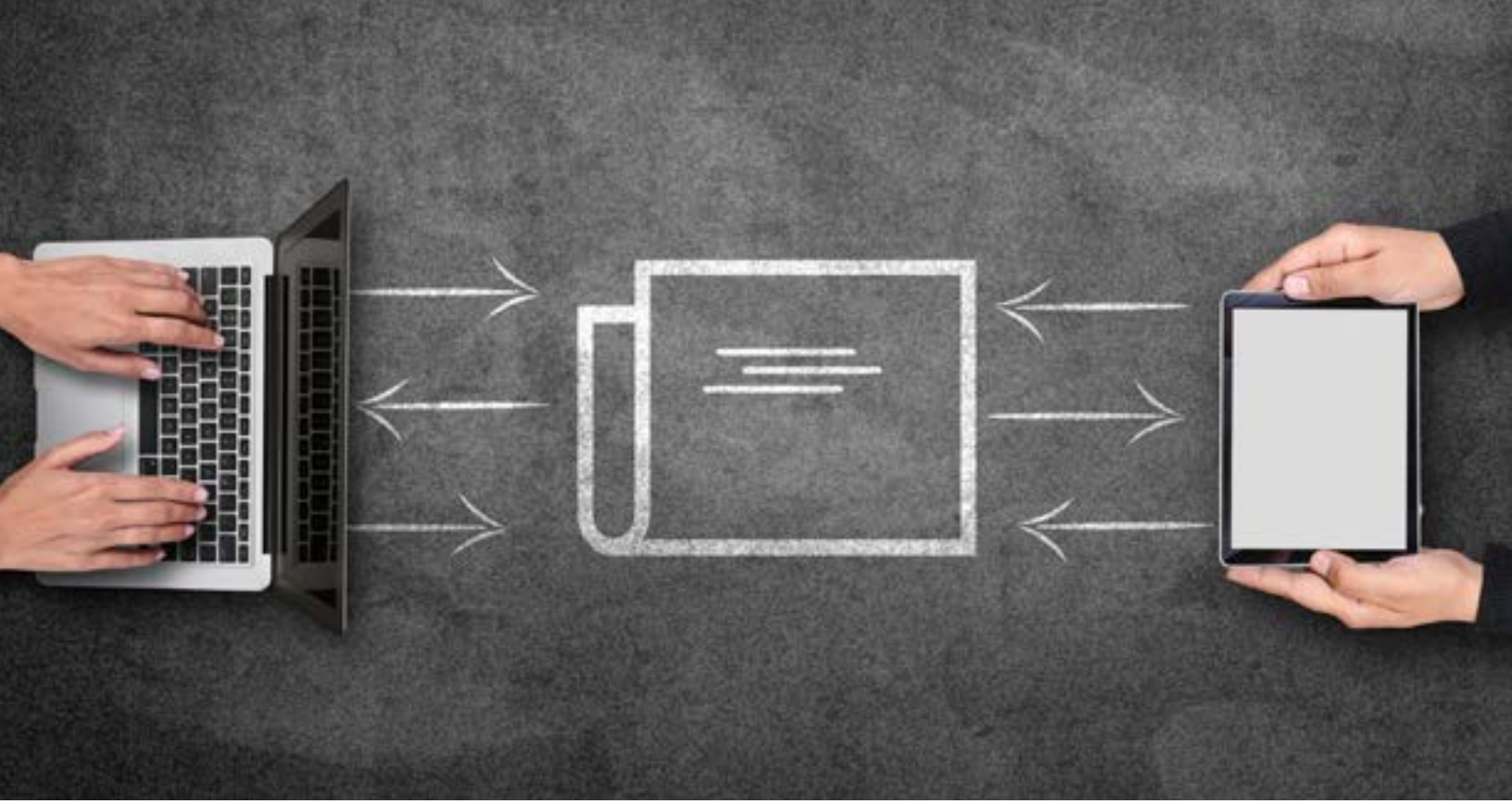
19% **suspicious links**

Representing over 19% of identified risks, suspicious links present a significant threat to organizations, highlighting the importance of security professionals providing multiple layers of protection to limit the risk of users interacting with suspicious or malicious links delivered in emails.

Attackers prefer domains that have a legitimate business purpose and content, which gives the domain a positive reputation score. This positive reputation score is preferred because it allows the attacker to bypass email security scans and increases the chance the email reaches the end user. However, once the domain is compromised by an attacker, these once non-malicious URLs become zero-day threats and represent substantial risk to end users.

Layering email security solutions, incorporating time-of-click analysis and suspicious link warning pages, reveal a greater level of risk reduction.

By quarantining links that turn malicious after delivery to an inbox, organizations can reduce risk by 100%. In addition, incorporating a suspicious link warning page if there are anomalous characteristics within the email, will reduce users visiting the destination site by 69.3%.



SHARED FILES CAN MEAN SHARED RISK

File sharing continues to be necessary for organizations to promote operational efficiency and ease of collaboration both internally and externally. Individuals require the ability to collaborate seamlessly, resulting in significant risk from file-sharing attacks.

2022 revealed that increased collaboration via the use of trusted file-sharing programs like docs.google.com or page.link, can easily bypass email security solutions as the root domain is determined to be non-malicious with good domain authority.

> Attackers using file sharing links on storage.googlesapis.com, storage.cloud.google.com, docs.google.com or page.link had the greatest quantity of potentially malicious links at 38%.

In these types of attacks, since the URL itself is deemed "good", landing in the user's inbox, where once clicked, bad actors install viruses, worms, spyware and other malicious code within the files to be automatically downloaded onto their machines once the user accesses the file sharing link.

Our data revealed that file-sharing links in these common collaboration-based platforms are being used as another popular technique to bypass security, with limited options to mitigate the risk.

Our data support the potential risk of file sharing based on the attacks using common sharing applications.

PERSONAL EMAIL USE CONTINUES TO IMPACT BUSINESSES

While quite common, the practice of allowing employees to utilize their personal email addresses to send information to their corporate account continues to pose a risk to organizations. However, personal domains contain an inherent risk to security teams, regardless of whether it's @gmail.com, @yahoo.com, @icloud.com, or any number of these personal accounts.

There is a data loss issue even if a legitimate account is being used, as personal email may not be well protected by the individual, even if strong protections are in place at the corporate level. In addition to data loss, organizations can experience a disruption based on exploits carried out on unsecured computers, represent just a few of the concerns related to the crossover of personal and work email.

Highly deliverable by definition, these accounts present a significant risk for data leakage:

- Always pass SPF/DKIM/DMARC
- Easily copied by an attacker who can set a desired display name
- May not be well-protected by the individual
- Frequent information exchange between personal and corporate accounts

1.2% **emails from personal accounts**

1.2% of all emails received within businesses were from personal accounts

Want to learn more?

- Download the Guide to SPF
- Download the Guidee to DKIM
- Download the DMARC Whitepaper

THE EVOLUTION OF THREAT IS DRIVING CHANGE

The combination of added threat and with the need for advanced detection characteristics have resulted in companies embracing a new market sector - **Integrated Cloud Email Security (ICES)**.

The 2021 Gartner Market Guide to Email Security asserts that *"As the threat changes, it's important to reevaluate the capabilities and effectiveness of the current solution compared to new products. Increasingly the combination of the cloud email providers' native capabilities and an ICES is replacing the traditional SEG."*

Benchmark data from 2022 concluded that the implementation of an additional email security solution can significantly reduce engagement with these risky emails, using a layered, defense-in-depth approach.

89% **reduced user engagement risk**

To minimize operational impact, while enhancing overall safety, security professionals who provide custom bannering to incorporate company policies and educating users about specific risks within emails, reduces the risk of a user engaging with an email by 89%.

With links continuing to be leveraged and increasingly used in attacks, quarantining malicious links, including pre and post-delivery, is a necessity for organizations. In addition, to increase the security posture of organizations, suspicious link warning pages should also be part of the proactive security posture.

When incorporated, suspicious link warning pages will prevent a user from reaching a destination site that appears suspicious over 69% of the time.

For known bad and highly anomalous emails, quarantine is a highly effective measure. False positive rates of any email security solution should not create a burden on Administrators and should fall below 3%. In addition, detection rates for the added security solutions should be greater 99.5%.

By applying a layered, defense-in-depth approach to email security, organizations can dramatically mitigate the risk phishing attacks, reducing the potential for a data breach to occur in 2023 and beyond.

THE BOTTOM LINE

Despite native controls capturing significant volumes of potentially malicious email, the platform continues to pose significant inherent risk. Email now dominates a vast percentage of work life, and is used as a means of both communications as well as sharing and data exchange. As reliance on this digital platform continues to grow, attacks have followed course while continuing to develop in sophistication.

Phishing attacks remain an all too common threat vector, succeeding in large part due to social engineering. These tactics involve attackers tricking employees into participating in their schema. Impersonation of both business entities and individuals is common, with these attacks using the trust implicit in a known sender to gain access to data, install malware, or even take over business accounts. The attacks have become increasingly individualized and targeted. Impersonation attempts frequently use easily accessible personal information readily available on the internet using just a few keystrokes. Sadly, we do not doubt that these types of attacks will continue to persist and succeed.

Despite heightened awareness, a lack of preparedness continues to cost companies data loss, financial impact, and business disruption. After all, only a single employee has to fall for an attack for it to be successful. As such, implementation of a behavioral-based security solution is imperative. Using advanced recognition techniques that extend beyond the traditional SEG and platform rule-based security measures, these tools facilitate user interaction that strengthens the security of the organization through in-the-moment awareness and participation.

Email threats represent one of the most commonly used means to attack organizations today. Tackling the types of threats that attackers continue to develop and refine with appropriate solutions is both your responsibility and your best defense.

Integration of API-based solutions allows faster deployment and time to value.

According to Gartner research, by 2025, 20% of anti-phishing solutions will be delivered via API integration with the email platform, up from less than 5% today.

ICES solutions:

"...go beyond simply blocking known bad content and provide in-line prompts to users that can help reinforce security awareness training, as well as providing detection of compromised internal accounts."

"...are deployed as a supplement to existing gateway solutions, but increasingly the combination of the cloud email providers' native capabilities and an ICES is replacing the traditional SEG."

About GreatHorn

GreatHorn protects organizations from more advanced threats than any other email security platform. By combining its highly sophisticated threat detection engine with accessible user context tools and integrated incident response capabilities, GreatHorn Email Security shields businesses from both sophisticated phishing attacks and fast moving zero-day threats, freeing security teams from the tedium of email security management while enabling them to respond to genuine threats faster than ever before.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other social engineering-based phishing attacks.