VIPRE
SECURITY GROUP

Email Security in 2023:

An Expert Look at Email-Based Threats

Content

Introduction

When you process 1.2 billion emails monthly, you notice a thing or two.

With more than 25 years in business and over four thousand active channel partners, VIPRE Security Group is an award-winning global cybersecurity, privacy and data protection company. Over the years, we've secured upwards of 20 million endpoints and keep consistent tabs on the state of email security.

After analyzing a cross-section of our email samples from 2022, we discovered a few trends worth unpacking. In this year's Email Security Trends Report, we'll dive into what precipitated email threat over the past year and discuss how companies can leverage this knowledge to stay one step ahead.

Threats Arising from Email Phishing

It is logical to conclude that the vectors most exposed to the internet are also the ones most exposed to threat actor attention.

For that reason, public facing email servers are prime targets for both active and idle criminal activity, and a host of cyber threats are transported via this route.

Phishing Statistics

According to the Verizon 2022 Data Breach Investigations Report[1], phishing is one of the four ways cyber attackers use to access and exploit your data.

Other methods include illegally accessing credentials, exploiting vulnerabilities, and botnets. While these exploitation methods themselves may come as no surprise, some of the phishing statistics we discovered last year might.

To contextualize our findings within the entire phishing landscape, we've also included statistics from this key industry research* below.

Phishing

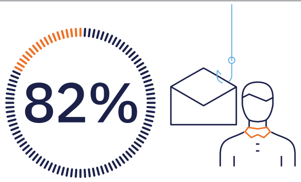
"Email encompasses the host of phishing, spam, and malware messages that come through." - Verizon 2022 DBIR

"Phishing is one of the top five most common action varieties in data breaches."

Between 2021 and 2022, phishing attacks increased for the finance and construction sectors, and finance still commands the majority share of phishing attention.

In **2022,** email phishing attacks accounted for **24% of all spam types** we received, compared to **only 11% in 2021** – an **increase of 13%.**

Breaches



In 2022, 82% of breaches involved the human element. Any time a user interacts with a process, there is a statistically higher chance of error.

The vast majority of breaches occur in a three-part process:

01 **Phishing**
02 **Malicious download**
03 **and Ransomware infiltration**

As the Verizon 2022 DBIR states, *"Our job as defenders is to lengthen that attack path."*

Web applications and email represent the top two most common breach vectors.

Spam

90%

spam emails 2022

The percentage of spam emails among our **2021** subset last year was a whopping **86%. However, in 2022 it rose to 90%.** These spam emails include phishing, scam, and commercial emails.

The **peak spam months** in **2022** were **August, September,** and **October.** This was largely due to a rise in phishing emails containing malicious HTML file attachments. These monthly trends vary slightly from our 2021 findings, in which the highest spam months were September, November and December. This could be due to an increase in LinkedIn and job spam as there was a surge in layoffs during that time frame, allowing attackers to create an additional attack angle.

There was a 22% increase in malspam emails with attachments from 2021 to 2022, as compared to malspam with links.

Of the links included in malspam emails, there was a 17% increase in links to newly created domains.

Industry Sectors

Financial institutions (48%) are still the most targeted sector by a wide margin, followed by construction companies (17%), who experienced a significant increase in phishing emails since 2021.

Last year, finance still held the lead (46%), with e-commerce coming in second (17%), a fact attributable to still developing online security practices born from the post-pandemic digital boom.

Attachments

QBot became the number one most common **malware family** we encountered in **malicious attachments,** taking over last year's Emotet.

Spoofed URL's

While Microsoft remained the most spoofed URL we tracked, this year Spotify came in second place. In 2021, Zoom (perhaps understandably) took second spot. This year, Zoom didn't even make the list.

In 2022 ".com" continued to be the most used Top Level Domain (TLD) in phishing attacks, followed by ".net" and ".org".

The number of newly created domains used for phishing ploys rose by nearly 10% YoY.

As you can see, phishing-as-a-profession is not going anywhere

Criminals are going where the money is, and counting on poor habits, human gullibility, and user error to get them there. Unfortunately, it's still working. As it lays out in the Verizon 2022 DBIR[1], phishing comprises the lion's share of social engineering activity and offers an explanation.

"If you wonder why criminals phish, it is because email is where their targets are reachable. And while only 2.9% of employees may actually click on phishing emails, a finding that has been relatively steady over time, that is still more than enough for criminals to continue to use it. For example, in our breach data alone, there were ***1,154,259,736*** *personal records breached. If we assume those are mostly email accounts, 2.9% would be* ***33,473,532*** *accounts phished, (akin to successfully phishing every person in Peru)."*

The numbers don't lie, and the more email is used as the primary form of business communication – and it is – the higher the risk of phishing will be. You could say it's good job security for threat actors. According to The Future of Digital Communication Study[2] by SendGrid, email remains the preferred method of communication across the board to the tune of 74%, with 89% of respondents using it monthly for either business or personal reasons. Despite the rising popularity of platforms like Slack, Trello, LinkedIn, or just social media in general, the number of emails sent per day has risen by nearly 5%[3] in the past year alone – and is expected to continue to rise. As long as email use continues to trend upwards, so will the risk, ingenuity, and vectors of phishing attacks.

Email Risk

Inbox surprises are designed to look like anything but – the more innocuous, the better. Here are a host of ways bad actors are getting around public perception, security controls, and our own best scrutiny.

Insider Threats | Every year, over one third (34%)[4] of businesses are affected by insider attacks. Over the last two years, they've increased by a staggering 44%[5] and they take an average of 85 days to contain – up from 77 back in 2020. A malicious insider is a particularly dangerous email threat as they not only have access to the contact information of key executives, but also the corporate knowledge, culture, and specifics they would need to launch – or facilitate – a convincing social engineering attack.

Spam | While this is probably the biggest category of them all, spam itself can be broken down into further subcategories for the sake of understanding specific motives and vectors.

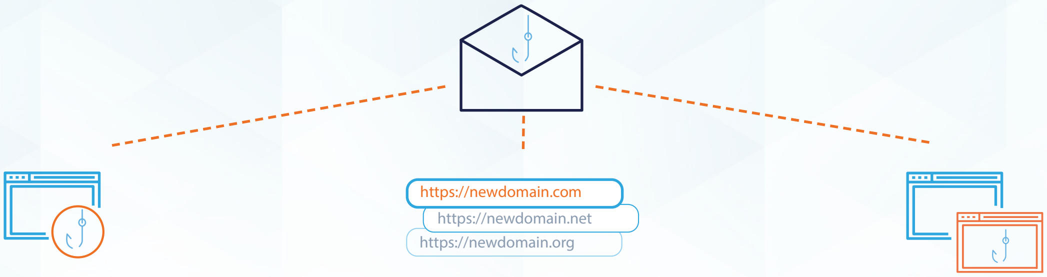
Holiday Spam | According to Norton's 2022 Cyber Safety Insights Report[6], 36% of Americans have fallen victim to holiday spam attacks. While we are trained to look out for those 'too good to be true' flash sale emails, cybercriminals have gotten sneakier and are coming from a different angle. Awaiting holiday deliveries, eager (and often harried, distracted, or unsuspecting) consumers will automatically confirm an address or login to a shipping company like UPS or DHL – only to find out later that the push was a set-up. Unfortunately, spam of this nature boasts a 60% click-through rate.

Job Spam | Interestingly, we noted an uptick in job-related spam in Q4 of last year, which was being exploited by bad actors to deliver phishing and malware. Industry research[7] from the Better Business Bureau notes that pandemic-related drivers created the 'perfect storm' for these types of scams, picking up on those desperate for remote or flexible-schedule jobs. According to AARP's director of fraud victim support Amy Nofziger[8], scammers 'follow the headlines' and have profited at the intersection of online hiring and work-from-home trends.

Nearly All North American Spam | In the last half of 2022, the US (54%) took over as the top-spam source for our clients. In the first half of the year, it had been Russia. Following the US was Canada (24%) and Chile (12%); the majority of spam emails from the latter were phishing related. It is important to keep in mind that most of the world's servers are located in North America. Countries from all over the world use servers based in the US and Canada, so the true origin of those spam emails is difficult to trace.

Email Risk

Domain Compromise | Within phishing emails, the phishing links we found were comprised of compromised websites (52%), newly registered domains (39%), and subdomain cybersquatting (9%).



Compromised Legitimate Websites/ HTML Smuggling (52%) | An increasing trend that we've seen over the past few months is bad actors hiding malicious HTML in compromised webpages within legitimate websites – take BBC.com, for example. Also known as HTML smuggling, this is especially nefarious as the established site won't trip any security sensors and passes all firewalls and controls – only to release the equivalent of toxic spores once inside. To combat this, you need a security tool proficient in sandboxing domains and vetting them continuously for safety – since these attacks can happen day-to-day, point-in-time investigations won't do.

Newly Registered Domains (39%) | Nefarious new domains are easy to set up and similarly easy to exploit. While some security controls flag for NRDs, they still largely evade most cyber defenses – passing with a 'clean bill of health' and bearing malicious payloads in the process. To avoid advanced detection, some bad actors even take the time to use AI (like ChatGPT) to create legitimate content, rank on Google, and wait out the 32-day period until their 'new domain' falls off the radar. Per our research, links to newly created domains represented 17% of the links included in malspam emails.

Subdomain Cybersquatting (9%) | This is an especially crafty tool as it leverages the official domain name itself. Subdomain cybersquatting is a spoofed side designed to look like it's affiliated with the legitimate one – canada-netflx.com, for example.

Additional Types of Email Risk

Malicious Attachments vs. Links | We noted an increase in the use of phishing emails with malicious attachments as opposed to malicious links between 2021 and 2022. While checking links should be no less important, companies need to spot the trend and invest in security solutions that can safely scan malicious attachments for danger before allowing a user to open them.

As-a-Service Models | The –aaS economy is a major driver of the proliferating phishing attacks we see. Phishing-as-a-Service (PhaaS), SMSishing-as-a-Service (SMaaS), and Hacking-as-a-Service (HaaS), among many others, are standardizing the underground economy and putting exploits on a subscription model. This makes them more affordable, more readily attainable, and more profuse in the public landscape.

MFA Sidestepping | Bad actors follow the security and technology trends as closely as we do, maybe even more. Jumping on the MFA bandwagon, cybercriminals are posing as the MFA vendor themselves and intercept real verification pushes to capture credentials into a spoofed site.

QR Code Spoofing | Phishing attacks are taking advantage of QR codes as they are increasingly found in organic advertising. Be cautious before paying via a QR code, downloading a QR scanner (you shouldn't need one), or downloading an app from a QR code – it could be a malicious link.

Financially Targeted Attacks | This should come as no surprise, but financially motivated attacks are still on the rise when it comes to the focus of phishing emails. Bank fraud accounted for 28% of all scam emails in H2 of 2022, and 48% of all malspam emails in Q3 & Q4 were directed at financial institutions.

Business Email Compromise | Business email compromise does more damage than we think and is more financially lucrative for attackers. The most recent FBI Internet Crime Report[9] states that BEC accounts for $2.4 billion dollars of losses, compared with $49.2 million from ransomware – making it 49 times more financially impactful. Per the Verizon 2022 DBIR, over 40% of all BECs involve phishing.

Domain Warming | We've also seen an increase in domain warming. This is when companies (paid for this very purpose) create a reputation for new domains by sending emails under a clean, legitimate IP address so they won't get blocked by spam filters. When they're eventually caught, they move on to the next domain and start over again.

Year-End Renewal Rush | Phishing actors take advantage of any digital current that flows into our inboxes, and every year that includes subscription renewals. According to an online Google and Harrison Poll[10], over half of internet users (52%) reuse passwords across accounts. It's all too easy to click on a 'Spotify' email - especially when your renewal is up, and they've leveraged the actual logo - and login to a spoofed domain.

Account Takeover (ATO) | This is probably one of the worst email related threat scenarios. What can start out as a case of stolen credentials can end up with a criminal leveraging internal permissions to heighten their attack damage across a network. Once the threat actor has successfully taken over an account, they have access to all the systems, privileges, and sensitive data as the compromised user.

Cloud Storage to Host Malicious Files | As the cloud expands, it increases capabilities for everyone. Phishing pages can be easily hosted and disguised in legitimate public cloud storage sites like Google Drive, Box, or AWS. Check source code to make sure that the assets behind the login are coming from the right source.

Threat actors want to blend into the fabric of our digital lives as much as possible, which makes these subtle phishing ploys all the more dangerous.

The Email Security Landscape: Predictions for 2023

Based on our two-year collection of data, we've made some predictions about what trends organizations can expect to see in the email threat landscape of 2023.

Expect more remote work-based attacks. If users are prone to mistakes within the vigilant environment of a corporate office, how much more so at home in their comfort zone? In addition to workers being off-their-guard, the amount of email communication necessitated by remote work also drives up the statistical chances of email-based attack. Web-based verifications for instances like Teams, Slack, and Asana can also increase the likelihood of hidden phishing exploits. Additionally, their frequency encourages security fatigue – and even less vigilance – among employees.

Brace for the growth of the as-a-Service economy. Bigger than the sum of its parts, the malicious – aaS economy is now an unstoppable machine. Once people have found a way to do something easier, cheaper, or better, human nature never trends back. Now that those previously barred from entry by technical restraints can just buy what they couldn't make, easily available nefarious exploits will continue to plague inboxes at an ever-higher degree.

Small businesses will become bigger targets. Cyber poachers are always looking for unlocked doors. Why break through a window when, with a little more time, you can find an entryway completely unguarded? As attackers continue to adopt aaS methods, the cybercriminal profile is changing to a less-sophisticated threat actor that increasingly wants an easy exploit, not necessarily a big one. What's easier than targeting small to medium-sized businesses that lag on cyber defenses because they think they're too small to hit? If SMEs don't scale their email security to the level of today's threats, they might find it difficult to do tomorrow.

Additional 2023 email threat trend predictions include:

An **increase** in **HTML smuggling.**

Rise in **MFA** and **QR Code-based phishing.**

Although in the number two spot, **Emotet** will be **widely used in 2023.**

Expect possible **tourism-related phishing** emails as travel continues to surge.

Watch for **phishing emails** around current events.

While knowing what's ahead is the first step, knowing how to defend against it may be the most important.

Email Security Goals

In fortifying against these email threats, there are certain best practices companies can adopt to avoid becoming the next opportunistic attack.

Implement a layered email security strategy. The harder you make it on attackers, the more likely they are to move on to greener pastures. While phishing and email threats will persist, bad actors are also working on an economy of time and resources. Layered defense, like VIPRE Advanced Threat Protection, could spell the difference between the next easy PaaS victim and the company that stays out of the press.

Invest in behavioral-driven analytics. The main threat of a phishing campaign is what happens after your credentials are stolen. To that end, companies must invest in proactive email protection solutions that can spot – and respond to – behavioral anomalies within the enterprise and that fit their organization. VIPRE EDR is built specifically to mitigate these instances in small to medium-sized businesses. Mistakes are inevitable, but ultimate compromise can be prevented.

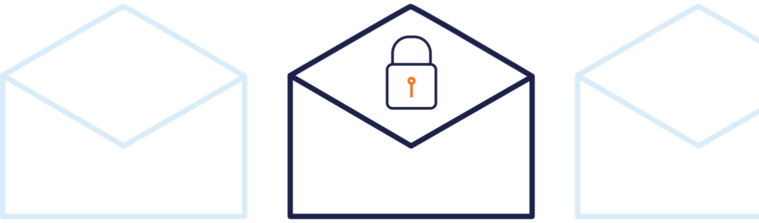
Secure data in transit. If we're not careful, we can end up doing a cybercriminal's work for them. Phishing attempts often request sensitive information to be sent via a response. Specialized platforms like VIPRE Email Security Cloud add-on can encrypt confidential emails and facilitate compliance. Not only that, VIPRE SafeSend notifies the user when they are sending externally sensitive information - adding that extra valuable layer of defense for employees.

Deploy email-specific security controls. Overall cyber safety is not enough to catch specifically crafted email threats that plant malicious links. Organizations need a dynamic solution that goes beyond static webpage checks. Does this link try to pull the Microsoft logo? Is it using JavaScript to create a page in real-time? Dynamic crawl abilities like the ones in the VIPRE email protection suite perform malicious reconnaissance before you visit the site – not after it's too late.

Protect all endpoints. Email threat actors are always looking for the weakest link in the chain. A comprehensive solution that secures all endpoints like cloud-based VIPRE EDR can scan files, processes, and network activity so you can catch email threats regardless of the stage of the exploit.

Train users for better security awareness. Because inevitable human error remains the leading cause of breaches, organizations must continue to train their workforce in cybersecurity best practices. A holistic solution calls for both technical controls and an expanded knowledge base. Security training programs like VIPRE Security Awareness Training educate a distributed workforce about what threats to watch for, where email-based exploits could be hiding, and how to leverage the tools around email security.

The safeguards you implement now will only have a wider, more lasting impact as your organization continues to grow. Your solutions should be tailored to the size of your enterprise and scale with your growth. That's why, when putting these best practices into place, it's integral to partner with the right provider.



VIPRE Email Defense

VIPRE Security Group believes in creating a holistic security solution for small to medium-sized businesses. Email security is an integral part of that solution.

That solution is achieved in two ways. First, technical controls implemented that are sufficiently scaled to meet – and beat – the level of today's emerging email threats. Secondly, trained personnel must be put in place to support these initiatives, both on the security side and on the part of the user.

VIPRE's comprehensive email protection platform serves as a first line of defense against phishing, viruses, and spam – both on-premises and in the cloud. Powered by AI, its six layers of scanning protect users against both known and emerging email threats. With attachment sandboxing, it scans for embedded HTML and zero-days. Link isolation allows it to detect malicious URLs while running in a safe, off-browser environment.

VIPRE SafeSend flags outgoing mail and prevents sensitive emails from being sent to the wrong person. If confidential data is detected, the user will be notified before a missend can occur. And VIPRE's Email Security Cloud add-ons can defend against phishing threats, malware agents, misaddressed emails, and data loss.

No security solution would be complete without the key factor that makes it run – its people. That's why one integral element of all VIPRE security solutions is our uncommon level of support. Our award-winning, highly qualified team of global support agents is ready to jump on a call with you right when you need them the most and walk you through mitigating solutions. They are here to make sure our security solutions deliver every ounce of value you expect them to, and to provide additional help and support when needed. Available 24/7/365, they have earned an impressive 90%+ CSAT rating.

Lastly, no defense-in-depth strategy is effective without the cooperation, compliance, and cohesiveness of its users. We don't want to help you build the enterprise security platform you've always wanted only to see it undermined by misuse. VIPRE Security Awareness Training can keep your workforce abreast of current changes, make them aware of attacker intentions and threat trends, and make them an asset to your security roadmap – not a liability.

Conclusion

The best laid plans are enough to build a future-proof, scalable, defense-in-depth strategy that can protect your enterprise against next year's email exploits. As defenders, it is our job to understand the adversarial approach and dig in our defenses. By scaling up email defense, we can lock down access to our number one threat vector and take a giant leap forward in building zero-trust.

Sign up today for your FREE 14 day VIPRE Email Security Trial.

*Whitepaper Industry Research References

[1] Verizon 2022 Data Breach Investigations Report / Verizon 2022 DBIR - https://www.verizon.com/business/resources/reports/dbir/

[2] The Future of Digital Communication Study - https://sendgrid.com/marketing/guide-future-of-digital-communication/

[3] Risen by nearly 5% - https://www.oberlo.com/statistics/how-many-emails-are-sent-per-day

[4] 34% - https://www.sisainfosec.com/blogs/insider-threat-human-vulnerabilities-resulting-in-cyber-attacks/

[5] 44% - https://www.proofpoint.com/us/resources/infographics/ponemon-cost-of-insider-threats-report

[6] 2022 Cyber Safety Insights Report - https://newsroom.gendigital.com/2022-11-01-Online-Holiday-Shopping-Frenzy-Study-Shows-1-in-3-Americans-Tend-to-Take-More-Risks-When-Shopping-Online-During-Holiday-Season

[7] Industry research - https://www.bbb.org/content/dam/bbb-institute-(bbbi)/files-to-save/2020-bbb-employmentscams-report.pdf

[8] Amy Nofziger - https://www.fastcompany.com/90795980/i-didnt-really-get-too-suspicious-until-almost-the-end-why-employment-scams-are-on-the-rise

[9] FBI Internet Crime Report - https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[10] online Google and Harrison Poll - https://services.google.com/fh/files/blogs/google_security_infographic.pdf

North America	UK and other regions	DACH Sales	Nordics Sales
sales@vipre.com	uksales@vipre.com	dach.sales@vipre.com	nordic.sales@vipre.com
+1 855 855 5566	+44 (0)800 093 2580	+49 30 2295 7786	+ 45 7025 2223