



| Brief |

Social Engineering Series: Email Phishing

B-2024-02-22a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Social Engineering, Phishing, Malicious Attachments

February 22, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on February 22, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Social Engineering Series: Email Phishing

ZeroFox's Social Engineering Series breaks down aspects of the threat into digestible reports and outlines defensive actions that can be taken by individuals and organizations. Part One of this series explores email-based phishing, the opportunities it offers threat actors, how it is used to capitalize upon and enable successful social engineering techniques, and what steps can be taken to increase vigilance and reduce the threat.

Key Points

- Social engineering allows threat actors to take advantage of fundamental human attributes that are seen as weak aspects of a network's attack surface and prone to manipulation, exposing cognitive biases and emotional triggers in the attacker's favor.
- Phishing is almost certainly the most commonly-employed method of social engineering. Successful attacks facilitate data theft or the deployment of malicious software via unauthorized network access.
- Techniques, tactics, and procedures (TTPs) vary significantly over time and between attacks, though the vast majority of phishing attacks leverage a form of pretexting and ultimately rely on the victim's active participation.

- Email phishing is almost certainly the most commonly-leveraged method of communication observed in phishing attacks. Email phishing offers the attacker a number of advantages, such as the ability to use attachments to deliver malicious payloads.

| Introduction to Social Engineering

Cyber threat actors are predominantly motivated by power and influence: financial power, political power, economic power, and competitive power. To achieve this, they leverage the human element at the end of the keyboard. Since the inception of digital communications, malicious actors have sought to develop new and unanticipated techniques to manipulate, deceive, or otherwise influence those in a position to undermine adjacent security protocols or unknowingly divulge information deemed to carry value.

Threat actors take advantage of fundamental human attributes which, from the threat actor's perspective, are seen as exploitable vulnerabilities of a network's attack surface and prone to manipulation, exposing cognitive biases and emotional triggers in the attacker's favor. These include:

- A tendency to trust other humans, commands, or instincts
- An urge to explore curiosities
- A propensity to respect perceived authorities
- A willingness to assist or offer help when requested, if possible
- A proclivity to reciprocate, in either a positive or a negative manner
- The predisposition to oblige by social norms

Activity of this nature is termed social engineering, because its aim is to manipulate human behavior toward a financial reward or network access using cyber-based tools. If conducted successfully, a threat actor is able to obtain an advantageous position that can be leveraged to evade the hardened endpoints of otherwise correctly-configured network defenses governed by predefined security protocol and not susceptible to human interaction or emotional manipulation.

The advantage contrived by a threat actor from successful social engineering efforts is usually accompanied by further exploitative action intended to meet some predetermined ends that are dependent on the threat actor's motivations. Malicious software may be delivered to the target network, access may be obtained and sold for financial profit, or data may be extracted for a wide variety of subsequent uses.

| Phishing Overview

Phishing is almost certainly the most commonly-employed social engineering method observed across the cyber threat landscape, and is leveraged in multiple forms by an array of actors seeking personal gain of different natures. Within a broad category of social engineering attack methods phishing is very likely the main vector, leveraged in over 60 percent of attacks. This is followed by the illicit use of stolen credentials.¹

- Phishing attacks seek to manipulate a network's human element into unknowingly assisting the attacker to circumvent certain security protocols which may otherwise prevent initial stages of the attack from taking place.

A key reason for the prominence of phishing is its flexibility in allowing the attacker to conduct follow-up exploits leveraging various types of malicious software for further financial, ideological, or political gain.

- In 2022, a reported 90 percent of cyberattacks began with some form of phishing, or the threat actors were otherwise in illicit possession of information or credentials that were leveraged in gaining network access.²
- Nearly 50 percent of ransomware incidents were estimated to have been enabled by a prior phishing attack, and 36 percent of data breaches were enabled by stolen credentials.³

Phishing can be broadly separated in two categories: mass phishing and spear phishing. These can be distinguished by the level of effort employed by the attacker and the subsequent extent of expected payoff should they be successful.

¹ [hXXps://www.verizon\[.\]com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf](https://www.verizon[.]com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf)

² [hXXps://www.cisa\[.\]gov/stopransomware/general-information](https://www.cisa[.]gov/stopransomware/general-information)

³ [hXXps://www.ic3\[.\]gov/Media/PDF/AnnualReport/2022_IC3Report.pdf](https://www.ic3[.]gov/Media/PDF/AnnualReport/2022_IC3Report.pdf)

Mass phishing is loosely categorized as the simultaneous sending of malicious communication to large numbers of targets (often hundreds or thousands). Contact information is often acquired illicitly via dark web marketplaces—with many organizations made more vulnerable by the sharing of email domain names, making them easier to acquire. While many targeted email addresses may be unattended or otherwise void, the relatively low-effort nature of this attack method means it can be re-deployed consistently by threat actors of low sophistication.

- Mass phishing is almost certainly the most commonly-leveraged approach to phishing, comprising the majority of the approximately 3.4 billion spam emails sent each day.⁴

Phishing attacks can also be individually crafted and highly tailored, targeting smaller numbers of victims. The success of such attacks require higher efforts and, as such, is expected to return higher rewards. An example of this is spear phishing, a term used to describe attacks aimed at a specific group or person rather than relatively indiscriminate targets.

- To enable the success of these attacks, the threat actor will often offer personal details related to the victim that are intended to subconsciously increase authenticity.
- This information can include names, job roles, references to an outstanding task, or other information that enables the attacker to masquerade as an authority or party known to the victim.

The extent to which a phishing attack can be personalized hinges significantly on the time and resources available to the attacker and the online footprint of the target.

- These types of attacks are often associated with Business Email Compromise attacks or Email Spoofing, both of which often seek to fool the victim into believing a phishing email is internally-generated.

However, not only high-effort phishing activity can lead to attacks causing significant disruption. Low-complexity mass phishing attacks can lead to the distribution of

⁴ [hXXps://aag-it\[.\]com/the-latest-phishing-statistics/](https://aag-it[.]com/the-latest-phishing-statistics/)

| Email Phishing

In order to catch victims off-guard, threat actors are constantly seeking new, unusual, and unsuspected approach methods. A primary aspect of the process is the communication method used to make initial contact with the victim. The array of options available enables the specific targeting of victims from different geographic regions, industries, and demographics.

- Each communication method has certain advantages and disadvantages for the threat actor at every step of the attack. From reconnaissance-stage target selection and information gathering, to conducting the social engineering ploy against the victim, to executing a malicious payload on a victim's network.

Email almost certainly remains the most commonly-leveraged method of communication observed in phishing attacks due to a number of advantages it offers the attacker:

- *Ubiquity*: Email is a familiar and very widespread tool that is used by both individuals and organizations. Almost all potentially lucrative victims of a phishing attack have access to an email account, increasing the targeting opportunities available to threat actors.
- *Customization*: Emails offer the attacker the opportunity to enclose highly-personalized messages within, the aim of which is to increase both the perceived authenticity of the sender and the chances of the victim carrying out the request. The extent of personalization within a phishing email is dependent upon the level of prior research conducted and the intended payoff in the event of a successful attack.
- *Trust*: Email is very likely regarded as a secure communication channel by many users—often based upon the reputation and stature of platforms such as Google and Microsoft, as well as faith in the security stature of the victim's organization. This likely leads to reduced vigilance at both individual and organization levels.
- *Low Cost*: Despite high potential payoff, email is generally a much cheaper option than other communication methods, both in terms of finance and time. This is particularly relevant for the conducting of mass phishing campaigns.

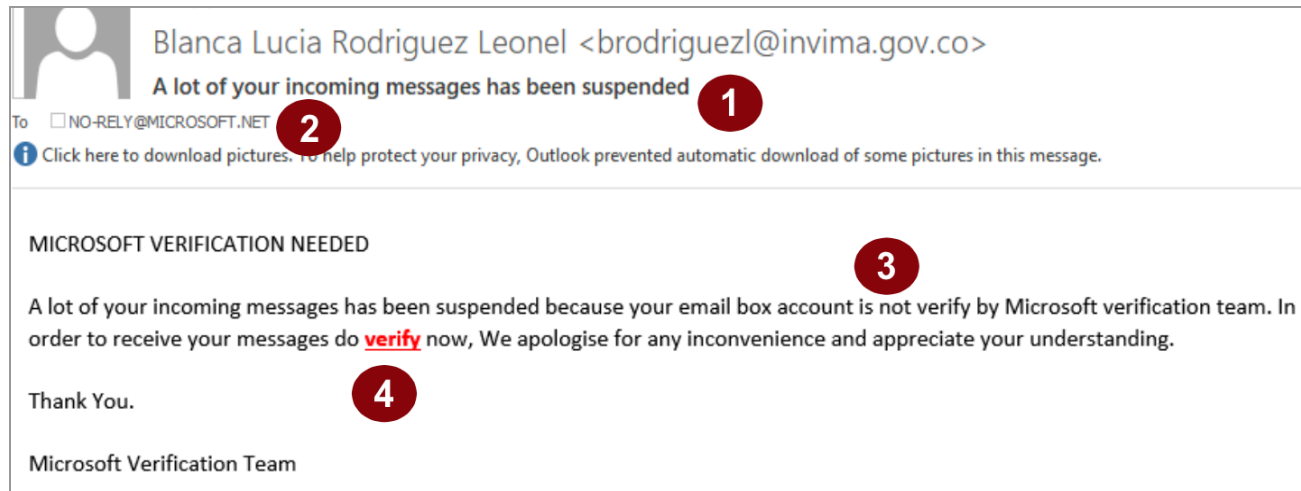
- *Attachment Exploitation*: Email offers threat actors the opportunity to deliver further malicious communications to the victim via attachments. Various file formats can be sent via email, the majority of which have the potential to conceal and deliver damaging software files unbeknownst to the victim.
- *Interception*: Many corporate environments rely heavily on email as the default method of daily communications. This offers threat actors the opportunity to hijack an ongoing conversation, reducing the need for pretexting to take place. Business Email Compromise (BEC) attacks are an example of this and will be covered in a future *Social Engineering Series* report.

The low-effort nature of mass phishing attacks means they often contain visible errors that are easily identified by webmail spam filters. These can penalize email communications based upon:

- Sender reputation
- Misleading subject lines
- Mis-matched geolocation
- The number of emails sent in a short period of time

Additionally, many errors will be obvious to a recipient who has a basic understanding of online security awareness. Common examples include:

- Spelling and grammatical errors
- Messages that attempt to instill a call to action within a short time frame
- Urgency necessary to avoid an apparent consequence
- Displayed text of embedded hyperlinks that does not match the URL within
- Abnormalities within the sender's email address



Phishing email sent as part of a likely mass phishing campaign

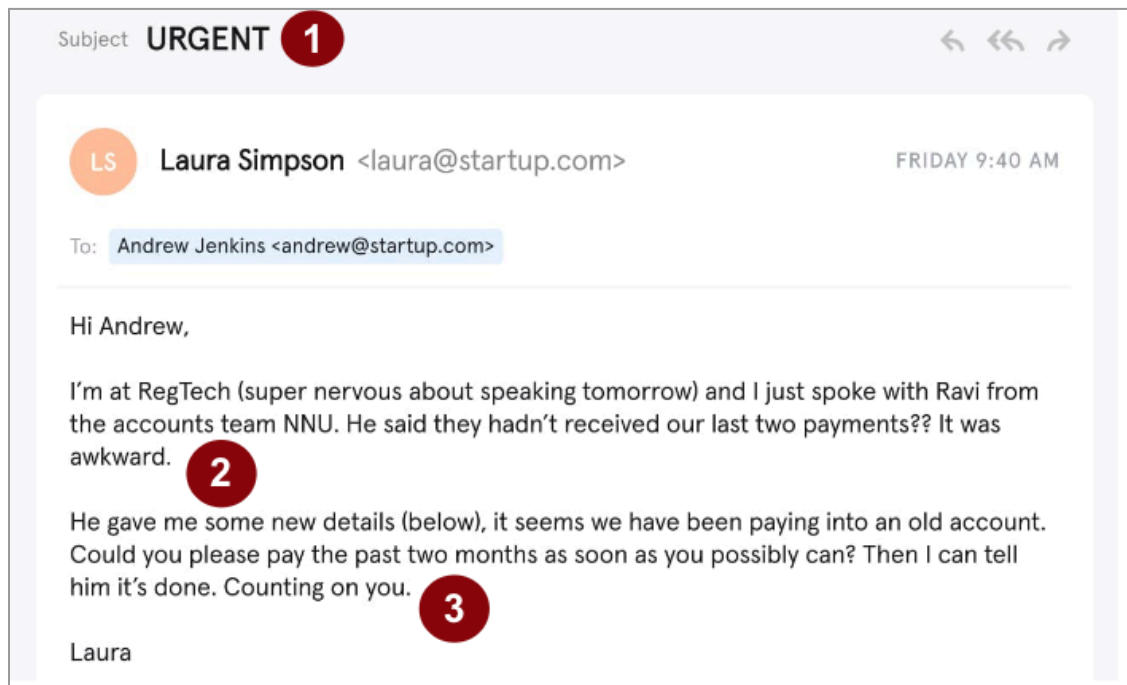
Source: ZeroFox Intelligence

- 1 Subject instills urgency and places responsibility upon the recipient.
- 2 Sender email contains spelling mistake and unlikely domain.
- 3 Email contains spelling and grammatical errors, which is unlikely in a genuine automated message from Microsoft.
- 4 Embedded malicious hyperlink, highlighted red to encourage action.

Emails used as a part of a higher-effort, targeted phishing campaign are often significantly harder to recognize, containing less obvious errors and requiring higher levels of vigilance from the victim. However, some commonly used techniques can be identified.

- Emails are likely to use headlines, key words, and bolded font to demand the victim's attention and instill urgency.
- The sender name may not match the email address from which email was received.
- The sender's address name or domain may contain subtle errors, such as letter replacements.
- The return path of the email may display details inconsistent with the sender's email address.

- If the email appears to be from a familiar sender, check for unusual behavior. This could be an unwarranted tasking, an unusual greeting, or discrepancies between the signature block and the sender address.



Phishing email sent as part of a likely spear phishing campaign

Source: [hXXps://www.tessian\[.\]com/blog/phishing-vs-spear-phishing/](https://www.tessian[.]com/blog/phishing-vs-spear-phishing/)

- 1 Subject instills urgency and places responsibility upon the recipient.
- 2 In order to gain trust, the email emphasizes familiarity by using first names, mutual connections and job titles.
- 3 Sender masquerades as a position of authority, attempting to instill urgency and fear should action not be taken.

| Malicious Attachments

Malicious email attachments were observed as very likely being on an upward trajectory in 2023 and were reportedly used in approximately 38 percent of Q1 2023 emails intent on stealing credentials, second only to embedded links.⁶⁷ Social engineering methods are

⁶ [hXXps://www.tripwire\[.\]com/state-of-security/phishing-trends-and-tactics-q1-2023](https://www.tripwire[.]com/state-of-security/phishing-trends-and-tactics-q1-2023)

⁷ [hXXps://cofense\[.\]com/blog/html-attachments-used-in-malicious-phishing-campaigns/](https://cofense[.]com/blog/html-attachments-used-in-malicious-phishing-campaigns/)

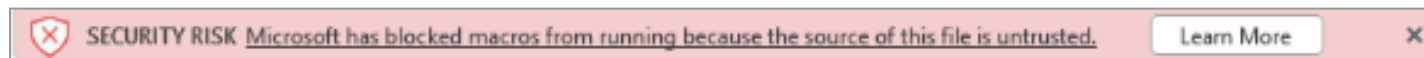
employed to make the attachment appear legitimate and increase the likelihood of interaction from the victim. Reportedly, 35 percent of ransomware was delivered by malicious attachment in 2023—the highest of any delivery method.⁸ Their popularity as a delivery method amongst threat actors stems from a number of reasons, with some key examples listed below:

- Attachments can be contextualized within the email, with the aim of justifying their presence and alleviating suspicion.
- A large variety of different file formats are used, often based upon the most appropriate attachment for the fictitious scenario employed. For example, an email masquerading as instructions to the victim to complete a government tax return would not be expected to contain a Microsoft Excel or Notes file, and their use may arouse suspicion.
- Email attachments can also be used to increase the likelihood of bypassing Secure Email Gateway (SEG) measures likely to flag the message as suspicious to the user. Webmail accounts may, for example, divert a message into a spam folder if it contains a URL link, particularly in the presence of other factors deemed suspicious. As the content embedded within a malicious attachment is not hosted on a website, SEG measures can find it more challenging to detect the phishing attempt.
- Attachments are more likely than links to remain on the targeted devices for a longer period of time, such as when the user is no longer online. This allows for more persistent access and prolonged attack, particularly if malware was successfully delivered by the attachment and does not require internet access for the malicious code to be executed.

Changes implemented by developers to their software Operating Systems (OS) or productivity applications can result in changes to a file type's popularity amongst threat actors. This was seen in Q1 2023 with Microsoft's disabling of VBA macros by default for internet-facing files, significantly reducing the ability to deliver malicious files to a

⁸ [hXXps://www.verizon\[.\]com/business/resources/Tff3/reports/2023-data-breach-investigations-report-dbir.pdf](https://www.verizon.com/business/resources/Tff3/reports/2023-data-breach-investigations-report-dbir.pdf)

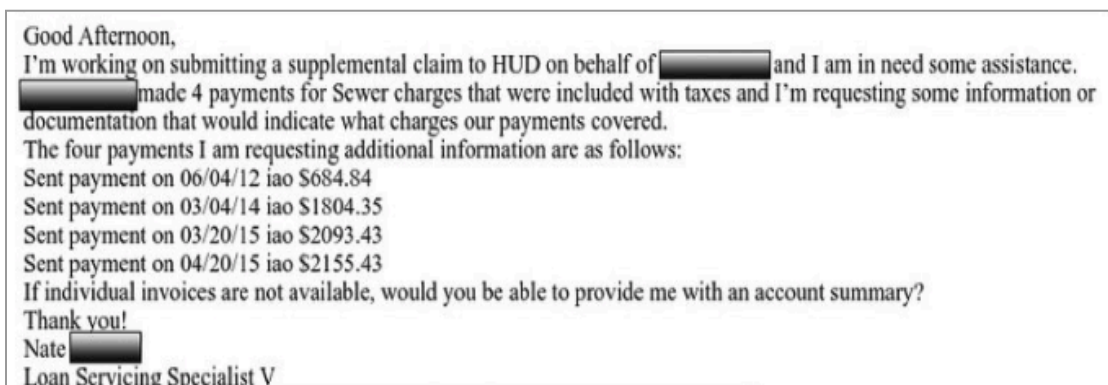
recipient. The warning message now confronting a user instead is almost certainly behind a reduction in the use of MS Office files as malicious attachments.⁹¹⁰



Warning confronting those in receipt of a Microsoft Office email attachment

Source: ZeroFox Intelligence

Another commonly-used file type is HTML, which has been used in HTML smuggling attacks often implicated in the delivery of the prominent malware strains QBot (QakBot) and Emotet. Threat actors are able to conceal a malicious script inside these files, which can assemble and embed itself on the target network upon activation. This method avoids malicious code being passed over a network, as this would require overcoming defenses such as firewalls and email gateways.¹¹¹²



QBot Phishing email

Source: [hXXps://www.phishlabs\[.\]com/blog/emotet-returns-from-hiatus-trails-qbot-in-q1-volume](https://www.phishlabs.com/blog/emotet-returns-from-hiatus-trails-qbot-in-q1-volume)

Other commonly-used file types include:

- **JPEG images.** These files have the advantage of being able to conceal malicious code within Exchangeable Image File Format (EXIF) headers, a metadata

⁹ [hXXps://learn.microsoft\[.\]com/en-us/azure/active-directory/manage-app](https://learn.microsoft.com/en-us/azure/active-directory/manage-app)

¹⁰ [hXXps://thehackernews\[.\]com/2022/07/microsoft-resumes-blocking-office-vba.html](https://thehackernews.com/2022/07/microsoft-resumes-blocking-office-vba.html)

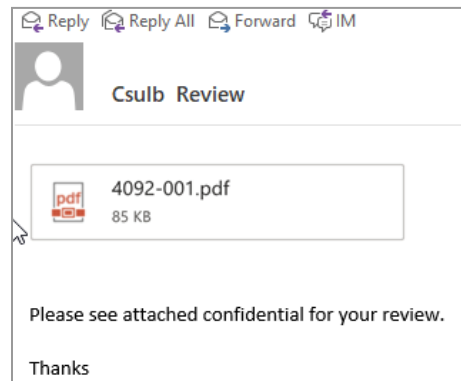
¹¹ [hXXps://www.cyfirma\[.\]com/outofband/html-smuggling-a-stealthier-approach-to-deliver-malware/](https://www.cyfirma.com/outofband/html-smuggling-a-stealthier-approach-to-deliver-malware/)

¹²

[hXXps://www.bleepingcomputer\[.\]com/news/security/qbot-phishing-abuses-windows-control-panel-exe-to-infect-devices/](https://www.bleepingcomputer.com/news/security/qbot-phishing-abuses-windows-control-panel-exe-to-infect-devices/)

standard. These are often undiscoverable without the use of optical character recognition (OCR) software.¹³¹⁴

- **Windows executive files (.exe).** These are often reported as one of the most commonly-leveraged file types, likely due to their generally-widespread use and familiarity generating less suspicion, their inherent execution capabilities, and their effectiveness when targeting Windows Users.¹⁵
- **LNK files.** These are also a popular delivery method due to their omission from Mark-of-the-Web controls, which would usually subject internet-originating files to additional scrutiny. Bypassing this enables legitimate applications like PowerShell, CMD, and MSHTA to open attachment files, folders, or applications, thereby resulting in the execution of malware without warning to the user.¹⁶



Embedded image designed to appear as a PDF attachment

Source: [hXXps://itss.csuchico\[.\]edu/phishing/pdf-phishing-emails/](https://itss.csuchico.edu/phishing/pdf-phishing-emails/)

Threat actors have been observed leveraging fake email attachments, whereby an embedded image will be designed to appear an attachment. This offers threat actors a means by which to embed a remote URL likely to appear as local and able to circumvent security checks. This attack method relies on the premise that email attachments are

¹³ [hXXps://umbrella.cisco\[.\]com/blog/picture-perfect-how-jpg-exif-data-hides-malware](https://umbrella.cisco.com/blog/picture-perfect-how-jpg-exif-data-hides-malware)

¹⁴ [hXXps://blog.cloudflare\[.\]com/2023-phishing-report/](https://blog.cloudflare.com/2023-phishing-report/)

¹⁵ [hXXps://web-assets.esetstatic\[.\]com/wls/2022/10/eset_threat_report_t22022.pdf](https://web-assets.esetstatic.com/wls/2022/10/eset_threat_report_t22022.pdf)

¹⁶ [hXXps://cyble\[.\]com/blog/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/](https://cyble.com/blog/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/)

more likely to be clicked than a hyperlink, which appears more suspicious, while also evading SEG measures that are hostile to embedded URLs.¹⁷

Compared to attachments, embedded links very likely have a significantly higher chance of reaching their intended victim than that of attachments. This is due in part to fundamental vulnerabilities in webmail configurations, which are accustomed to being confronted with high levels of unknown but legitimate email addresses. For example, many organizations' marketing departments rely upon this to reach new customer bases.

Other tactics, such as URL redirecting and using cloud-registered domains, have proven effective at circumventing or exhausting SEG defenses in place. Despite this, there is a roughly even chance that attachments will become more prominent over time as individuals and organizations become increasingly aware of the dangers posed by links.

Resilience – Email Phishing

- *Scrutinize emails, even if they appear to have originated inside the organization. Look for incorrect or unusual grammar, spelling mistakes, mismatched hyperlink URLs, and illegitimate sender addresses.*
- *Do not divulge personal details unless the sender can be verified. The majority of legitimate organizations would not ask for such information via email.*
- *Reduce the impact of an email phishing attack by ensuring networks and associated accounts are configured according to the principle of least privilege.*
- *Individuals and network endpoints should be granted only the minimum level of access and permissions needed to conduct a specific role.*
- *Ensure accounts with administrator rights are not being used for everyday tasks, such as web browsing or email communications. Credentials of administrator accounts are highly sought after by threat actors, as the elevated privileges enable lateral movement, persistence establishment, and data theft.*

¹⁷[hXXps://cdn2.hubspot\[.\]net/hubfs/4660171/Understanding%20Phishing%20-%20Fake%20Attachments.pdf](https://cdn2.hubspot[.]net/hubfs/4660171/Understanding%20Phishing%20-%20Fake%20Attachments.pdf)

- *Ensure an organization-level system is in place that enables employees to report suspicious email communications in order to bring awareness to ongoing campaigns and protect other users.*
- *If they are not already, ensure organizational email servers are correctly and appropriately configured with authentication measures such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). These will prevent messages from being marked as junk mail and domain spoofing.*

Outlook

Email is almost certainly going to remain a key aspect of the phishing threat landscape for the foreseeable future. While the use and technology associated with remote communication methods is continually evolving, the cost-efficient, reliable and straightforward nature of email technology will very likely ensure it remains a favorable option for threat actors for as long as it remains wide-spread amongst both individuals and organizations.

Email attachments will almost certainly remain a significant threat, though threat actors leveraging them to deliver malicious payloads to victim networks must continually evolve their TTPs to circumvent security features associated with software manufacturers, email service providers, and corporate network defenses. Higher-effort attacks seeking to conduct spear phishing, BEC, account takeover or impersonation, will likely become more common as security protocols, organizational vigilance and individual awareness become more proficient at hindering phishing attacks of low-sophistication. Mass-style phishing is unlikely to decrease in prominence, however, as it will almost certainly continue to offer threat actors successful results when correctly leveraged against unalert victims.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%