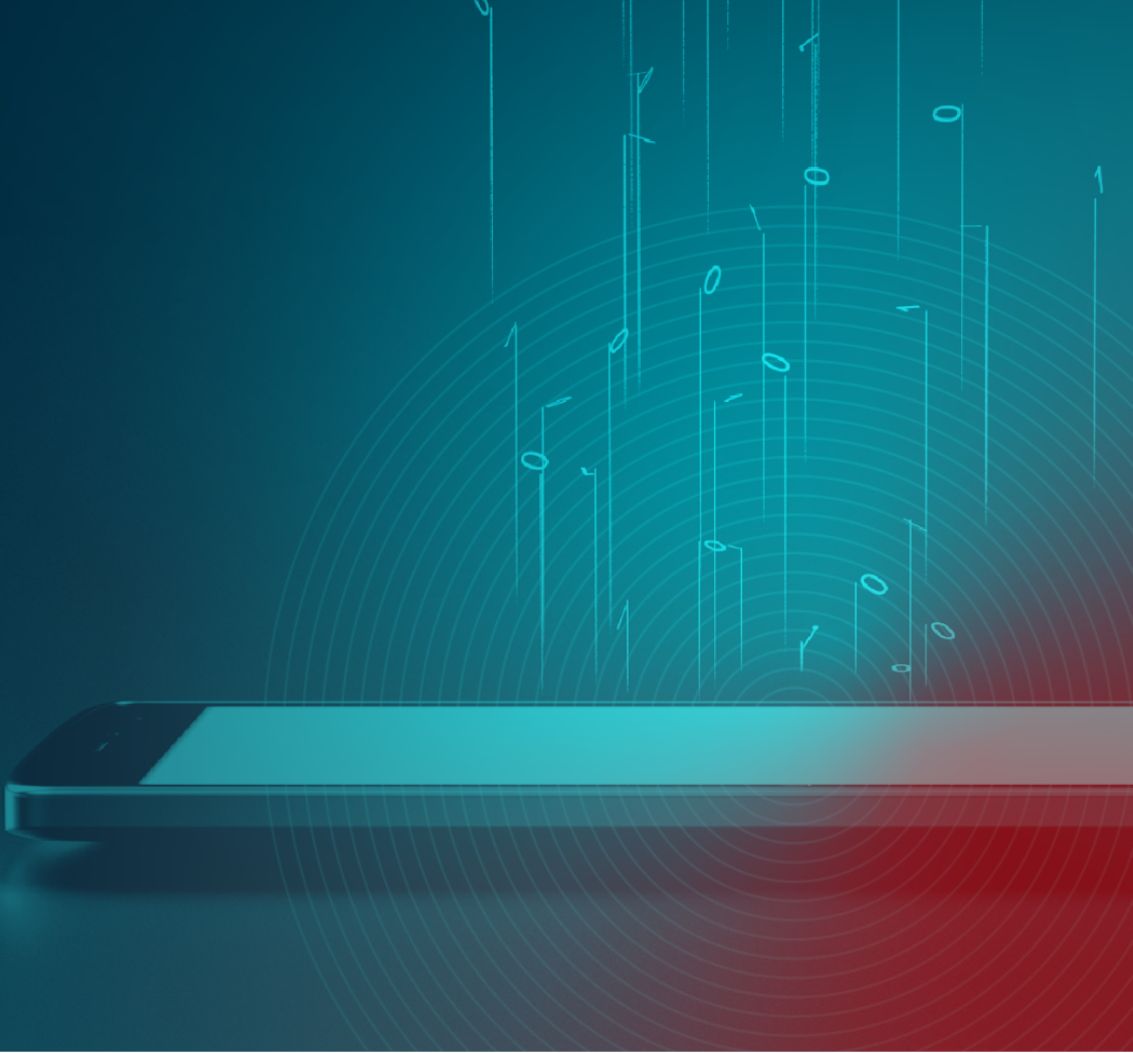
ZEROFOX Intelligence

› ASSESSMENT

2023
Phishing Trends

Classification: TLP:CLEAR



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 2:00 PM (EDT) on September 12, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

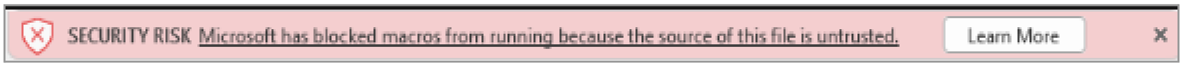
| Assessment | 2023: Phishing Trends

| Key Points

- Threat actors continue to evolve the techniques leveraged in phishing attacks to overcome security protocols and end-user cyber hygiene practices, as well as to capitalize on contemporary vulnerabilities.
- Email attachments remain a primary delivery method for malicious software in phishing attacks. Increasingly diverse file types are being leveraged—due in part to a need to circumvent security controls.
- Threat actors are increasingly exhibiting methods able to bypass multi-factor authentication (MFA) security protocols, including various types of "in-the-middle" attacks, MFA fatigue, and Open Authorization (OAuth) consent phishing.
- Phishing-as-a-Service continues to proliferate in both dark web marketplaces and private messaging channels, where sellers offer varied, competitive services, and contribute to significantly lowered barriers of entry to threat actors.
- Search engine platforms are likely increasingly able to mitigate against traditional search engine optimization (SEO) poisoning methods, such as typosquatting and keyword stuffing. However, the threat from SEO cloaking, webpage hijacking, and URL redirecting is likely on an upward trajectory.

An Evolution in Phishing Email Attachment Types

In 2023, ZeroFox Intelligence observed an evolution in the type of malicious attachments leveraged in phishing campaigns, with increasing diversification away from Microsoft Office files. This is very likely driven partly by Microsoft disabling VBA macros by default in 2022, resulting in typical internet-facing files being subjected to "Mark-of-the-Web" controls warning users of suspicious email attachments that may contain malware.[1]



SECURITY RISK Microsoft has blocked macros from running because the source of this file is untrusted.

Warning confronting those in receipt of an MS Office email attachment

Source: ZeroFox Intelligence

To circumvent these controls, threat actors increasingly leverage files such as Windows image files (ISO), archive files (RAR), Windows Shortcut files (LNK), OneNote files, restricted permission messages (RPMSG) files, and Windows Script files to deploy malicious payloads.[2] Threat actors have also been observed leveraging HTML smuggling to deliver prominent malware strains such as QBot and Emotet, whereby threat actors conceal a malicious script inside these files that is able to assemble and embed itself on the target network upon activation. This avoids malicious code being passed over the network.[3][4]

Malicious email attachments will very likely remain one of the most prevalent means of malware distribution for the foreseeable future. Reporting states that malicious attachments are leveraged in approximately 40 percent of phishing attacks and have

[1] hXXps://learn.microsoft[.]com/en-us/deployoffice/security/internet-macros-blocked

[2] hXXps://cyble[.]com/blog/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/

[3] hXXps://www.cyfirma[.]com/outofband/html-smuggling-a-stealthier-approach-to-deliver-malware/

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

been responsible for the delivery of 35 percent of ransomware so far in 2023—the highest of any delivery method.[5][6][7] Despite security controls being regularly updated to account for these file types—ensuring suspicious files are flagged to end users—it is very likely threat actors will continue to pivot to file types that circumvent security controls.[8]

The Growth of MFA Bypassing Techniques

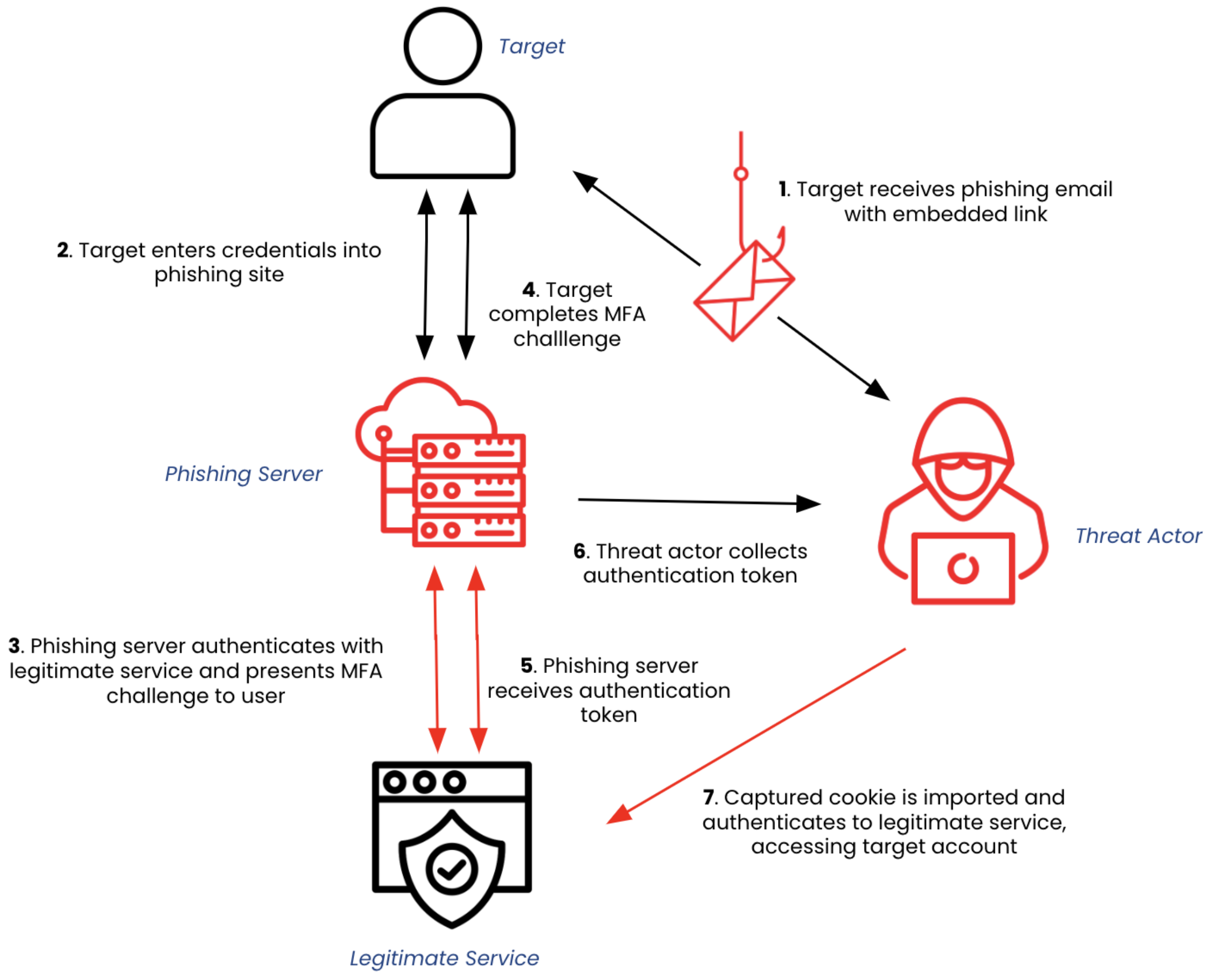
ZeroFox Intelligence assesses that threat actors are increasingly leveraging methods to undermine MFA into their phishing attacks, either by intercepting or circumventing MFA codes. Use of real-time MFA-bypassing solutions are on an upward trajectory, including “in-the-middle” techniques, MFA fatigue, and OAuth consent phishing. This enables the circumvention of MFA methods long-considered secure.[9][10][11]

In 2023, “in-the-middle” techniques are some of the most frequently-observed methods used to gain access to MFA-secured networks. They enable threat actors to intercept or bypass MFA protocols by stealing communications without the victim’s knowledge.[12][13] Threat actors create and exploit new sessions, or intercept existing ones, via session hijacking—including the stealing or selling of cookies and authentication tokens—session fixation, or session cloning. Exploiting vulnerabilities at the application and network layers can grant threat actors access to an authenticated session, undermining MFA protocols. Attackers can seize control of session permissions and parameters, facilitating greater opportunity for exploitation and detection avoidance. Phishing-as-a-Service (PhaaS) operations are increasingly incorporating “in-the-middle” capabilities into their offerings. Passive hijacking methods are also assessed to be on an upward trajectory, with threat

[5] hXXps://www.verizon[.]com/business/resources/Tff3/reports/2023-data-breach-investigations-report-dbir.pdf
[6] hXXps://www.tripwire[.]com/state-of-security/phishing-trends-and-tactics-q1-2023
[7] hXXps://cofense[.]com/blog/html-attachments-used-in-malicious-phishing-campaigns/
[8] hXXps://www.helpnetsecurity[.]com/2023/03/10/protection-malicious-onenote-documents/
[9] hXXps://mytechdecisions[.]com/network-security/2023-hacking-tactics/
[10] hXXps://securityboulevard[.]com/2023/04.the-art-of-mfa-bypass-how-attackers-regularly-beat-two-factor-authentication/
[11] hXXtps://blog.lastpass[.]com/2021/12/the-evolution-of-multi-factor-authentication/
[12] hXXps://www.aon[.]com/cyber-solutions/aon_cyber_labs/bypassing-mfa-a-forensic-look-at-evilginx2-phishing-kit
[13] hXXps://www.sisainfosec[.]com/blogs/best-practices-for-implementing-mfa-to-combat-brute-forcing-attacks/

actors leveraging packet sniffers—including open source tools such as Kismet and TCPDump—to capture and extract traffic traversing target networks.

It is likely the exploitation of OAuth frameworks increased in 2023, with greater permissions granted to third-party applications that do not require user credentials. "Consent Phishing"—luring victims to fake OAuth login pages and requesting the access needed for further exploitation—has facilitated the deployment of infostealers, social media manipulation, and full account takeover.


Target
1. Target receives phishing email with embedded link
2. Target enters credentials into phishing site
4. Target completes MFA challlenge
Phishing Server
6. Threat actor collects authentication token
Threat Actor
3. Phishing server authenticates with legitimate service and presents MFA challenge to user
5. Phishing server receives authentication token
7. Captured cookie is imported and authenticates to legitimate service, accessing target account
Legitimate Service

High-level example of how a token theft attack can take place

Source: ZeroFox Intelligence

Increasingly Sophisticated PhaaS Market

The threat from PhaaS operations very likely increased in 2023, with more off-the-shelf packages leveraging sophisticated capabilities. These services considerably lower the barriers to entry for threat actors, enabling less technically-skilled individuals to carry out targeted attacks for minimal cost. They are also increasingly available through private channels such as instant messaging forums, lessening the need for would-be threat actors to navigate the dark web.[14] Offerings can be purchased for as little as USD 50, with some of the most sophisticated packages available for USD 400 per month.[15] With high potential, scalable return on investments, and ease of acquisition, PhaaS offerings are very likely to remain a considerable threat for the foreseeable future.

ZeroFox Intelligence notes a range of capabilities becoming increasingly prevalent in PhaaS offerings. These include kits that are able to account for regional differences (with geo-blocking), prevent engagement from unwanted sources (such as researchers), and leverage multiple detection evasion techniques. ZeroFox Intelligence has observed an increase in PhaaS packages leveraging Domain Generation Algorithms (DGAs), which generate random domains threat actors can pivot to between during attacks, making it harder for victims to block and remove these domains.[16]

Adversary-in-the-Middle (AitM) PhaaS packages offering MFA-bypassing solutions—including reverse proxy and cookie-injection capabilities—are becoming increasingly prevalent, enabling threat actors to steal credentials and session cookies in real time. The presence and impact of these MFA kits on the threat landscape have since grown significantly and eased out lower-sophistication offerings from the market.

EvilProxy & Evilginx

EvilProxy is one of the most popular PhaaS packages available on the market. Leveraged to target MFA-protected accounts, it is cheap (approximately USD 400 per

[14] hXXps://thehackernews[.]com/2023/04/researchers-uncover-thriving-phishing.html
[15] ZeroFox Internal Collections
[16] hXXps://www.techtarget[.]com/searchsecurity/definition/domain-generation-algorithm-DGA

month) and easy to customize and deploy.[17] It utilizes reverse proxy relays to authenticate requests and user credentials between the victim and the legitimate service website. This enables threat actors to steal authentication cookies once a user logs into their account, bypassing MFA controls. In 2023, EvilProxy has been leveraged to target thousands of end-users and harvest credentials such as Microsoft 365 logins.[18] EvilProxy is known to leverage brand impersonation—including of Concur Solutions, DocuSign, and Adobe—scan blocking to make it harder for security services to analyze malicious domains and a multi-step infection chain.

Evilginx is a sophisticated reverse proxy tool for "in-the-middle" attacks leveraged in PhaaS offerings. It enables login credential and session cookie harvesting via phishing domains and facilitates MFA bypass.[19] Evilginx mirrors a website to lure users into entering credentials via Phishlets, configuration files in YAML for proxying a legitimate website into a phishing domain. Phishlets are open source and widely available. In May 2023, Evilginx 3.0 was released touting various improvements, such as refined TLS certificate management and session cookie extraction.[20] Previous iterations have been leveraged in attacks facilitated by both Initial Access Brokers (IABs) and the Robin Banks PhaaS offering, which advertises the Evilginx tool for up to USD 1,500 per month.[21]

Growth of SEO Poisoning

SEO poisoning attacks associated with the impersonation of brand names have been on an upward trajectory in 2023, with droppers and stealers such as BatLoader, GootLoader, and Vidar among the most prominent malware strains being delivered.[2223] Threat actors manipulate open-source search engine algorithms that are designed to return prioritized results bespoke to the user. Instead of legitimate sources, results are "poisoned" to prioritize malicious domains. Once accessed, malicious sites or

[17] hXXps://thehackernews[.]com/2023/08/cybercriminals-increasingly-using.html
[18] hXXps://www.bleepingcomputer[.]com/news/security/evilproxy-phishing-campaign-targets-120-000-microsoft-365-users/
[19] hXXps://hackmag[.]com/security/evilginx-phishing/
[20] hXXps://www.bleepingcomputer[.]com/news/security/robin-banks-phishing-service-returns-to-steal-banking-accounts/
[21] hXXps://www.ironnet[.]com/blog/robin-banks-still-might-be-robbing-your-bank-part-2
[22] hXXps://www.bankinfosecurity[.]com/seo-poisoning-attacks-on-healthcare-sector-rising-hhs-warns-a-22365
[23] hXXps://www.sentinelone[.]com/blog/breaking-down-the-seo-poisoning-attack-how-attackers-are-hijacking-search-results/

advertisements facilitate the delivery of malware, data theft, further phishing attacks, or fraudulent activity such as brand impersonation.

Two of the most prominent methods of SEO poisoning observed in 2023 are SEO cloaking and keyword stuffing. SEO cloaking—the manipulation of search engine web crawlers by revealing different information to that with which the search engine user is presented—is achieved via methods such as IP address filtering, IP cloaking services, and the utilization of JavaScript to decipher between a human user or search engine web crawler. Keyword stuffing—whereby irrelevant keywords are inserted into a webpage's text, HTML code, or

metadata with the intent of receiving a higher ranking from the algorithm—also very likely remains prominent.[24] While very likely increasingly mitigated through algorithm detection capabilities, this technique is most apt to be successful when masquerading as a search result with very little competition, such as those relating to particularly niche subject matter with limited publicly-available information.

In Q1 2023, Top Level Domain (TLD) provider Freenom paused its free registration service for domain extensions such as .tk, .ml, .ga, and .cf.[25] This was likely a contributing factor towards the number of web-facing .ga domains reducing from approximately 5.3 million to 2,600 in 2023, coinciding with a reduction in the number of recorded cyber incidents emanating from these domains.[26] As threat actors lose access to low-effort, free domain registration and find their malicious web pages deranked by search engine platforms, they are increasingly likely to seek exploitation of those that already already have a consolidated reputation. There is a roughly even chance that this will lead to increased emphasis placed by threat actors on website compromise attacks, malicious redirects, fake landing pages, and pharming attacks.

Such attacks are predominantly conducted by financially-motivated threat groups. An ongoing brand-impersonation campaign first observed in Q2 2022 leverages thousands of random country TLDs, which are registered months in advance, to impersonate well-known sport brands. Customers visiting these domains are subject to credential stealing, almost certainly used by the threat actor for financial gain.[27]

[24] hXXps://developers.google[.]com/search/docs/essentials/spam-policies
[25] hXXps://securityboulevard[.]com/2023/03/sued-by-meta-freenom-halts-domain-registrations/
[26] hXXps://www.netcraft[.]com/blog/impact-of-freenom-halting-registrations-on-cybercrime/
[27] hXXps://cybernews[.]com/editorial/nike-adidas-massive-scam-campaign/

Industry competitors engaging in sabotage also use SEO poisoning. Malicious advertisements and URL-redirecting is leveraged to land the user on a different, competing webpage. Bots are used to generate fake “clicks”—simulating visits to a website and thereby increasing its search engine ranking—and competing websites are subject to measures that decrease its algorithm credibility, such as link spamming and review bombing.[28]

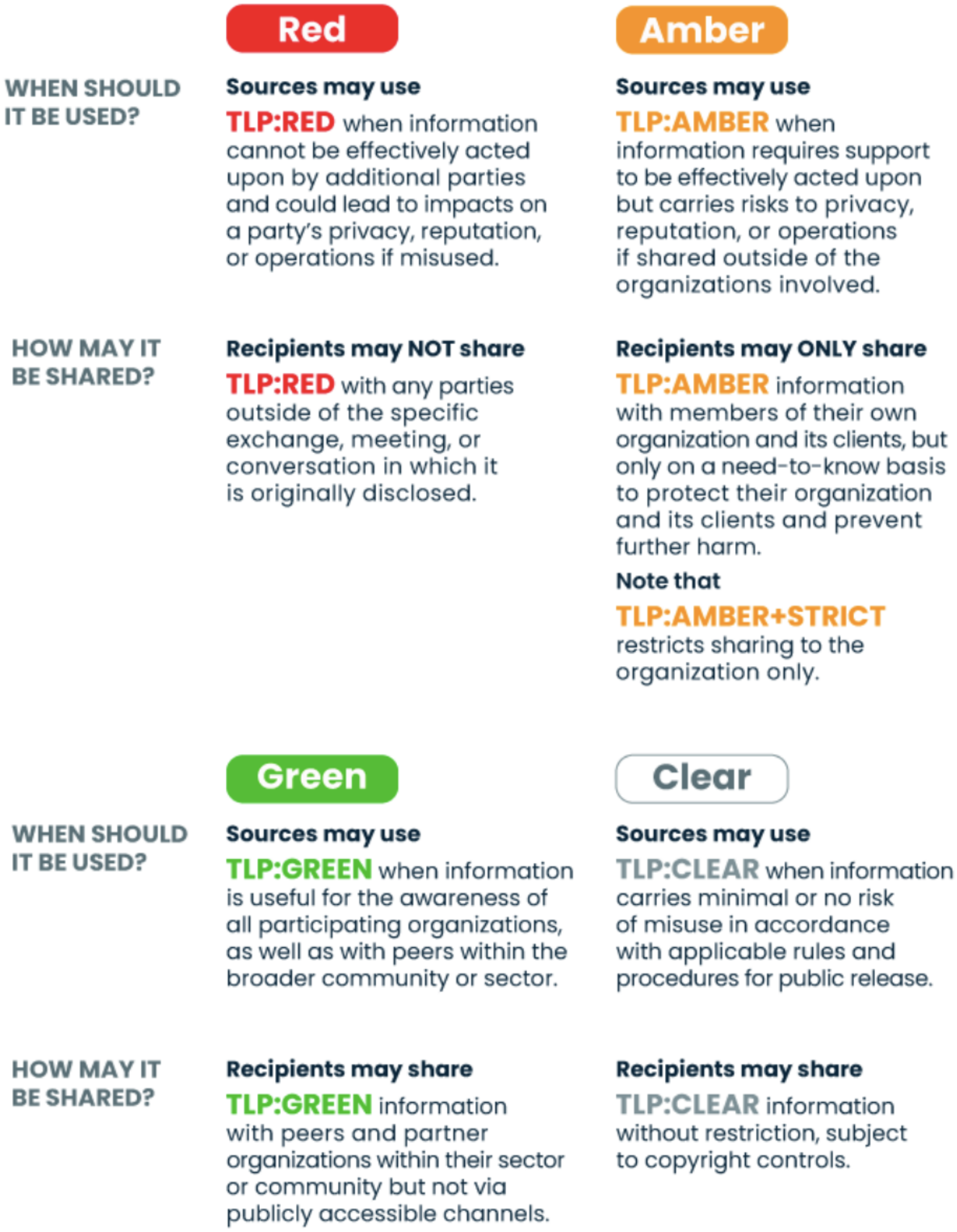
Recommendations

- Develop a comprehensive cybersecurity policy outlining acceptable use of technology, user security procedures (SyOps), credential guidance, audit processes, and data handling procedures.
- Adopt an organization-wide zero-trust cybersecurity architecture, ensuring that access to devices, networks, and information is kept at what is minimally required for operations based upon a principle of least privilege. Continuously test and scrutinize the legitimacy of trust in place.
- Develop a clear and comprehensive incident response strategy consisting of business resilience and continuity plans—including third party services' incident reporting procedures and key authorities.
- Conduct social engineering awareness training programs that educate staff on how to identify phishing attacks, emerging trends, and how personnel should report suspicious incidents.
- Implement secure password policies with phishing-resistant MFA, complex passwords, unique credentials, and the separation of user and privileged accounts.
- Protect remote end-point devices with phishing-resistant MFA protocols compliant with FIDO2 or PKI standards. Introduce WebAuth security with the use of external, physical authenticators. Perform risk assessments to identify high-risk devices, networks, and individuals.
- Restrict accounts with remote access privileges, prohibiting reuse of passwords across accounts.

[28] hXXps://rockcontent[.]com/blog/negative-seo/

- Establish secure configuration baselines for user systems with macros disabled by default.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Ensure all business IT assets are updated with the latest manufacturer software updates and security patches, supported by the implementation of an effective patch management system.

Appendix A: Traffic Light Protocol for Information Dissemination

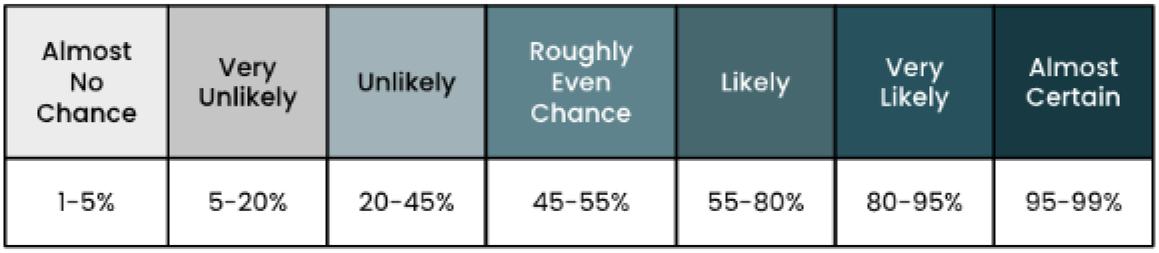


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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 judgements 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 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%