



Brief

Introduction to Social Engineering: MFA Bypass via Phishing

B-2024-03-12a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Social Engineering, Phishing, MFA Bypass

March 12 , 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 0900 AM (EDT) on March 12, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Introduction to Social Engineering: MFA Bypass via Phishing

ZeroFox's Social Engineering series breaks down aspects of the threat into digestible reports and outlines defensive actions that can be taken to combat it. Part Three of this series takes a deep dive into the bypassing of multi-factor authentication (MFA) security protocols, why and how threat actors do it, and how the threat can best be mitigated.

| Key Points

- MFA uptake has been on a consistent upward trajectory since its inception, and today its use is widely expected, considered best practice, and a part of basic cybersecurity hygiene.
- Despite improving security, some MFA protocols are still susceptible to bypass or circumvention by threat actors seeking to gain illicit network access. This type of activity is almost certainly on an upward trajectory as of 2024, as threat actors continuously evolve their techniques, tactics, and procedures (TTPs).

| Multi-Factor Authentication Overview

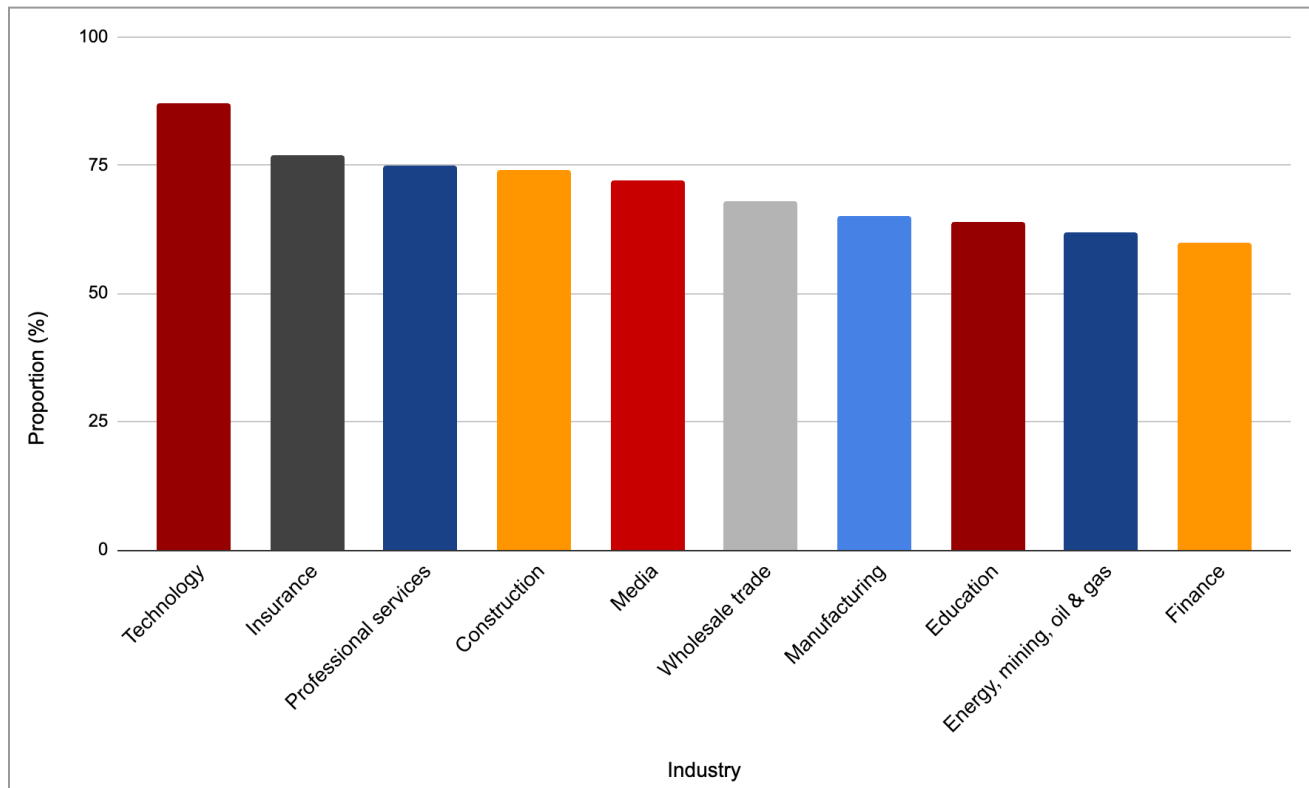
MFA is an evolution of two-factor authentication (2FA)—a manifestation of zero-trust cybersecurity architecture designed to scrutinize the implicit trust afforded to users of endpoint devices. 2FA requires users seeking to access a network to satisfy an identification challenge, in addition to providing a correct username and password. The number of times that a user is confronted by these challenges varies but typically will be one of the following:

- Every time access is requested, offering the highest level of security.
- Upon the detection of anomalies, such as a new log-in device or location.
- Time-sensitive, such as once per day or after periods of inactivity.

While 2FA was almost certainly effective in protecting the attack surfaces of limited, less complex networks, it's consistent improvement has been driven by a number of factors, including:

- The growing competency of cyber threat actors, particularly their increasing proficiency in circumventing or undermining some 2FA procedures.
- The proliferation of smart devices, Internet-of-Things (IoT) components, personal IT devices, and reliance upon cloud computing platforms, all of which introduce additional threat vectors.
- The increasing dispersion and complexity of networks and organizational supply chains, both of which lead to the growth of digital attack surfaces.
- The data privacy and security compliance requirements to which organizations may be bound, providing legal incentive to protect the information of clients and customers.
- A growing public and organizational awareness of cyber threats, leading to higher standards being demanded from third parties (such as software and hardware manufacturers, storage operators, and software-as-a-service providers) to offer the latest MFA solutions.

Technological advancements help to enable this continuing evolution, with tools such as biometric security features becoming widely-available in smart devices and leading to MFA procedures being perceived as less arduous to regularly undertake.



Top 10 industries by MFA adoption rate, 2023

Source: <https://www.okta.com/the-secure-sign-in-trends-report/>

How Multi-Factor Authentication Works

MFA is a broad term that is inclusive of 2FA methods but also accounts for authentication procedures that demand more than two identification challenges, offering an additional layer of security that must be overcome by a threat actor seeking illicit access. These challenges can be broken down into four separate categories. Unlike 2FA, MFA procedures should include challenges from more than one of the below categories.

- Something the user *is*: Biometric information, such as fingerprint, facial, voice, or iris recognition.

- Something the user *knows*: Information such as usernames, passwords, personal identification numbers (PIN), and pre-defined secret questions and answers.
- Something the user *has*: Information in the user's physical possession, such as physical or digital authentication tokens generated from a mobile device, or a time-based one-time password.
- *Somewhere* the user is: The user's geographic location is scrutinized using GPS or IP geolocation.

MFA procedures are also considered to be either in-band or out-of-band. The former refers to a process whereby the identification challenge is presented to the user via the same communications channel that is requesting authentication. Out-of-band MFA refers to processes that use separate communication channels.

- An example of in-band MFA is an SMS message sent to a mobile phone, on which the user is attempting to access mobile banking. In this case, the challenges share both a device and a network.
- An example of out-of-band MFA is the acquisition of a time-based one-time-password (TOTP) from an external app, needed to activate a login session on a separate network. This is widely considered significantly more secure and more likely to prevent MFA bypass attacks such as credential stuffing and keylogging, due to the lesser likelihood that both networks are compromised.

MFA uptake has been on a consistent upward trajectory since its inception, and today its use is widely expected, considered best practice, and a part of basic cybersecurity hygiene.¹ Reporting suggests that approximately 57 percent of organizations globally have implemented MFA—the vast majority of which is software-based and uses third-party applications such as Google Authenticator, Duo Security, or LastPass Authenticator.²

Correctly configured MFA can help protect networks from malicious activity such as phishing, brute-force attacks, SIM swapping, key logging, credential stuffing, and password-reuse attacks.

¹ [hXXps://www.okta\[.\]com/the-secure-sign-in-trends-report/](https://www.okta.com/the-secure-sign-in-trends-report/)

² [hXXps://www.lastpass\[.\]com/-/media/10aa2f653c774e428aa4cc6732734828.pdf](https://www.lastpass[.]com/-/media/10aa2f653c774e428aa4cc6732734828.pdf)

| Multi-Factor Authentication Bypass via Phishing

Although correctly-implemented MFA is significantly more secure than 2FA or a simple name and password, it is still susceptible to bypass or circumvention by threat actors seeking to gain illicit network access via various phishing methods. This type of activity is almost certainly on an upward trajectory as of 2024, as threat actors continuously evolve their TTPs to enable the targeting of an ever-growing proportion of global networks that have implemented MFA protocols.

The malicious techniques leveraged in MFA bypass are becoming increasingly sophisticated, diverse, and able to bypass authentication methods long-considered secure, also varying between technical exploitation attacks and those that heavily rely upon social engineering techniques and the victim's assistance.³⁴ These are some examples of the most commonly used and dangerous MFA techniques that are very likely to be continually leveraged throughout 2024.

Open Authorization (OAuth) abuse. OAuth is an authorization framework that provides legitimate access to resources hosted by other web applications. These accesses are increasingly exploited by threat actors, due to the permissions granted to third-party applications without requiring the user's credentials. Threat actors have been observed consent phishing, by luring victims to fake OAuth login pages and requesting the level of access needed for further exploitation. This can include the delivering of info-stealing malware, social media manipulation, or a full account takeover.⁵

MFA Fatigue. In this method of MFA bypass, threat actors run malicious scripts able to repeatedly attempt to log in to an account using previously stolen credentials. This technique relies upon the account owner becoming fatigued with the process, eventually granting permissions either by accident or to stop the influx of requests. The threat actor may bolster this process by sending spam communications masquerading as an

³ [hXXps://mytechdecisions\[.\]com/network-security/2023-hacking-tactics/](https://mytechdecisions.com/network-security/2023-hacking-tactics/)

⁴

[hXXps://securityboulevard\[.\]com/2023/04/the-art-of-mfa-bypass-how-attackers-regularly-beat-two-factor-authentication/](https://securityboulevard.com/2023/04/the-art-of-mfa-bypass-how-attackers-regularly-beat-two-factor-authentication/)

⁵

[hXXps://www.csoonline\[.\]com/article/573699/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html](https://www.csoonline.com/article/573699/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html)

authority, such as an IT department or equipment manufacturer.⁶ This MFA bypass method is often associated with the now-defunct international threat group LAPSUS\$, which has successfully leveraged MFA fatigue attacks against companies such as Uber and Nvidia.

SIM Swapping. Also known as SIM Hijacking, this is a technique that relies heavily upon social engineering to circumvent MFA processes. To accomplish this, the threat actor must persuade a victim's mobile network provider that they are the legitimate owner of the phone number and that control should be transferred to them via a new SIM card. If this is achieved, the victim can lose access to accounts and data, and the threat actor is able to intercept various communications. These attacks are usually performed in a highly targeted, tailored manner due to the need to conduct victim research and use voice communications to deceive mobile network providers.

Other phishing-enabled MFA bypass techniques used include Clickjacking (the malicious use of an altered interface designed to manipulate the user into unknowingly visiting or accepting something unintended), Keystroke Logging (the capture of authentication codes as they are inputted by the user), and Brute Force (a trial-and-error approach that is largely mitigated by the scrutinization of too many guesses and the short timeframe of many TOTP's).

Although some MFA bypass attack techniques do not directly leverage social engineering, they may have earlier in the attack chain—such as in the gaining of initial network access. Many Man-in-the-Middle (MitM)—sometimes called Adversary-in-the-Middle (AitM), are examples of this. These attacks are a broad range of techniques characterized primarily by a threat actor intercepting communications without the knowledge of a victim with the intent of stealing, altering, or otherwise undermining them. MitM is leveraged to conduct an array of attacks capable of

6

[hXXps://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/](https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/)

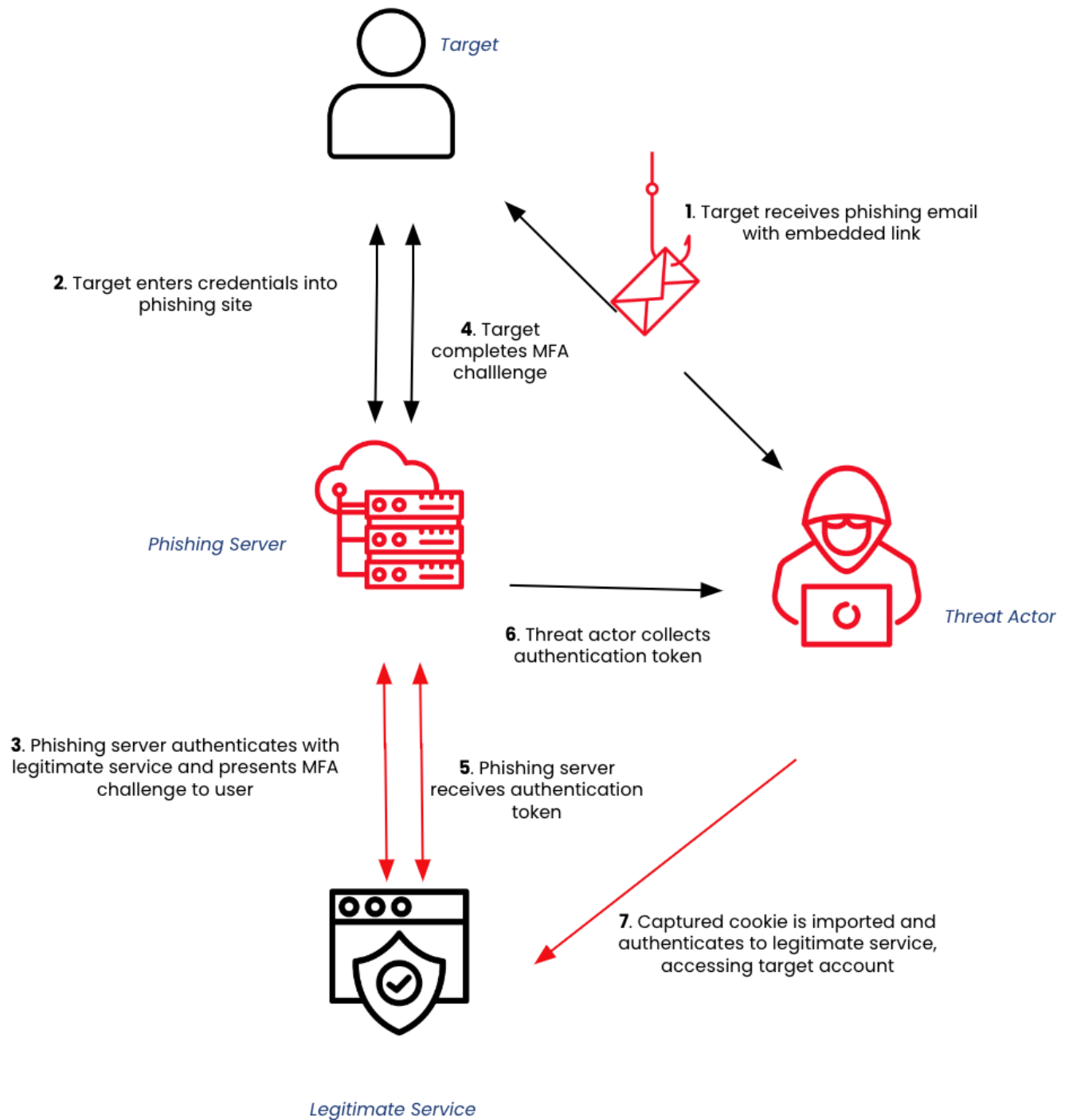
bypassing MFA protocols. These are some of the most prominently observed attack methods leveraged to gain access to a target network in 2023.⁷⁸

- *Session Hijacking (application layer)* are attacks whereby a threat actor gains access to an active session via an open application. These typically exploit fundamental security flaws in the session-management security of open web applications. Examples of techniques used include tabnabbing, sniffing, session fixation, response manipulation, HTTP downgrade, cross-site scripting (XSS), and Man-in-the-Endpoint attacks such as skimming and Man-in-the-Browser (MitB) attacks.
- *Session Hijacking (network layer)/Transport-Layer Hijacking* exploits vulnerabilities in the network's data flow shared by online applications, such as the transmission control protocol (TCP) or the user datagram protocol (UDP). Techniques leveraged by threat actors include DNS and internet protocol (IP) spoofing, address resolution protocol (ARP) spoofing, and blind hijacking.
- In bypassing MFA protocols, threat actors create and exploit new sessions as well as intercept existing ones. This is achieved via token theft, session fixation, or session cloning and can provide the attacker increased control over the session permissions and parameters, ultimately offering greater opportunity for exploitation and detection avoidance.
- Passive Hijacking techniques are also used to circumvent MFA protocols, with malware such as packet sniffers deployed with the intent of capturing information traversing a network. Many of these tools are open source, such as Kismet and TCPDump. Promiscuous modes and proxy servers can also be used passively for similar malicious purposes.

7

[hXXps://www.aon\[.\]com/cyber-solutions/aon_cyber_labs/bypassing-mfa-a-forensic-look-at-evilginx2-phishing-kit](https://www.aon.com/cyber-solutions/aon_cyber_labs/bypassing-mfa-a-forensic-look-at-evilginx2-phishing-kit)

⁸ [hXXps://www.sisainfosec\[.\]com/blogs/best-practices-for-implementing-mfa-to-combat-brute-forcing-attacks/](https://www.sisainfosec.com/blogs/best-practices-for-implementing-mfa-to-combat-brute-forcing-attacks/)



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

Source: ZeroFox Intelligence

| Multi-Factor Authentication Best Practice

While any level of MFA (including 2FA) can provide enhanced security, some best practices have emerged that are recognized by the security industry as the ideal standard for organizations to pursue. The protection and usability offered by phishing-resistant MFA tools that are Fast ID Online (FIDO)-certification level 2 compliant, such as Yubikey and 5C Nano, are among the best available. This is due to a multitude of features such as unique public-private keys for each user that are securely stored on a device or hardware token and generate a cryptographic proof of the user's identity, which is verified by the server when logging in.⁹ FIDO can also be integrated with convenience features such as single sign-on (SSO), which allows users to securely access multiple applications within a single session.

Other MFA methods are likely to be less secure, though they can significantly enhance network security if configured correctly. Those using third-party authentication applications should ensure that TOTP are generated on a separate device and network and secure the application via biometric or password security if possible. Users of these applications should be aware of their potential weaknesses, such as the lack of end-to-end encryption present in many of them.

SMS or email-based MFA should be avoided if possible, as they are no longer considered sufficiently secure to provide protection against contemporary threat actor TTPs. These methods can in some cases be undermined by open source phishing tools such as Modlishka or EvilginX and are likely to become more insecure over time as new, more effective methods replace them.

⁹ <https://fidoalliance.org/specifications/>

Resilience – MFA Bypass

- Organizations of all sizes and industries should implement a company-wide comprehensive MFA policy. Research suggests that while approximately 87 percent of organizations with 10,000+ employees use MFA, only 34 percent of organizations with less than 100 employees do.¹⁰
- Ensure employees receive training covering contemporary social engineering threats and the importance of correctly using MFA tools.
- As the most secure form of MFA, physical authentication devices should be used where possible. Devices such as USB and public key infrastructure (PKI) keys are the least susceptible to interception, tampering, or compromise.
- If TOTP MFA is to be used, it should utilize an out-of-band communication and challenge users for something they **are** (biometric), alongside at least one other challenge from a different category.
- SMS and email-based MFA should not be used. It is the least secure and susceptible to interception and bypass, even if correctly configured.
- MFA challenges should be as regular as possible, without causing significant disruption or the frustration likely to lead to misuse.
- Implement a password policy mandating that passwords are at least 12 characters long and consist of upper and lowercase letters, numbers, and special characters. Passwords should be regularly changed and never reused.
- Maintain a principle of least trust by ensuring access is continuously scrutinized and adjusted and implementing identity and access management (IAM) solutions along with network segmentation.
- Safeguard classified, sensitive, or business-critical assets using secure, off-site backup methods, compartmentalization, and authentication mechanisms.
- Where possible, monitor logs provided by MFA tools to identify suspicious activity.
- Ensure IT assets, software, and MFA tools are updated with the latest original manufacturer security patches.

¹⁰ [hXXps://www.lastpass\[.\]com/-/media/10aa2f653c774e428aa4cc6732734828.pdf](https://www.lastpass.com/-/media/10aa2f653c774e428aa4cc6732734828.pdf)

| Outlook

In response to increasing cybersecurity awareness and an evermore dynamic threat landscape, MFA uptake is very likely to continue accelerating globally across organizations of all industries and sizes. This will almost certainly be part of broader movements toward zero-trust network security architecture, which will increasingly be considered necessary as a part of basic cyber hygiene. MFA protocols are also very likely to be increasingly mandated at legislative levels, starting with government-associated departments before becoming inclusive of more heavily-regulated industries such as manufacturing, finance, insurance, and energy.

To encourage their use, MFA developers will focus on providing protection from commonly leveraged bypassing techniques while implementing features aimed at convenience, such as SSO and biometric sign in. In response, threat actors will almost certainly continue to evolve and enhance their attack methods, leveraging topical lures to target the network's human element in efforts to circumvent MFA-hardened security edges.

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%