



| Brief |

Social Engineering Series: Non-Email Phishing

B-2024-02-22b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Social Engineering, Phishing

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: Non-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 Two of this series is a deep dive into the non-email, alternative communication methods that threat actors leverage to conduct phishing attacks.

Key Points

- Numerous different communication methods are used in phishing attacks, enabling threat actors to conduct highly-bespoke campaigns targeting specific individuals, organizations, industries, or regions.
- Threat actors leverage voice phishing, SMS phishing (aka smishing), QR Code phishing and USB phishing as alternative delivery methods to email phishing. Each of these offers the attacker unique opportunities, strengths and weaknesses.
- The methods adopted by threat actors conducting phishing attacks will continue to evolve alongside the communication channels used by individuals and organizations and will adapt in response to increased public awareness of contemporary threats, modern security protocols, and the fundamental ways that people interact with technology.

| Non-Email Phishing

Threat actors leverage an array of different communication methods when carrying out phishing attacks, each enabling the attacker to target different audiences and best-leverage contemporary themes that are designed to demand the victim's attention. The TTPs observed during phishing attacks are somewhat indicative of several factors, such as the attacker's sophistication, the level of initial research conducted (and thereby the extent of personalized targeting), and the desired end state.

While email is almost certainly the most commonly leveraged means of communication leveraged in phishing attacks, other methods are often used.

Voice Phishing

Voice phishing, also known as vishing, is the use of methods that allow the attacker to directly and immediately communicate with the victim via spoken communications. Telephone is almost certainly the most commonly-deployed method to achieve this, though Voice over Internet Protocol (VoIP) technologies such as Skype and WhatsApp are also used. Threat actors using vishing can exploit the following advantages:

- *Defense Bypassing*: Using telephone communications can allow the attacker to bypass defense protocols that may scrutinize and prevent malicious emails, such as Secure Email Gateway (SEG) security measures.
- *Low Resource Investment*: Vishing attacks can take place using only a telephone, with little requirement for further hardware, technical knowledge, or detailed information about the potential victim.
- *Human Interaction*: Vishing allows the attacker to exploit fundamental human tendencies with manipulation. Threat actors may leverage the subconscious trust present during many human interactions, as well as the immediate pressure of a phone call, to coerce the victim towards misguided, ill-conceived decision making.
- *Adaptability*: In contrast to other phishing methods that may rely upon a predetermined template or script, vishing allows the threat actor to adapt and respond to the victim's response and demeanor in real time. However, this could

also prove to be a major hurdle for the threat actor depending on their general preparedness for the vigilance of the victim.

Resilience – Voice Phishing

- *If the caller is unknown and unexpected, end the call and contact the organization via a phone number from its official website.*
- *Verify the identity of the caller. Legitimate organizations will expect this scrutiny and should offer sufficient verification.*
- *Attackers immediately pose security questions to increase their authenticity. Do not divulge personal information until the caller's identity has been verified.*
- *Do not call a different number upon the caller's request. This number could be spoofed to increase its legitimacy.*
- *Identify if pressure or scare tactics are being employed. Threat actors will almost always convey a fictitious scenario that urges prompt action by the victim. This can go as far as threatening fines, particularly if the attacker is mimicking a government department employee.*
- *Remember that legitimate organizations will not ask for personal information over the phone—or will at least offer an alternate, more secure means if requested.*

Short Message Service Phishing

Short Message Service (SMS) phishing (aka smishing), whereby a threat actor uses text messages to conduct an attack, is known as smishing. Like other types of phishing, the attacker usually claims a false authority, using social engineering methods while urging the victim to either divulge sensitive information or access an included, malicious link. Despite being vulnerable to disruption at the cellular network-provider level, smishing attacks increased significantly over recent years, very likely due to the abundance of topical lures available to use as leverage. Some of the key advantages of using SMS messaging in phishing attacks are:

- **Wide Reach:** Similar to email phishing, smishing offers a threat actor the ability to conduct a large number of attacks over a short period of time—and with minimal

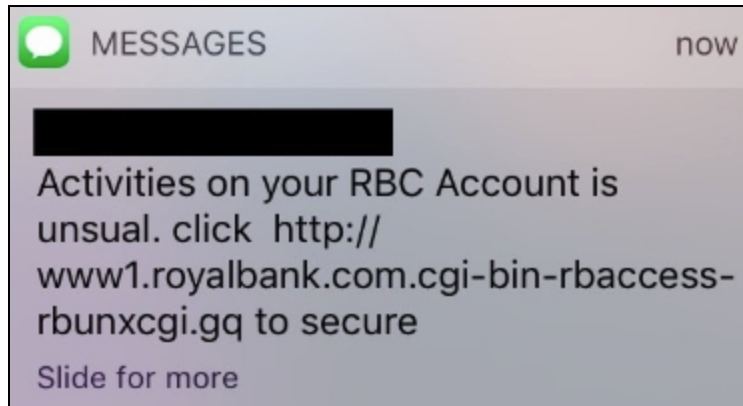
effort. This makes it an efficient option in conducting low-risk, low-payoff attacks. However, the threat actor is somewhat limited by restricted character counts.

- *Applications:* Instant messaging (IM) applications such as Whatsapp, Viber, Skype and Telegram are also being increasingly used in smishing attacks. The growing popularity of these applications has led to their implication in phishing attacks, the facilitating of bot accounts and the hosting of phishing-focused support groups for threat actors.
- *High Engagement Rate:* Mobile phones are usually significantly more reachable than emails—particularly corporate email accounts, which are often only accessible in work environments. Research suggests that text messages are opened at five times the rate of email, with subsequent clickthrough rates also higher.¹
- *SMS Spoofing:* Threat actors are able to increase the perceived authenticity of text messages by impersonating an individual or organization, which carries more credibility than an unfamiliar number. This can be achieved by changing, or “spoofing,” the sender's name or phone number and ultimately increases the chance of the message being opened, malicious instructions being followed, and any enclosed payload being delivered.
- *Perceived Authenticity:* Most people are much more accustomed to unwanted email messages, whether marketing-related or malicious phishing emails, than they are SMS. With up to 50 percent of global emails sent daily considered “junk mail” (compared to 10 percent of SMS messages), victims are more likely to view a text message received on a mobile phone as authentic.²

¹ [hXXps://blog.clicksend\[.\]com/text-messaging-statistics/](https://blog.clicksend.com/text-messaging-statistics/)

²

[hXXps://www.reach-interactive\[.\]com/resources-and-blog/sms-marketing-statistics/#:~:text=5,being%20viewed%20is%20much%20higher.](https://www.reach-interactive.com/resources-and-blog/sms-marketing-statistics/#:~:text=5,being%20viewed%20is%20much%20higher.)



SMS phishing attempt masquerading as a Microsoft security notification

Source: [hXXps://www.malwarebytes\[.\]com/blog/news/2017/03/sms-phishing-for-the-masses](https://www.malwarebytes.com/blog/news/2017/03/sms-phishing-for-the-masses)

Resilience – SMS Phishing

- *Deny an attacker's reliance upon the victim's engagement or curiosity. If an SMS message seems suspicious, do not engage.*
- *Ensure security software is installed and updated on mobile devices, blocking malicious communications and preventing the execution of harmful payloads.*
- *Be aware of Multi-Factor Authentication (MFA) Phishing. Attackers attempt to steal MFA tokens or verification information either by direct interception or by directing the victim toward a malicious web page.*
- *Be aware of enticements that may promise the victim some form of reward for following an included hyperlink.*

QR Code Phishing

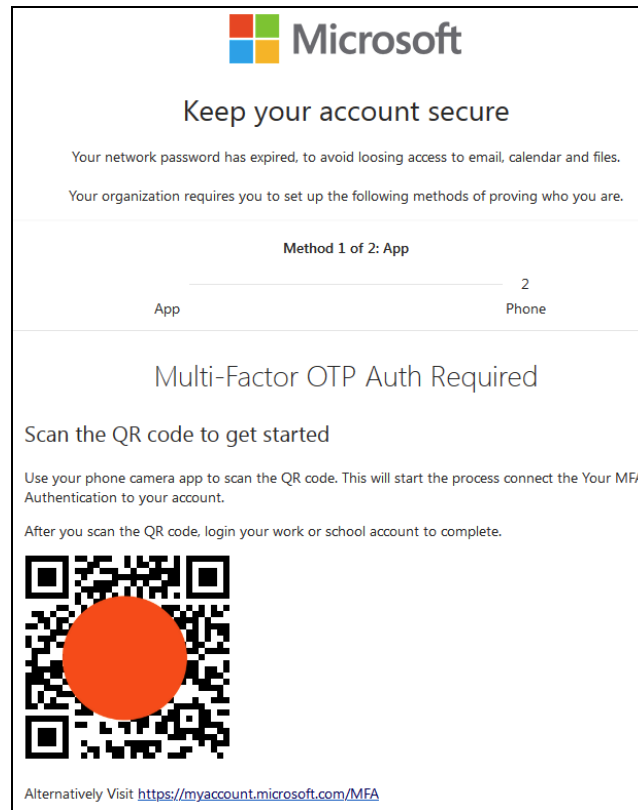
Over the past few years, the use of Quick Response (QR) codes in phishing attacks has increased significantly, aided by the widespread accessibility to camera phones and mobile phone utility. This has subsequently resulted in their leveraging during phishing attacks; threat actors socially engineer a victim into accessing a malicious QR code, believing it to be legitimate, and then guide the victim to a falsified webpage, leading to further exploitation. These types of attacks are known as quishing and have increased

significantly since the first widespread campaign was discovered in 2023.³ Some notable advantages of quishing over other types of phishing include:

- *Novel Nature*: Compared to other older, more established phishing methods, the threat posed by quishing is relatively new. This almost certainly means that attackers leveraging this technique are less likely to encounter resilience, either at the individual or organizational level.
- *Distribution*: Threat actors are able to implement malicious QR codes in a variety of ways. They can be implemented into fabricated situations, such as embedding them within an email masquerading as a security notification from Microsoft. They have also been used to replace legitimate QR codes in hard copy. This involves the threat actor simply removing or covering the legitimate code with a malicious replacement, leveraging implicit trust between the victim and the service with which they are seeking to interact.
- *Evasion*: Using a wide array of distribution methods, threat actors are able to avoid many of the defense measures that may mitigate email phishing and smishing attacks, such as SEGs and the multitude of smishing detection methods used by cellular network providers.

3

[hXXps://www.bleepingcomputer\[.\]com/news/security/major-us-energy-org-targeted-in-qr-code-phishing-attack](https://www.bleepingcomputer.com/news/security/major-us-energy-org-targeted-in-qr-code-phishing-attack)



Quishing attempt, masquerading as a Microsoft security notification

Source:

[hXXps://perception-point\[.\]io/blog/qr-code-red-quishing-attacks-and-how-to-prevent-them/](https://perception-point[.]io/blog/qr-code-red-quishing-attacks-and-how-to-prevent-them/)

Resilience – QR Code Phishing

- Verify the URL associated with the QR code (usually by holding the camera in place). Do not open the link if it appears to lead to an unexpected destination.
- Be aware of the QR code-scanning application being used, the information it may share with third parties, and the security features that may or may not be included.
- If the QR code is enclosed within an email, conduct a vigilant check of the rest of the content, such as the sender address, logos, and general grammar.
- If the QR code is in a public place, search for any signs of tampering.
- Enable MFA protocols on mobile devices, if possible.

USB Phishing

Incidents of USB phishing have increased significantly over recent years—often as a part of cyber espionage campaigns that target industries associated with sensitive, proprietary information. This targeted method of phishing requires higher effort and prior research by the attacker and involves using a USB storage device to gain immediate access to a target network via an unknowing victim of social engineering. Some advantages of this attack vector are:

- *Targeting Versatility:* USB phishing can be leveraged as part of an attack targeting a specific individual, organization, or demographic by planting the device in a location that increases its likelihood of being introduced to a target network. This could include public facilities, office environments, or even in the place of a legitimate USB device.
- *Payload Diversity:* Leveraging the immediate network access potentially granted, a large range of subsequent malicious payloads can be delivered to the target network. This includes data-stealing malware or ransomware that can encrypt files. In the case of Human Interface Device (HID) spoofing attacks, software can also grant the attacker remote access to the network, enabling further, subsequent attacks.
- *Access:* USB Phishing can be adopted by threat actors seeking access to an encrypted, segmented, or compartmentalized network, which is usually associated with those containing sensitive or protected information. Many other phishing methods rely on external network connection, such as the internet, for attacks to take place. However, secured networks are often connected only to internal, or air-gapped, networks. This can also assist the attacker in bypassing many of the usual network security protocols, many of which operate in the network and transport layers.

Resilience – USB Phishing

- *Prohibit the use of unknown drives being connected to organizational networks. Ensure the appropriate authority is notified in the event of a breach.*
- *Be aware of the dangers posed by malicious USB devices. Threat actors leave them in deliberately-convincing locations or even send them in the mail while masquerading as a tech manufacturer.*
- *Disable autorun features on devices to prevent any malicious software from automatically executing.*
- *If a USB device is suspicious, operate its contents in a safe virtual sandbox.*

Outlook

The methods adopted by threat actors conducting phishing attacks will continue to evolve alongside the communication channels used by individuals and organizations and will adapt in response to increased public awareness of contemporary threats, modern security protocols, and the fundamental ways that people interact with technology.

It is very likely that initial financial cost will continue to be a primary consideration for threat actors when choosing a communication method by which to conduct phishing attacks. As the cost of such technology varies across the world and is constantly changing—for both the attacker and victims—threat actors must carefully consider the cost-to-payoff ratio of their campaigns. Threat actors are very likely to continue “hijacking” ongoing, legitimate communication channels, exploiting the victims’ familiarity with licit institutes as a means to encourage their engagement with malicious content.

| 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%