Mishing Solution Brief

Defending Against Mobile Threats in the Enterprise

ZIMPERIUM®

The Challenge: A Mobile-First Attack Strategy

Cybercriminals are increasingly targeting mobile devices and applications within enterprises as a first-strike option for penetrating security defenses, corporate networks and sensitive data. The massive casino attacks in 2023 are one example where voice calls (vishing) were used as an initial attack method, leading to credential theft and significant business interruption and data loss. By combining social engineering tactics with mobile-specific features like voice calling, text messages, the camera, as well as corporate email, attackers are finding users more vulnerable than ever. Mobile devices present a large attack surface, which is exacerbated by the fact that many lack proper security solutions.

Collectively, these tactics contribute to what is now referred to as **"Mishing"** – a broad spectrum of mobile-targeted phishing attacks that exploit mobile devices and applications to steal sensitive information and penetrate corporate networks. While mishing affects both consumers and organizations, its implications for enterprises and the public sector are serious. Understanding the unique risks associated with mishing is critical to protecting corporate and public data, as well as maintaining overall mobile security.

WHAT IS MISHING?

Mishing involves the targeting of mobile devices via email, text message, voice call or QR codes, exploiting vulnerabilities in mobile environments, including unsafe user behavior as well as minimal security on most mobile devices.

Common Mishing Tactics

Mobile-targeted Email Phishing

This attack is launched via a standard email message but only executes the attack when a link (or attachment) is clicked by the user from a mobile device. If clicked from a standard endpoint device such as a laptop, the attack is aborted and the user is taken to a safe page such as Google.com.

Smishing

Smishing is a targeted phishing attack that is delivered by text/SMS. Deceptive SMS messages lure victims into clicking on malicious links or sharing sensitive data. This type of attack has become more common as cybercriminals have seen success in duping users into unknowingly downloading malware to their device.

Vishing

Vishing is a voice-based attack used to trick users into taking unsafe follow-on actions on the device or revealing confidential information, such as passwords. Often, it serves as an entry point to other attacks, such as smishing.

Quishing

Quishing uses mobile cameras to deliver phishing attacks via malicious QR codes, exploiting users' trust in QR codes to redirect them to phishing sites or malware.

Why Mishing is a Growing Threat for Organizations

Several factors contribute to the increasing prevalence of mishing among enterprises and public sector organizations:

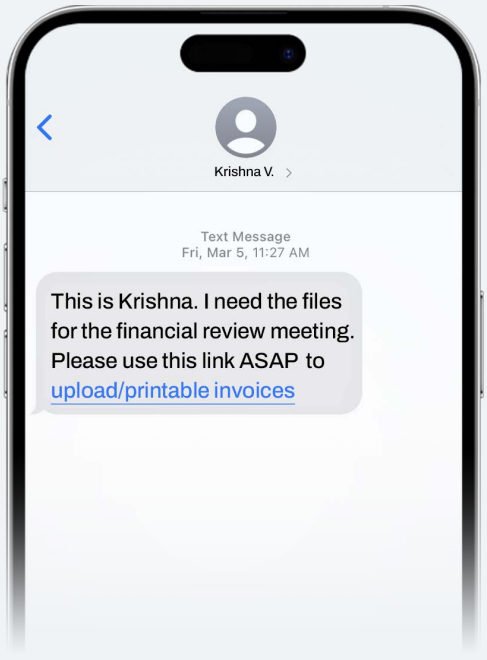
- **Increased Mobile Usage:** Cybercriminals target the vast pool of mobile device users within enterprises, taking advantage of smartphones' widespread use for communication, data access and collaboration.
- **Remote Work on Personal Devices:** The shift to remote work has led to a greater reliance on mobile devices, with employees often using their own personal mobile devices to access corporate networks and sensitive information. As a result the attack surface has increased for cybercriminals.
- **Expanded Access to Sensitive Data:** The rise of cloud-based apps means more corporate and public sector data is being accessed via mobile devices, heightening the risk of exposure from mishing attacks includes credential theft and even hijacking of one-time-passwords (OTP).
- **False Sense of Security:** Many users and organizations consider mobile devices to be more secure than desktops and laptops, leading to careless behavior when handling suspicious messages or links.
- **Limited Security Measures:** The majority of mobile devices are not protected by a mobile threat defense solution, making them extremely susceptible to mishing and other sophisticated attacks.

How to Protect Against Mishing

To safeguard against mishing, enterprises and public sector organizations should adopt the following best practices:

User Best Practices

1. **Be Skeptical of Mobile Messages:** Treat unsolicited messages with caution. Verify the legitimacy of the sender before responding or clicking on any links to prevent unauthorized access to sensitive information.
2. **Avoid Clicking on Unknown Links:** refrain from clicking links from unknown or unverified sources. Instead, manually enter the URL into your browser to ensure you are visiting a legitimate site and safeguarding corporate data.
3. **Exercise Caution with QR Codes:** Be wary when scanning QR codes from even trusted sources. Always review the destination URL before proceeding to minimize exposure to phishing sites.
4. **Maintain Updated Software:** Regularly update device operating systems and applications to patch known vulnerabilities and protect against new threats.



Organizational Best Practices

1. **Deploy Comprehensive Mobile Threat Defense:** Utilize advanced mobile security solutions that provide real-time mobile threat protection for both known and zero-day threats, blocking malicious activities such as dangerous links, attachments or malware downloads before they can compromise the user and the device.
2. **Implement Mobile App Management:** Ensure that all applications used within the organization are properly vetted for vulnerabilities, including 3rd-party and in-house developed apps. Enforce policies to identify and block apps that request suspicious or excessive permissions that may compromise security.
3. **Educate Employees:** Organizations should provide regular training on recognizing and avoiding mishing attempts. Employees should be aware of the risks and know how to handle suspicious messages.

Mishing is an insidious and increasingly common attack vector in today's mobile-centric world, particularly for enterprises and public sector organizations that rely on mobile devices and apps for remote work and access to sensitive information. By understanding the nature of mishing and adopting proactive mobile security measures, organizations can better protect their critical information from cybercriminals. Zimperium Mobile Threat Defense helps reduce enterprise risk and protects against mishing by scanning all URLs contained in emails, text messages and QR codes to break a phishing attack chain.

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank. Learn more at **www.zimperium.com** and connect on LinkedIn and X (@Zimperium).

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244