

Mishing and Executive Impersonation Protection







www.zimperium.com



Today's Mobile Threat Landscape

With attackers pivoting to a mobile-first attack strategy, mobile phishing has grown to a broader category known as *mishing*¹ that encompasses four attack vectors, all of which take advantage of the unique features of mobile devices that differentiate them from personal computers running either the Windows or Mac operating systems. These features and the corresponding attack vector are:

MOBILE DEVICE FEATURE	ATTACK TECHNIQUE
 Text Messaging (SMS)	Smishing
 Camera with QR code feature	Quishing
 Voice based phishing	Vishing
 Mobile Email client	Mobile targeted Email Phishing

Attackers have chosen a “mobile-first” attack strategy because mobile devices are mostly unsecured and they are the devices most commonly used to provide two-factor authentication access to data and networks. In 2023, 82% of phishing attacks seen by Zimperium labs specifically targeted mobile devices.²

The Executive Impersonation Challenge

Executive Impersonation has become more and more common. Employees can receive messages from what appears to be an executive asking for an action to be taken, usually financial, via an email or text message. This is just a different application of Smishing and Mobile targeted email phishing with a social engineering overlay of the employee appearing to be contacted by the CEO or other executive to create a sense of urgency. In the last two years, these messages have become more believable and human-like due to the use of artificial intelligence. For voice-based phishing (vishing), sophisticated AI is able to mimic a human voice conversation that is believable to the intended victim.



Security Challenges with Executive Impersonation via a Mobile Device

Employee training to recognize phishing is less effective on mobile devices because the details that are more easily visible on a laptop or desktop email client are harder to access and view on a mobile device. Similarly, on a phone, the user may not know the phone number of the sender. However, the urgency of the sender claiming to be an executive combined with a URL often causes the employee to opt for action and click on the link without thinking before acting.

Some vishing or smishing messages can leverage technology to fake the incoming number to make it appear legitimate to the recipients. There are readily available apps,³ marketed for amusement, to fake a caller's identity. It is easy to imagine the same approach being leveraged for criminal purposes.

Challenges and Zimperium Protections

Mishing:

Mobile email phishing and Smishing

Phishing URLs contained in a spoofed email or unfamiliar text sender can trick an employee into leaking sensitive data, login credentials, or be the first step in a larger attack.

Zimperium Protection

Zimperium phishing protection leverages a database of known phishing URLs, coupled with classifiers to identify and provide AI powered zero day protection against phishing attempts via text (smishing), as well as all other mobile mishing techniques. Coupled with the native features in both iOS and Android to filter messages to only known senders named in your contacts list, which can be synched with the corporate directory, robust executive impersonation protection is delivered by Zimperium MTD.

Protection without Compromising Privacy

Phishing protection and Executive impersonation protection needs to be provided without compromising device owner privacy by performing all functions on device without sending personal data to the cloud, particularly on a user-owned device.

Zimperium Protection

With a privacy-by-design approach, Zimperium MTD's detections, including smishing protections, are done on-device, so that private information is never sent to the cloud.

About Zimperium

Zimperium has helped thousands of enterprises and government agencies around the world to successfully employ a mobile-first security strategy—and we're here to help your organization do the same.

Please feel free to [contact us](#) if we can help your team advance its mobile-first security strategies.

Sources

¹ <https://www.zimperium.com/blog/mishing-the-rising-mobile-attack-vector-facing-every-organization/>

² "2024 Global Mobile Threat Report", Zimperium Labs.

³ <https://apps.apple.com/us/app/fake-call-me/id1528244199> and
https://play.google.com/store/apps/details?id=com.unit.fake.call&hl=en_US&pli=1



Learn more at: [zimperium.com](https://www.zimperium.com)
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244

© 2024 Zimperium, Inc. All rights reserved.