ivanti

Stay Safe from Mishing Attacks

"Mishing" or mobile phishing attacks are malicious actors' most common tactics to breach your mobile ecosystem. How wide is this threat vector? Mishing easily impersonates actions mobile users engage in regularly.

4 Common Mishing Schemes:

Mobile email phishing

The most commonly known tactic arrives in the form of a routine email. Because users believe that mobile devices are less vulnerable, they're more willing to click embedded links or open attachments.

Vishing

Mobile devices are also our telephones. When a call comes in, users may be more likely to give out personal information, which threat actors may record to impersonate the user to gain access to personal or sensitive information.

Smishing

These attacks arrive in the form of texts or SMS. Like email phishing, cybercriminals might impersonate a known contact asking for help with information or send a link suggesting the recipient needs to review. What actually happens is the cybercriminal installs malware onto the device, exploiting users' information.

Quishing

QR codes are a handy way to directly link to content without manually keying in a URL. Cybercriminals may overlay a replacement QR code on otherwise-legitimate signage. Users may not even know they are scanning a link to ransomware or other harmful content.

5 Reasons Mishing is on the Rise:

1. **Ubiquitous mobile use:** It's a mobile-first world, with an ever-growing portfolio of apps at our fingertips.
2. **Using personal devices for work:** Blended work and personal use catch users off-guard during off-hours.
3. **Personal apps introduce risk:** Users don't consider personal apps and browsing can unlock access to corporate systems.
4. **Security misconceptions:** Users believe mobile operating systems and app stores are inherently more secure.
5. **Confusing management with security:** Mobile device management (MDM) offers important policy and access control, but zero-day threats and mishing risks remain.

Ivanti Mobile Threat Defense increases defenses against mishing, zero-day and ransomware threats. And when integrated with Ivanti Neurons for MDM, you can deploy without any end-user interaction, helping you reach 100% user adoption. It's time to take mobile security more seriously.

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit www.ivanti.com.

Request a demo

ivanti

For more information, or to contact Ivanti, please visit www.ivanti.com.