Lookout

Five Ways Employees Can Be Phished on Mobile

Mobile threats are the new way into the enterprise

Your employees know how to spot phishing attempts on PCs, but it's much more difficult on mobile devices. With countless channels to socially engineer mobile users, malicious actors can surprise us where we least expect it.

1. SMS and iMessage

2. 3rd Party Messaging Apps

3. Social Media Platforms

4. Email and Productivity Suites

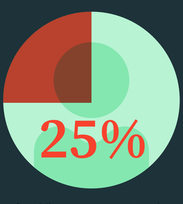
5. QR Codes

4,000,000

mobile phishing attacks were prevented by Lookout in 2023

A successful phishing attack grants attackers access to everything.

Employee identities are the keys to data stored in the cloud. Threat actors target mobile devices to steal credentials, bypass MFA solutions, and quietly gain access to your data.



of mobile users encountered multiple phishing attacks in 2023

of enterprise employees tapped at least six phishing links in 2023

Mobile phishing attacks don't just steal credentials.

A lot of malicious websites try to steal credentials. Others deliver malware or exploit a vulnerability to gain access to the device itself. Some even do both.

48%

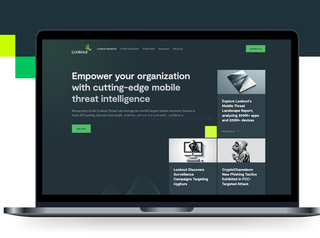
of malicious sites intend to deliver malware or exploit vulnerabilities.

Real World Threat: CryptoChameleon

Lookout researchers discovered an advanced phishing kit exhibiting novel tactics to target government and enterprise organizations via mobile devices. This kit enables attackers to:

- Build carbon copies of single sign-on (SSO) pages
- Use a combination of email, SMS, and voice phishing to deceive targets
- Steal usernames, passwords, password reset URLs and photo IDs.

To learn more about CryptoChameleon and threats like it, visit the Lookout Threat Lab.



Lookout