Why enterprises need to protect against mobile phishing

Mobile users are three times more likely to fall for phishing scams, according to Lookout. In fact, 56% of users received and tapped a phishing URL on their mobile device. These users tapped an average of six phishing URLs on their devices over the course of a year.

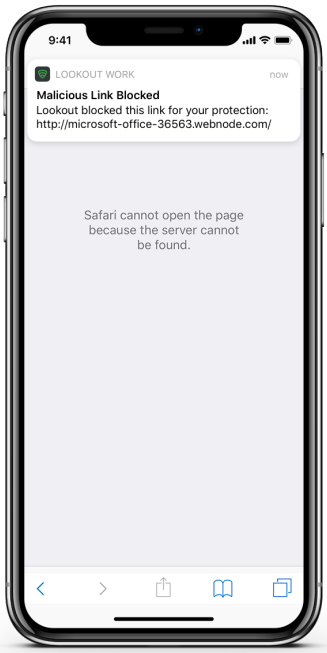
3x Enterprise users are three times more likely to fall for a phishing link when on a small screen than when using a desktop OS.

If an attacker is successful in tricking a user into providing corporate credentials, the attacker can then gain access to corporate systems and move unchecked through your infrastructure and your data.

How Lookout protects against phishing attacks

Lookout Phishing and Content Protection, a comprehensive feature in Lookout Mobile Endpoint Security, is designed to protect enterprises from phishing attacks from any channel, including email (corporate or personal), text messages, messaging apps, and URLs embedded into apps.

Lookout inspects all outbound connections made by the mobile device and installed apps at the network level when a user attempts to connect. What is different about this approach is that it does not rely on inspecting message content, and therefore does not violate end-user privacy. Lookout correlates the URL being accessed against known malicious URLs identified by the Lookout Security Cloud and alerts the end user if it is malicious prior to the connection being completed. This real-time alert prevents exposure to risky content such as malicious apps or websites with known vulnerabilities.



Through the Lookout console, admins can block users who are attempting to make connections on mobile to known malicious URLs hosted on risky websites that may attempt to extract credentials.

Malicious URLs include ad fraud, botnets, command and control centres, compromised and links to malware, malware call-home, malware distribution points, phishing/fraud, spam URLs, and spyware.

This feature is not enabled on Lookout Mobile Endpoint Security by default. An administrator must turn on Phishing and Content Protection in the console and the end user must grant the necessary permissions on the device.

Admins can also opt to warn users of risky websites before proceeding. If Phishing and Content Protection is disabled on a user's device, admins have the ability to mark the device as being out-of-compliance until protection is turned back on.

Why Lookout

Extend your phishing protection to mobile by adding a powerful line of defence against phishing attacks across personal email, texts, messaging platforms, and apps.

Accelerate digital transformation by confidently embracing the use of mobile devices for work and protecting against malicious content whether the employee is inside the protected corporate network or not.

Comprehensive protection at scale across the entire spectrum of mobile risk including the web and content threat vector, one of the most prevalent mobile vectors used by attackers to exfiltrate enterprise data.

The Lookout Difference

- Lookout has amassed one of the world's largest mobile security datasets due to our global scale and mobile focus. Lookout has collected security data from over 170 million devices worldwide and over 70 million apps, with up to 90,000 new apps added daily.
- This global sensor network enables our platform to be predictive by letting machine intelligence identify complex patterns that indicate risk. These patterns would otherwise escape human analysts.
- Mobile is a new era of computing and requires a new era of security solution designed exclusively for this platform. Lookout has been securing mobility since 2007 and has expertise in this space.

Lookout empowers your organisation to adopt secure mobility without compromising productivity by providing the visibility IT and security teams need. To learn how you can secure your mobile fleet today, visit lookout.com/uk.