Lookout

Mobile Threat of the Month

April 2025

Mobile Phishing: iOS Users Targeted Twice as Often as Android

Lookout

Mobile Threat Landscape Report: 2024 in Review

In April, Lookout published its annual Mobile Threat Landscape Report, offering an in-depth review of 2024's most significant mobile security trends. The report analyses key threats, including mobile phishing campaigns, newly discovered malware strains, exploitable vulnerabilities in iOS and Android ecosystems, risks stemming from device misconfigurations, and the growing use of AI by threat actors to enhance their attacks. These findings provide critical insights into the evolving challenges facing mobile security and the tactics employed by malicious actors.

Analysis by Lookout Threat Lab researchers revealed alarming trends, underscoring the need for proactive mobile security measures. Among the most striking findings, data showed that iOS users encountered twice as many phishing attacks as Android users, a stark contrast to conventional security assumptions. Highlighting the evolving sophistication of mobile threats and the importance of multi-platform vigilance in cybersecurity.

Why iOS users are more heavily targeted by phishing:

1. Access to corporate data

iOS is a more lucrative target for attackers as it is the mobile operating system of choice for most enterprise organisations. This is largely due to the complexity of an Android-heavy environment, which results in managing multiple device manufacturers and maintaining a more open mobile ecosystem.

2. iOS is not natively secure

Contrary to popular belief, iOS devices are not immune to cyber threats. While Apple's ecosystem includes robust built-in protections, these safeguards offer little defence against external risks like phishing. Attackers increasingly target iOS precisely because users and organisations assume it requires no additional security, making it a vulnerable and high-value attack surface.

3. Phishing can target any app

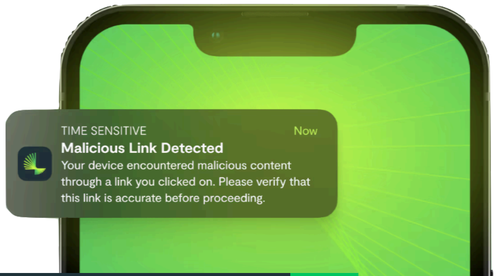
Unlike malware, which depends on exploiting operating system vulnerabilities, phishing attacks operate through web-based deception. As these scams are delivered via messaging platforms, accessible on any device, iOS users face the same level of risk as Android users. The attack surface isn't defined by the device's OS, but rather by the apps and services that facilitate communication.

Does that mean Android users are less at risk?

While iOS users face heightened phishing risks, Android devices remain more vulnerable to broader mobile threats. Lookout's research reveals that the top five most prevalent malware families exclusively target Android systems. Additionally, the platform's fragmented ecosystem leads to widespread use of outdated operating systems, leaving devices exposed to both known and zero-day exploits. This combination of prevalent malware and delayed security updates creates a significantly larger attack surface for Android users compared to their iOS counterparts.

Lookout Mobile Security

Lookout enables organisations of all sizes to stay ahead of modern-day cyber attacks by adopting a security strategy that safeguards iOS, Android and ChromeOS mobile devices. Lookout's extensive AI-driven dataset encompasses data from over 220 million devices, 375 million apps, and billions of web items to pinpoint and prevent mobile threats accurately.



TIME SENSITIVE Now

Malicious Link Detected

Your device encountered malicious content through a link you clicked on. Please verify that this link is accurate before proceeding.