Lookout

Critical Mobile Phishing Trends

Key findings from our annual Global State of Mobile Phishing Report

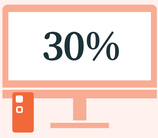
Mobile phishing is one of the most common ways for attackers to steal employee login credentials. Remote work and the popularity of bring your own devices (BYOD) have dramatically increased the frequency of such attacks. As a result, the number of employee phishing victims is rising at an alarming rate.

View Full Report

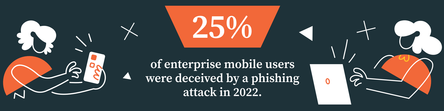
Relaxed BYOD policies have created blind spots for security and IT teams.

In 2022, more than 50% of personal devices were exposed to mobile phishing attacks

and more than 30% personal and enterprise mobile devices were targeted by phishing attacks at least four times.



Mobile phishing attacks are harder to spot.



of enterprise mobile users were deceived by a phishing attack in 2022.

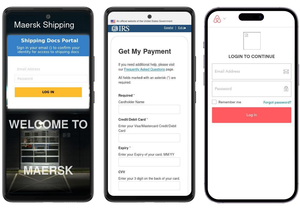
More than 40% of those tapped on at least six malicious links.

Phishing tactics aren't just via email anymore.

Phishing attacks are no longer confined to email. Attackers now take a hybrid approach.

Attackers are using a combination of vishing (voice phishing), smishing (SMS phishing), and quishing (QR code phishing) compromise an employee's credentials directly, or get past other security measures like multi-factor authentication (MFA)

Hybrid phishing attacks increased more than 7x in Q2, 2022 compared to Q1, 2021.

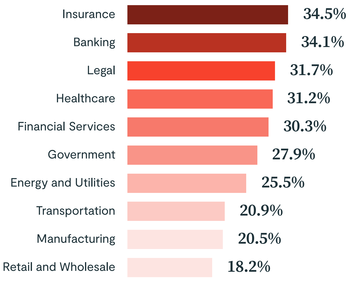


Financial Impact of a Mobile Phishing Attack

$ 3 8 7 6 5 5 0

Is your industry high risk?

Some of the most-regulated industries are frequent phishing targets. That's likely due to the high amounts of sensitive information and data they own (i.e., PII, PHI, intellectual property, or financial data).



For more information on the phishing encounter rates in your region, take a look at our interactive global map.

To learn more about the global state of mobile phishing, download the full report.

Lookout

Download Report