Ø

CYBERCRIMINALS WANT YOUR ORGANIZATION'S LOGIN CREDENTIALS

How to defend against mobile threats

Your mission is increasingly tied to mobile as your employees telework. Tablets, smartphones, and Chromebooks are often the devices of choice when supporting diplomats, ensuring battlefield safety or enhancing citizen services in the field. Cybercriminals know this and are targeting these devices to compromise your infrastructure.

Outdated mobile OSs leave you vulnerable.

99% of government Android users run outdated operating systems. This exposes your agency to hundreds of vulnerabilities.





Attackers are using your employees' logins to steal data.

Over 70% of phishing attacks against government employees sought to steal login credentials. This is a 67% increase from 2019, meaning cyberattackers are increasingly focused on using your employees to compromise your infrastructure.

Mobile app threats evolved rapidly in 2020.

App threats surged by nearly 20 times as the risks of a widely used app software development kit became known.



How do you protect your teleworking employees?

Mobile security must stop mobile phishing attacks while detecting app, device and network threats. It needs to secure the user, the endpoint and your organization while safeguarding user privacy. It also must work equally well for agency-owned and bringyour-own-approved devices (BYOAD).

> Stop phishing credential theft? Visit lookout.com/gov to learn more.

