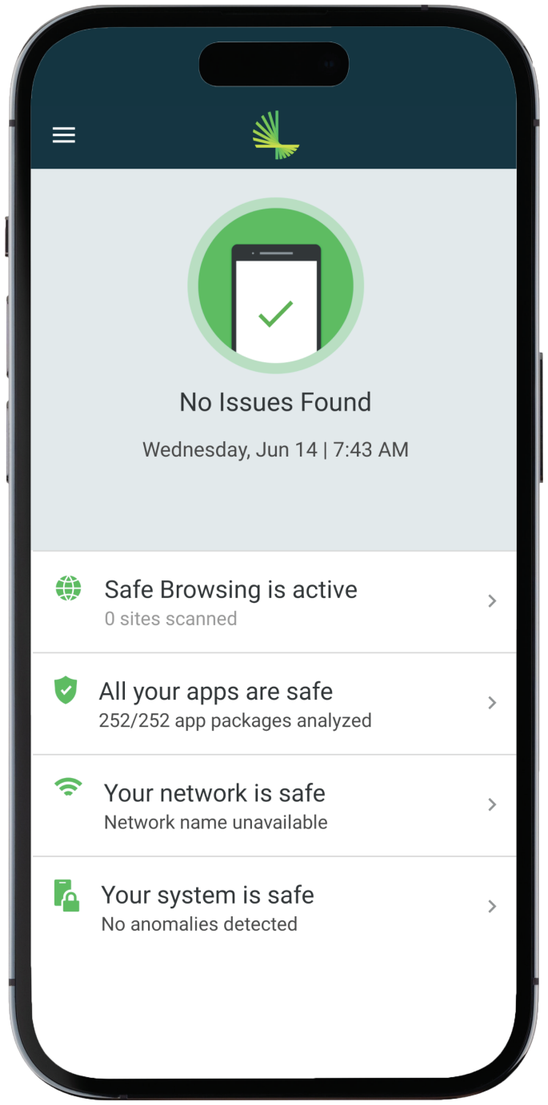
Sales Talk Tracks

Typically mobile devices are still not protected with the same mandatory mindset as PCs or laptops...

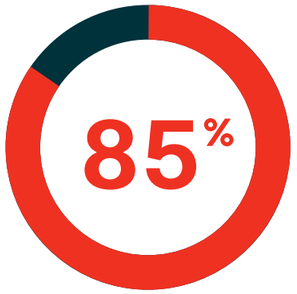
yet today more than half of the devices employees use to access company data now run iOS, Android or Chrome OS.

Mobile is often a much easier target for attackers to exploit. Phishing, for example, is harder to spot on mobile.

As a result, mobile is increasingly the entry point for cyber attacks.



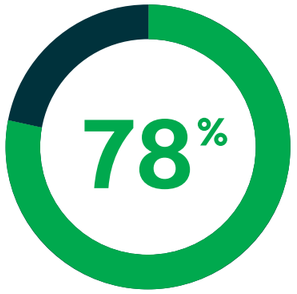
How secure are your mobile devices? Understand the threats.



of phishing attacks on mobile occur outside of email.

Employees are 3x more likely to click on a phishing link on mobile.





of Lookout customers were protected from a mobile threat in the last 12 months.

Safe Browsing

Phishing attacks

Harmful web content

Scanning QR codes

Apps

A mix of personal and corporate apps

Apps which leak or transfer data

Access to MFA tokens

Networks

Unsecured WiFi networks or hotspots

Device

Outdated operating systems

Risky device software

Tackling Objections

“I have never seen an attack on mobile.”

Without a mobile security solution in place any security attack on mobile is likely to go undetected. Phishing attacks on mobile increase on average by 85% every year.

“What’s the impact of a cyber attack on mobile?”

Depending on the hackers objectives the impact of a cyber attack can vary in severity, from personal credentials being compromised to financial loss, operational downtime or a crippling ransomware attack. Mobile security should be thought of as an insurance policy — an attack could happen at anytime across any device.

“I have a Mobile Device Manager.”

An MDM’s role is to manage mobile devices, it does not provide security against the majority of threats identified on mobile. Lookout compliments an MDM by adding a necessary layer of protection against mobile risk.

“Aren’t mobile devices natively secure?”

Any native protection with Android, iOS or Chrome is more focused around the device and operating system, consider external threats targeting a mobile device such as phishing, harmful web content or connecting to insecure networks.

“My IT is outsourced to another company.”

Your IT provider can manage Lookout on your behalf. They will have access to a management console where they can control deployment to your users and set mobile security policies to ensure your users, mobile devices and organisation are secure.



Lookout Differentiators

- The recognised leader in mobile security
- Backed by an unrivalled mobile threat dataset
- Simple remediation and user experience — enterprise grade security suited to SMBs

Lookout

About Lookout

Lookout, Inc. is the endpoint-to-cloud cybersecurity company that delivers zero trust security by reducing risk and protecting data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards digital information across devices, apps, networks and clouds and is as fluid and flexible as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and safely.

© 2023 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, and LOOKOUT with Shield Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, the 4 Bar Shield Design, and the Lookout multi-color/multi-shaded Wingspan design.

Lookout

Mobile Security

Simple Selling Guide

