



# Lookout Mobile Endpoint Security

## Understanding mobile risk

With the ability to stay connected from anywhere, tablets and smartphones have become indispensable tools that we use everyday. But our reliance on these devices has also introduced new risks, both to our personal privacy as well as enterprise data.

### Mobile threats

Your smartphone, just like your laptop, is susceptible to risk. Mobile devices may be more resilient to some threats, but they are just as vulnerable to others, namely phishing, application, network, and device threats.

Apps that you download and install on your mobile device may contain malicious code or present risks to your corporate or personal information through unsecure data handling practices. Every network your mobile device connects to has the potential to be unsafe. And the devices can be compromised by attackers targeting software vulnerabilities. So what's at risk? Your personal data, including texts, calls, contacts, and photos, as well as work data, including sensitive financial and corporate information.

### Why do I need Lookout?

Because your mobile device stores so much sensitive information, it's increasingly becoming a target for cyberattacks. Adding Lookout Mobile Endpoint Security to your mobile device will identify and minimize these threats and make it difficult for an attacker to steal your data.

### What does Lookout do

Lookout Mobile Endpoint Security scans the operating system, apps, and media on your device for suspicious activity. Lookout compares that data against its dataset, that includes telemetry from hundreds of millions of devices and apps. When a threat is detected, Lookout alerts your company as well as your user with instructions on how to remediate the issue.

### What Lookout doesn't do

Lookout firmly believes that your privacy is as important as your security. This is why we want to be completely transparent about the data we collect to help safeguard your device and the security of each employee. Lookout does not collect the following data types: Image, audio, video files, texts, personal information, or data generated using apps. Lookout for Work app won't impact your phone's performance or interfere with data stored on your device.

## Mobile risks

### Mobile phishing

On a mobile device, there are countless channels for a phishing attack to be delivered, including text messages, social media, and messaging apps.

### Downloaded apps

Any app installed to a mobile device could present a risk to your data, whether it's risky data handling practices or outright malicious behavior.

### Networks

Mobile devices can easily connect to any network, whether it's at a coffee shop or your home Wi-Fi. This means your data could be exposed to any risk associated with these networks.

### Devices

Out of date operating systems or software vulnerabilities can lead to your device being exploited.