# Mobile Security for the REMOTE WORKER

Lookout analyzed its mobile security data of 100 million apps and nearly 200 million devices to provide a view into the current security risks confronting remote workers as they spend more time working from their tablets and smart phones.

## Dynamics of remote work

### Mobile device use is increasing.

Lookout data shows a **37.1%** increase in iOS enterprise users between January and April 2020. Workloads are shifting to mobile devices as employees choose the ease, simplicity, and convenience of mobile.

### Employees are taking more risks.

A survey conducted by Tessian reveals that **52%** of employees believe they can get away with riskier behavior when working from home, such as sharing confidential files via email instead of more trusted mechanisms.[1]

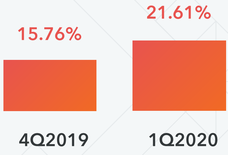
### The 9 to 5 workday is gone.

Hours shift as remote workers balance home responsibilities. An ESG survey shows that remote employees work **6 additional hours per week** outside of normal working hours.[2]

## Threats are targeting mobile devices

### Phishing attacks are on the rise.

Lookout users encountered phishing attacks at a rate exceeding 21% in 1Q2020 up 37% from 4Q2019. Phishing attacks designed for mobile are proving to be effective.



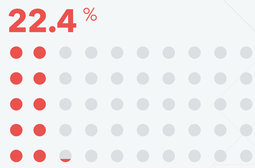

**26%**

### Productivity apps attract phishing.

Employees using Office 365 and G-Suite remain highly targeted by phishing attacks. Lookout data reveals average global phishing encounter rates exceeding 26%.

### Don't wait to update.

Devices running outdated and vulnerable operating systems or apps put the security of the device and corporate data at risk. This risk increases when it's left up to BYOD users to keep their device up-to-date. Lookout 1Q2020 data showed that only 22.4 percent of Lookout enterprise users were running the latest version of iOS.




# Tips for SECURING REMOTE WORKERS

## Establish a security baseline for mobile devices.

With workloads shifting to mobile devices, it's a good idea for companies to set a baseline of security expectations for devices that access corporate data. Some helpful questions to get started:

| | | |
|---|---|---|
| Should personal mobile devices be allowed to access corporate data? Or only company-issued ones? | What operating systems should be allowed to access corporate data? What are the minimum operating system versions required? | What minimum security controls should be in place (e.g., passcode is set, encryption is enabled, device is free from malware)? |

## Keep a close eye on Shadow IT.

Ensuring only IT-approved mobile apps are in use becomes more challenging in a remote workplace. Often, with the best of intentions, employees use an unapproved app for work, which can put intellectual property at risk.

If there is anything we can do to help support your business, please don't hesitate to contact us at lookout.com.

Lookout

1. https://www.zdnet.com/article/cybersecurity-half-of-employees-admit-they-are-cutting-corners-when-working-from-home/

2.ESG Research Report, 2019 Digital Work Survey, December 2019