U.S. Federal
MOBILE THREATS

Lookout analyzed its mobile security data of 100 million apps and nearly 200 million devices to provide a view into the current mobile security risks facing US Federal government mobile users.

Dynamics of remote work

Mobile device use is increasing.

Lookout data shows a **26.3%** increase in iOS for US Federal government employees between January and April 2020. Workloads are shifting to mobile devices as remote workers choose the ease, simplicity, and convenience of mobile.

US Federal agencies are securing telework.

A survey conducted by Lookout and MeriTalk in April 2020 reveals that **97%** of Federal security managers say their workforce uses mobile for multi-factor authentication, application access or data access.[1]

US Federal employees are productive from home.

According to a Federal News Network survey, more than half, **52%**, said they were more productive at home than at the office. Another 40% said their productivity was about the same.[2]

Threats are targeting teleworkers

Mobile phishing attacks increasingly target the US Federal government.

136% Phishing attacks against Federal mobile users increased 136 percent in 1Q2020.

45% Campaign-related phishing scams grew 45 percent during this period.

39.7%

39.7 percent of US Federal mobile users encountered phishing attacks.

29%

Productivity apps attract phishing.

Federal government users accessing data with Office 365 and G-Suite remain highly targeted by phishing attacks. Lookout data reveals average global phishing encounter rates of 29 percent.

Dramatic increase in mobile malware attacks on the Federal government

Malware detected on mobile devices of federal government users increased 450 percent.

Yet, nearly 1 percent of Federal mobile users downloaded unapproved apps.

84%

Pandemic drives growth of new mobile threats.

The number of new threats discoveries each month since the pandemic was declared exceeds the 2019 monthly average by 84 percent.

Tips for
SECURING REMOTE WORKERS

Establish a security baseline for mobile devices.

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

How can federal agencies allow both government-issued and personal mobile devices secure access to government data?	What mobile apps should be allowed to access government data?	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 highly classified data at risk.

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Our platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect you from the full spectrum of mobile risk. As a result, Lookout delivers modern endpoint security with the most comprehensive protection from device, network, app and phishing threats without prying into your data.

As a FedRAMP JAB P-ATO certified organization, Lookout is well qualified to provide mobile security solutions to federal agencies.

For more information on how we can help you, see our government solutions.

Lookout

1. MeriTalk. Mobile Threat Defense for Feds' New Normal. Lookout Survey Infographic. Lookout, v1, May 2020.

2. Ogrysko, Nicole. Federal News Network. Feds are enjoying full-time telework but doubt agencies will embrace it later. May 4, 2020.