Post-perimeter security for field agents

Survey reveals phishing attacks targeting remote government field agents on mobile devices.

Government agencies are struggling to adapt

Government agencies are struggling to adapt their security architectures to the fluid and unsecured environments that mobile devices introduce. Government agents are especially at risk. They rely heavily on mobile devices to access work resources such as email, case files, and other applications. Often traveling to various geographies, field agents can be exposed to app-based, network-based, and device-based threats. These threats seek to exploit mobile devices as they operate outside the traditional security perimeter. Back-end systems accessed remotely by field agents contain sensitive government data and personally identifiable information (PII), which could be used to compromise the financial well-being, privacy, and identity of US citizens.

Work has changed.

- **Critical data has moved to the cloud.**
- **Mobile devices have become critical productivity tools.**
- **Field agents often use untrusted networks to access gov data.**

Senators call for more protection of government data

The current threat level drove two senators to call on the Department of Homeland Security to do more to protect government data. In February of 2019, Senators Ron Wyden and Marco Rubio wrote a letter to the DHS urging it to conduct a risk assessment of the national security threat posed by data-sharing and VPN apps that expose government user traffic to servers located in countries that could become potential adversaries. Late last year, Lookout sponsored a survey, which documented dangerous mobile behavior by government employees.

Security Tip

Installing the latest operating system updates protects against software vulnerabilities.

42% reported they only updated 'when it's convenient'

14% never update

Source: "Americans and Cybersecurity" Survey [1]

Key Findings of Lookout Risk Assessment

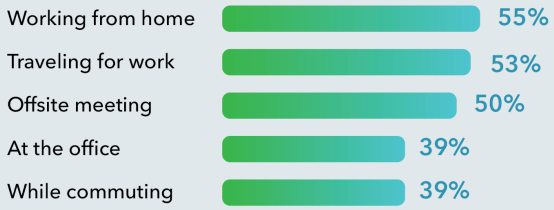
- Respondents at all level of government use their mobile devices to review work data outside their agency's network perimeter.
- A plurality of respondents review work data on their mobile devices in many situations, both inside and outside of the office.
- Nearly 1 in 2 respondents have received a phishing message on their mobile device, most commonly through email.

Government Business Council (GBC) conducted a 4-question poll on post-perimeter security to a random sample of 306 federal, military, state, and local government employees in November 2018.

1. Do you access work data on your mobile device when you're not connected to your agency network?

Percent of respondents, n=35

2. Where do you access work data on your mobile device?



Percent of respondents, n=135
Note: respondents were asked to select all that apply

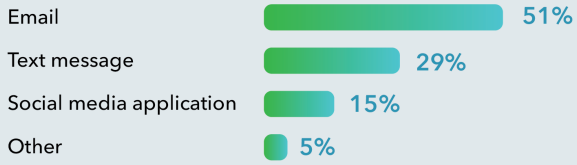
Nearly half (45%) of government employees report reviewing work data on their mobile devices outside of their agency's network.

1 in 3 respondents review work data on their mobile devices in all the environments listed. **55%** review work data on their mobile device from home.

3. Have you encountered phishing on your mobile device?

Percent of respondents, n=296

4. How was the phishing message delivered to your mobile device?



Percent of respondents, n=133

Summary

As data continues to move to the cloud, government organizations must adopt a post-perimeter security strategy to safeguard sensitive information. Government field agents often travel to remote locations with limited infrastructure, connecting mobile devices to untrusted networks. Cybercriminals not only exploit vulnerable networks but also launch phishing attacks designed to be effective on mobile. In fact, Lookout data reveals that users are three times more likely to click on a phishing link on a mobile device than on a laptop or personal computer. With a deep understanding of the cybersecurity requirements of government field agents, Lookout is well positioned to safeguard government agents as they work beyond the traditional security perimeter.

[1] Pew Research Center: "Americans and Cybersecurity." January 26, 2017. https://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/