Lookout®

U.S. GOVERNMENT THREAT REPORT

Telework exposes government to heightened mobile risk

Executive summary

Mobile devices have unlocked previously untapped potential for your organization, enabling your employees to work however and from wherever they're the most productive. These modern endpoints, alongside cloud applications, now provide the same access to your sensitive data and confidential information as traditional computer endpoints. As a result, cyberattackers have built strategies to target both mobile devices and desktops to ensure they find vulnerable entry points into your infrastructure.

A single successful phishing or ransomware attack enables intruders to gain access to nearly any category of a government agency or department's data. While mobility and cloud applications have enabled your organization to remain productive while remote, they also significantly increase the risk of successful attacks.

A challenge to securing mobile devices is that the traditional approach to endpoint security solutions does not work for their modern operating systems. iOS, Android and Chrome OS devices operate differently and present a unique attack surface for threat actors seeking to compromise all levels of government. To secure your organization against phishing, malicious applications and device compromises, a modern approach to mobile security is needed.

Key findings from 2020

- 99 percent of U.S. government Android users are exposed to hundreds of vulnerabilities due to out-of-date operating systems.
- App threats surged by nearly 20 times across all levels of government as the cybersecurity community recategorized the risks surrounding embedded adware.
- 1 in 15 government employees were exposed to phishing threats. With over two million federal government employees alone, this represents a significant potential attack surface because it only takes one successful phishing attempt to compromise an entire agency.
- Over 70 percent of phishing attacks against government organizations sought to steal login credentials, which is a 67 percent increase from 2019.
- Nearly one quarter of state and local government employees use personal unmanaged devices, outpacing the nearly 9 percent in the federal government.

Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 2019 to December 31, 2020

Our methodology

To understand the challenges facing U.S. government agencies, we looked at data specific to our federal, state and local customers from the Lookout Security Graph. The Graph, which includes telemetry data from analysis of nearly 200 million devices and over 135 million apps, enabled us to identify and break down the most prominent threats agencies faced in 2020. Information used in this report was compiled from de-identified, aggregated data.

Priority drivers for mobile security

One of the biggest technological challenges for all government entities has been the rapid shift to telework and away from physical locations in response to COVID-19. Almost overnight, government agencies and departments were forced to telework, provide telehealth, and hold all previously face-to-face activities, even court hearings, virtually. As a result, employees relied more heavily on smartphones, tablets, and Chromebooks to balance the demands of at-home and work life. The increased number of mobile devices accessing government data increases the attack surface for threat actors to launch cyberattacks against government agencies.

To compromise a government's infrastructure, attackers have turned to mobile spear phishing campaigns to steal an employees' login credentials or deliver malicious payloads to their mobile devices. These attacks use social engineering to convince the employee to visit a phishing page or tap a link that silently delivers malware. While social engineering attacks cannot be blocked, agencies can block access to phishing sites and detect apps with embedded malware.

Malicious actors have embraced mobile phishing because they can use any one of the hundreds of apps on the average person's mobile device. Attackers can socially engineer targets on a personal level through social media apps, messaging platforms, games and even dating apps. An attacker will target particular individuals, including department heads, law enforcement officials, city superintendents, revenue officers or other government officials to gain privileged access to the data they want to steal.

Since most employees use a smartphone, tablet, Chromebook, or all of these, to access government data, these devices create a new widespread attack surface that is often overlooked. If these mobile endpoints are not properly secured, they can represent a significant gap in an agency's security architecture and compliance posture.

Mobile risk exposure across U.S. federal, state and local government agencies

The rate at which devices are exposed to mobile phishing, app threats, device and network threats is increasing. These increased exposure rates are specific to government agencies protected by Lookout and are derived from our industry-leading dataset of security telemetry.

Phishing campaigns target personal mobile devices

Your employees work differently now. While teleworking from home, they want to use their tablet, smartphone, and Chromebook to remain productive while also using them to manage their personal lives. To meet these expectations, agencies are increasingly adopting BYOD strategies. But this makes securing mobile endpoints even more challenging.

Federal departments have been slower than state and local agencies to adopt BYOD strategies. Less than 10 percent of federal employees use their personal tablets and smartphones for work. Personal mobile devices represent the new frontier of shadow IT with many agency employees using the tablet, smartphone, and Chromebook for telework. This type of shadow-BYOD doesn't provide IT and security teams complete visibility into which mobile devices are accessing the agency or department's data and underscores the security gap they create.

Managed vs. Unmanaged Mobile Device Usage

	Federal	State and Local
Managed	91.34%	75.69%
Unmanaged	8.66%	24.31%

Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 to December 31, 2020

With nearly a quarter of state and local government employees using their personal devices for work, these agencies are leading the government adoption of BYOD. While this provides employees with greater flexibility, these unmanaged personal devices are more frequently exposed to phishing sites than managed devices. This is because personal unmanaged devices connect to a broader range of websites and use a greater variety of apps because of the individual's needs and interests. Fortunately, state and local departments are showing a growing awareness of the need for mobile phishing protection across both managed and unmanaged devices.

Mobile Phishing Exposure Rates Across Managed vs. Unmanaged Mobile Devices

	Federal	State and Local
Managed	2.66%	6.18%
Unmanaged	16.62%	11.02%

Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 to December 31, 2020

Overall, state and local employees are more frequently exposed to phishing sites than federal agency employees. This is because these departments have a higher proportion of BYOD employees who have unrestricted use of their devices. As a result, these employees are exposed to phishing sites at a higher rate.

Fortunately, with the increasing adoption of modern endpoint security solutions and mobile phishing protection, a BYOD strategy can be implemented securely while also respecting privacy. With crowdsourced data, modern security solutions are able to detect threats without inspecting content. With proper security in place, all government agencies and departments will have visibility into cyber threats targeting their mobile fleet, regardless of whether a device is managed or not.

Phishing campaigns steal credentials

Mobile phishing threats can be broken into two categories: credential harvesting and malware delivery. With credential harvesting, a threat actor can log in as a government employee and move laterally around the organizations's infrastructure until they locate the sensitive data they want to steal and exfiltrate it.

Malware delivery attempts to trick employees into installing malicious apps to the device. A recent example of an app with malware is the well-known Wroba trojan that silently installs on the device in the background when the link is tapped. Once installed, the malware harvests and steals sensitive information such as financial data and contact lists.

Phishing attacks designed to steal credentials or deliver malware can be delivered through social engineering within any app including social media platforms, messaging apps, games or even dating apps.

Phishing Exposure in 2020

All Government	Federal	State and Local
1 in 15	1 in 30	1 in 13

Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 to December 31, 2020

Credential harvesting nearly doubles

Threat actors are increasingly using phishing attacks for harvesting credentials rather than delivering malware when targeting federal, state and local agencies and departments. In 2020, over three-quarters of phishing attacks sought to steal credentials. When compared to 2019, credential theft attacks against federal agencies increased at a rate of 90 percent while malware delivery decreased at a rate of 47 percent. State and local departments experienced a similar trend with credential theft attacks increasing at a rate of 42 percent and malware decreasing at a rate of 55 percent.

Cybercriminals are targeting mobile devices as an entry point for executing more invasive and persistent attacks. All government entities need mobile security that includes endpoint detection and response capabilities to proactively hunt for these threats, which have penetrated your environment.

Year Over Year Comparison of Credential Harvesting and Malware Delivery

	All Government		Federal		State and Local	
	2019	2020	2019	2020	2019	2020
Credential Harvesting	42.68%	71.47%	39.79%	75.53%	56.14%	79.65%
Malware Delivery	57.32%	28.53%	69.41%	36.61%	69.15%	30.89%

Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 2019 to December 31, 2020

In any organization, the first line of defense against phishing is an employee's ability to spot a phishing message. Each time a mobile employee is exposed to a phishing site, the Lookout app notifies the individual and provides security tips. Over time, employees become better at recognizing phishing messages.

In the table below, 71.62 percent of federal employees and 62.42 percent of state and local employees who received a notification from Lookout that they had clicked on a phishing link did not click on subsequent mobile phishing links. This reinforces the difficulty for an employee to identify a phishing link on a mobile device and indicates that once they are notified, they use better judgment.

Number of Mobile Phishing Links Government Employees Clicked On

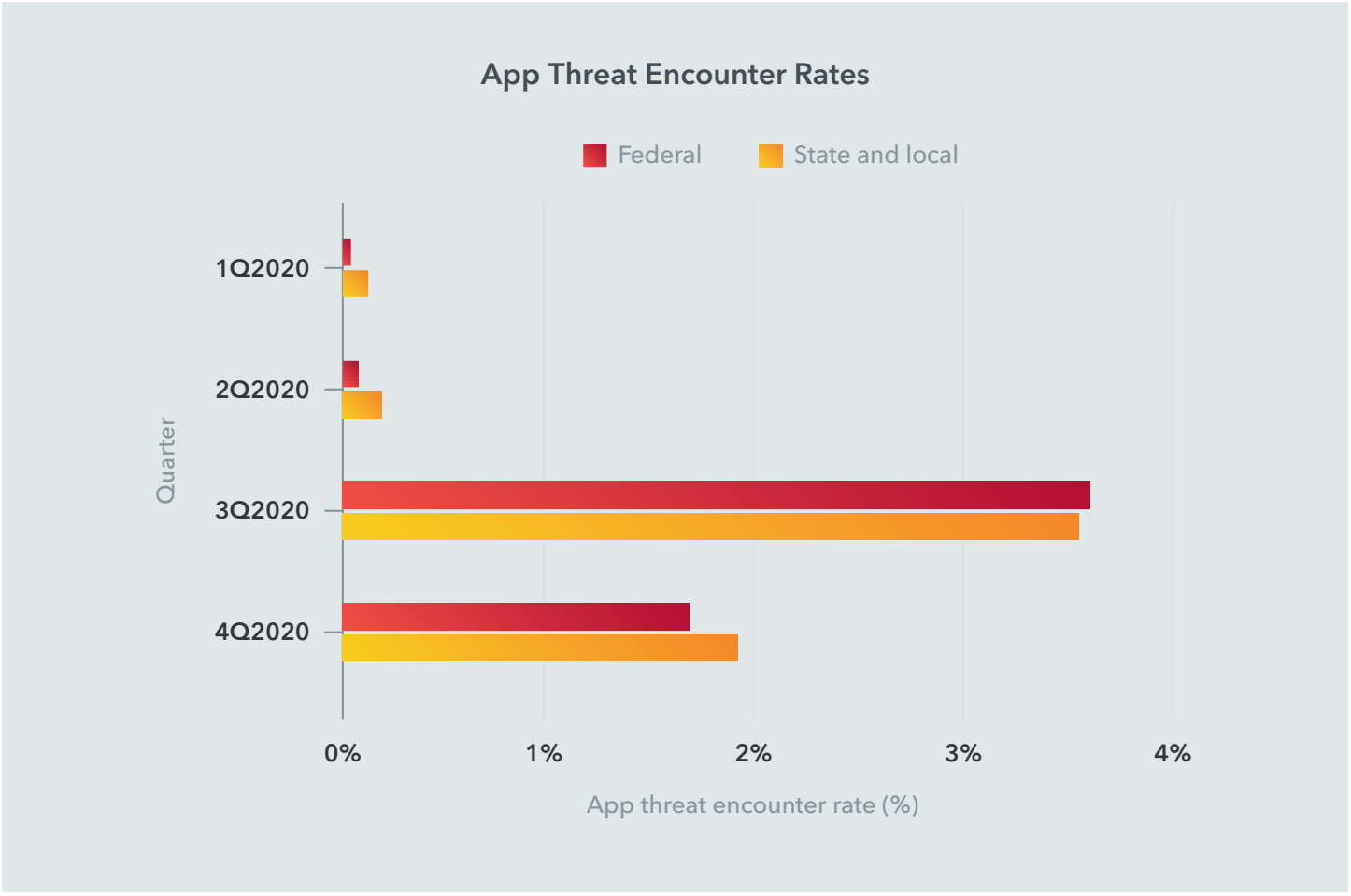
Number of unique URLs an employee clicked	1	2	3-5	6+
US Federal	71.62%	18.08%	9.06%	1.24%
US State and Local	62.42%	18.61%	13.84%	5.13%

Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 to December 31, 2020

While mobile phishing attacks have become sophisticated, threat actors reuse techniques enabling employees to recognize them if educated. This shows that ongoing phishing and cybersecurity education is essential to enable employees to spot social engineering attacks. Your mobile endpoint security solution should contain in-app education so that employees are educated every time a threat on their device is detected. All government entities need to ensure that they evolve their phishing training beyond desktops and emails to include challenges related to mobile phishing.

Software development kits increase mobile app risk

Government personnel were exposed to fewer mobile application threats in the first half of 2020 than they were in the second half. Industry groups like the Google App Defense Alliance, of which Lookout is a founding member, work to prevent malicious apps from making it onto official app stores. However, this does not prevent apps with malware from being sideloaded from unofficial third-party app stores that lack security review of apps, and include high percentages of mobile malware.



Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 to December 31, 2020

The spike in the third quarter of 2020 is due to the updated classification of SourMint, a widely-used advertising software development kit (SDK), to riskware because of its insight into user browsing habits. For comparison, across all private industries, there was a four percent exposure rate in that same quarter, indicating both the federal and state and local government were equally susceptible to the malicious SDK as the private sector.

This higher app threat exposure level continued in Q4 increasing by nearly 20 times for the year. This level of app threat exposure may be here to stay as advertising SDKs increasingly show up in mobile apps. These SDKs often contain vulnerabilities that can provide back-doors for entry by threat actors.

Some of the government-agency risks caused by malicious apps include:

- Compliance violations due to data handling practices
- Excessive permissions that allow an app to see data in other apps on the device
- Access to the camera and microphone to spy on the user
- Access to the device's file system
- Connections to servers in foreign countries

Having visibility into the permissions and capabilities of all apps on a mobile device is key to ensuring a strong security posture for your organization. But, you must also respect end-user privacy. Since many employees want the flexibility to use personal devices for work, mobile apps have become the new frontier of shadow IT. By understanding the capabilities of all apps across your mobile fleet and being able to build access policies around them, you can ensure you are aligned with data privacy laws and keep your organization's confidential information secure from malicious actors.

Government employees exposed to hundreds of vulnerabilities

U.S. federal, state and local government employees use older versions of Android and iOS operating systems exposing them to hundreds of vulnerabilities.

Android - 3 months after Android release[1]

OS version	Percent of government devices	Number of vulnerabilities in OS[4]
11[3]	0.08%	>50
10	38.30%	266
9	28.20%	173
8	22.80%	636

iOS - 3 months after iOS 14 release[2]

OS version	Percent of government devices	Number of vulnerabilities in OS[5]
14	67.80%	>50
13	27.90%	>195
12	3.40%	>65
11	0.04%	>130

[1] Source: https://www.cvedetails.com/version-list/1224/19997/1/Google-Android.html

[2] Source: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ios

[3] Source: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=android+11

[4,5] Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 to December 31, 2020

Google and Apple release regular software updates to fix bugs and resolve security issues. A cybersecurity best practice is to keep a mobile operating system up-to-date. However, government agencies or departments may choose to delay updates until their proprietary apps have been tested. This delay creates a vulnerability window during which a threat actor could use a mobile device to gain access to the organization's infrastructure and steal data.

The number of vulnerabilities associated with a particular operating system version represents the risk of remaining on that version. Although vulnerabilities can be patched, there are still obstacles to overcome:

- Attackers can exploit vulnerabilities to actively target and take over a device or surpass its built-in security measures.
- Patching usually requires action by the employee to update the device.
- If an employee is running an old version, they present a risk to the organization that could be easily eliminated with an operating system update.
- In order to protect against exploitation of known vulnerabilities, your team needs to have mobile vulnerability and patch management capabilities. Only with visibility into endpoint and app vulnerabilities will you know exactly where these weaknesses exist and when they need to be updated in order to prevent security gaps from being exploited by threat actors.

Reduce agency risk from mobile phishing and app threats

Government employees use iOS, Android and ChromeOS devices everyday to stay productive and increase efficiency. This makes them targets for cyberattackers because their devices are a treasure trove of data and a gateway to government infrastructure.

While the shift to telework came quickly, it is here to stay and many agencies and departments are increasingly considering a bring-your-own-approved-device (BYOAD) strategy. By requiring personal devices to come from an approved list of devices, agencies can extend the benefits of BYOD while ensuring a standard of device quality and security.

Regardless of whether devices are managed, BYOAD, or BYOD, protecting these modern endpoints requires a different approach — one that is built from the ground up for mobile. Only a modern endpoint protection solution can detect mobile threats in apps, device operating systems and network connections while also protecting against credential harvesting and malware delivery attacks through phishing.

Due to the personal nature of smartphones, tablets and Chromebooks, endpoint security must protect the user, the device and the organization while respecting user privacy. For guidance on how to secure iOS, Android, and ChromeOS devices, many government IT and security teams have turned to the National Institute of Standards and Technology (NIST) Special Publication 800-124 as a framework to develop their strategy to secure mobile devices in a complex environment.

Mitigation of Mobile Threats to Government (Adapted from NIST SP 800-124 REV.2)[6]				
Threats (NIST)	**Mobile Security***	**EMM**	**VPN**	**Education**
Exploitation of underlying vulnerabilities in devices	✓			
Device loss and theft		✓		
Credential theft via phishing	✓			✓
Installation of developer and EMM profiles	✓			✓
Accessing enterprise resources via a misconfiguration device	✓	✓		
Installation of unauthorized certificates	✓			
Use of untrusted mobile devices	✓			
Wireless eavesdropping	✓		✓	
Mobile malware	✓			✓
Information loss due to insecure lock screen		✓		✓
User privacy violations	✓			✓
Data loss via synchronization		✓		✓
Shadow IT usage		✓		
Exploitation of vulnerabilities within the underlying EMM platform				✓
EMM administrator credential theft		✓		
Insider threat	✓	✓		✓

*Mobile security includes Mobile Threat Defense (MTD) and other security functions provided by Lookout.

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.

Lookout is FedRAMP Joint Advisory Board (JAB) Provisional Authority to Operate (P-ATO) certified and proud to serve federal government agencies.

To learn more about how Lookout protects government agencies, visit lookout.com/solutions/government.

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2-draft.pdf