Lookout

Rise in Mobile Phishing Credential Theft Targeting U.S. Public Sector

U.S. Government Threat Report

Table of contents

Executive summary

Mobile devices have unlocked previously untapped potential for your organization, enabling 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 can result in intruders gaining access to nearly any category of a government agency or department's data. While mobile and cloud apps have helped your organization remain productive while employees telework, 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 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 security. Mobile Device Management (MDM) provides basic security capabilities, such as pushing software updates, but lacks the continuous monitoring and protection capabilities to secure your organization against phishing, malware, and device compromises.

Key findings from 2021 and first half of 2022

- Nearly 50% of state and local government employees are running outdated Android operating systems, exposing them to hundreds of device vulnerabilities.
- 1 in 8 government employees were exposed to phishing threats.
- Almost 50% of all phishing attacks in 2021 sought to steal credentials of government personnel, up from 30% in 2020.
- Federal, state, and local governments increased their reliance on unmanaged mobile devices at a rate of 55% from 2020 to 2021, indicating a move toward bring your own device (BYOD) to support telework.

Our methodology

To understand the challenges facing U.S. government agencies, Lookout analyzed data specific to our federal, state, and local customers from the Lookout Security Graph. The graph, which includes telemetry data from analysis of more than 200 million devices and more than 175 million apps, enabled us to identify and break down the most prominent mobile threats agencies face. For this report we specifically reviewed data from 2021 and the first half of 2022. Information used in this report was compiled from de-identified, aggregated Lookout data.

Priority drivers for mobile security

One of the biggest technological challenges facing all government entities has been the rapid shift to telework in recent years. Security teams are acutely aware of the emerging risks that come from using cloud apps and having a workforce that connects using endpoints they have no visibility into.

The good news is that the U.S. federal government is increasingly focused on cybersecurity challenges. President Biden signed Executive Order 14028 to improve cybersecurity in 2021 and since then the U.S. Office of Management and Budget (OMB) has released a series of memos with actionable guidelines and requirements.

These memos require agencies to provide the government visibility into cyber threats on all endpoints, including mobile devices, and adopt widely accepted security measures and related best practices, including the need to:

- implement enhanced security for cloud services and critical software;
- comply with event logging requirements for incident response;
- expand endpoint detection and response (EDR) coverage capabilities to mobile devices;
- and implement a zero trust architecture (ZTA) strategy.

Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 2020 to June 30, 2022

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

Based on the latest Lookout data, there are a few specific trends that government agencies and departments should be aware of — specifically as they relate to the increased usage of unmanaged mobile devices as well as phishing encounter rates.

Out-of-date mobile device operating systems also present risk to federal, state, and local governments because these devices contain vulnerabilities that can be exploited by bad actors.

Phishing campaigns target personal mobile devices

Your employees work differently now. While teleworking, they want the freedom to use their tablet, smartphone, and laptops for work as well as to manage their personal lives. To meet these expectations, agencies are increasingly adopting BYOD programs. Unfortunately, this increased flexibility also introduces additional challenges to the protection of mobile endpoints.

As telework continued through 2021, there was a significant rise in the number of unmanaged mobile devices across both the federal and state and local governments. Personal mobile devices represent the new frontier of shadow IT with many agency employees using tablets, smartphones, and Chromebooks for telework. This type of shadow BYOD eluminates what little visibility IT and security teams had into unmanaged devices connecting outside the corporate perimeter.

Managed vs. Unmanaged Mobile Device Usage

	Federal		State and Local	
	2020	2021	2020	2021
Managed	91.34%	86.82%	75.69%	61.86%
Unmanaged	8.66%	13.18%	24.31%	38.19%

With more than one third of state and local government employees using their personal devices for work in 2021, these agencies are leading the government adoption of BYOD. While this provides employees with greater flexibility, these unmanaged 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.

In our analysis, we saw a steady rise in mobile phishing encounter rates for state and local governments across both managed and unmanaged devices, increasing at rates of 48% and 25% respectively from 2020 to 2021. This steady climb continues through the first half of 2022.

We also saw a steady decrease in phishing exposure rates for federal unmanaged devices, suggesting agencies increased security awareness for BYOD participants. Phishing exposure rates for federal managed devices, however, increased from 2020 to 2021 only to then decrease in the first half of 2022. It's expected that holiday-focused phishing attacks in the second half of 2022 will elevate exposure rates.

Mobile Phishing Exposure Rates Across Managed and Unmanaged Devices

	Federal			State and Local		
	2020	**2021**	**2022 (Q1 and Q2)**	**2020**	**2021**	**2022 (Q1 and Q2)**
Managed	2.66%	9.57%	5.95%	6.18%	9.13%	13.59%
Unmanaged	16.62%	10.42%	8.52%	11.02%	13.8%	14.57%

With the increasing adoption of modern endpoint security solutions and mobile phishing protection, a BYOD strategy can be implemented easily and 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

To further understand the impact of mobile phishing on government entities, we also analyzed the different types of attacks. Mobile phishing threats can be broken into two categories: credential harvesting and malware delivery.

With credential harvesting, the goal is to trick the victim into giving up their login credentials so the threat actor can log in as a government employee and move laterally around the organization's infrastructure. The attackers usually use these opportunities to find additional vulnerabilities or sensitive data they can compromise.

Malware delivery attempts to trick employees into installing malicious apps to the device. New and upcoming spyware such as Predator have been used in phishing attacks across the globe. Alien is one of the most recent examples of mobile phishing malware being studied by government agencies. The goal is similar to credential harvesting in that these attacks are looking to compromise an organization's infrastructure.

Either types of phishing attacks can be delivered through social engineering within any app including social media platforms, messaging apps, games, or even dating apps.

Mobile phishing exposure rates for 2020, 2021 and first half of 2022			
	2020	**2021**	**2022 (6 months)**
Federal	1 in 30	1 in 7	1 in 11
State and Local	1 in 13	1 in 11	1 in 7
All Government	1 in 15	1 in 8	1 in 11

Credential harvesting increases dramatically

Malware delivery continues to represent roughly 75% of all mobile phishing attacks across all industries. However, when targeting federal, state, and local government entities, threat actors are increasingly using phishing attacks for harvesting credentials rather than delivering malware.

In 2021, almost 50% of all phishing attacks sought to steal credentials. The proportion of credential theft attacks against federal agencies increased at a rate of nearly 47% from 2020 to 2021 while the proportion of malware delivery decreased by 12%. State and local departments experienced a similar trend with credential theft attacks increasing and malware decreasing gradually.

Phishing attacks seem to be getting more sophisticated as well, with 16% attempting to deliver malware as well as trying to steal credentials. These sophisticated attacks increased across both federal and state and local from 2020 to 2021, emphasizing the need for advanced mobile phishing and malware detection.

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 & Malware Delivery						
	All Government		**Federal**		**State and Local**	
	2020	**2021**	**2020**	**2021**	**2020**	**2021**
Credential harvesting	31%	46%	33%	47%	30%	45%
Malware delivery	79%	70%	80%	68%	80%	75%
Both credential harvesting and malware delivery	11%	16%	13%	15%	10%	20%

Users learning from past mistakes

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 individual is notified and provided security tips. Over time, employees become better at recognizing phishing messages.

In the table below, well over 50% of federal, state, and local employees who received a notification that they had clicked on a phishing link did not click on a subsequent mobile phishing link. This highlights 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				
# of URLs an employee clicked	1	2	3–5	6+
Federal 2021	58.3%	18.83%	16.6%	6.26%
State and Local 2021	57.02%	19.01%	17.51%	6.30%

While mobile phishing attacks have become sophisticated, threat actors continue to reuse techniques enabling employees to recognize them once educated to do so. This shows that ongoing phishing and cybersecurity education is essential to enable employees to spot social engineering attacks. Your mobile threat defense solution should contain in-app education so that employees are informed 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

Based on Lookout data, state and local employees are generally more exposed to app threats than their federal counterparts. This is likely related to the fact that state and local governments have a higher proportion of BYOD devices.

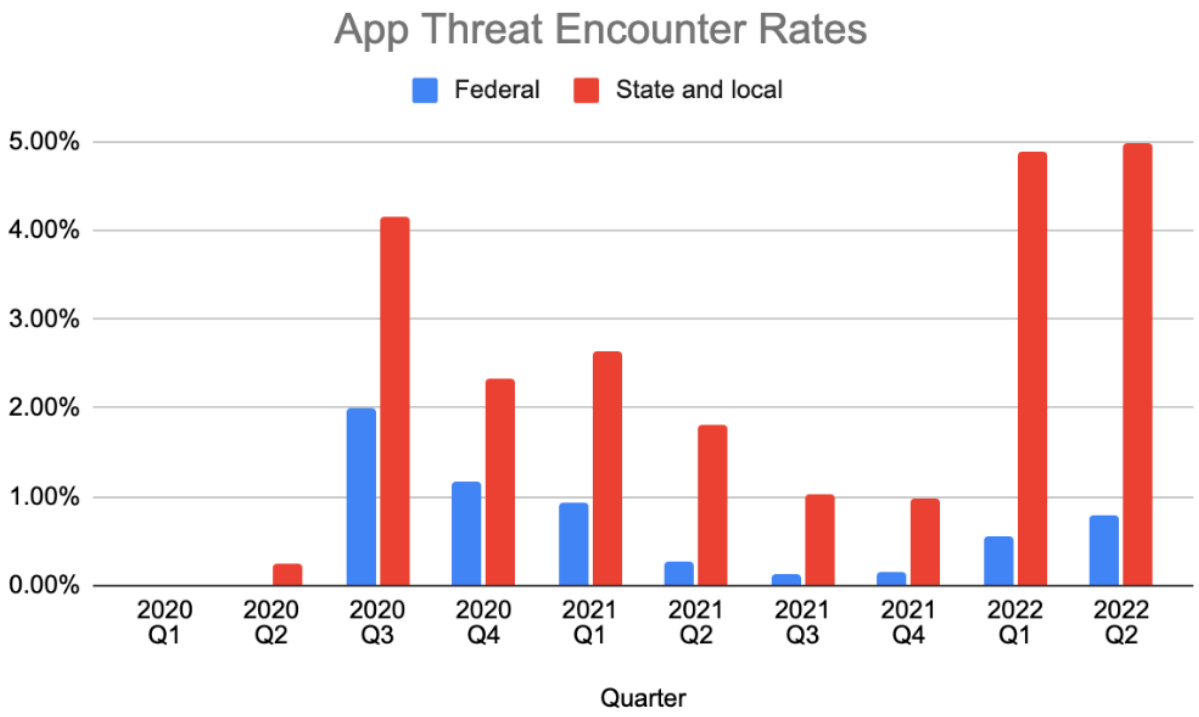
Industry groups like the Google App Defense Alliance, of which Lookout is a founding member, work to prevent malicious apps from making it onto official app stores. However, this does not prevent malware from being sideloaded from unofficial third-party app stores that lack security reviews.

Looking back at 2020, we see an initial spike in app threats, which resulted from a reclassification of the SourMint software development kit to riskware. This trend of a higher level of app threats has since been sustained. Overall, federal employees are less exposed to app threats, meanwhile state and local governments have found it increasingly difficult to manage this threat vector. In fact, the first half of 2022 produced sharp spikes in encounter rates among state and local employees, reaching an average of 4.94%.

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 government agencies. Balancing this while respecting user privacy is paramount. Many employees want the flexibility to use personal devices for work, yet employers need to manage the sprawl of shadow IT that is exacerbated by mobile apps. By understanding the capabilities of all apps across the agency's mobile fleet and being able to build access policies around them, governments can ensure alignment with data privacy laws and keep confidential information secure from malicious actors.



Government employees exposed to hundreds of vulnerabilities

Based on Lookout data, nearly 50% of all U.S. federal, state, and local government employees use older versions of Android and iOS operating systems, which means they are exposed to hundreds of vulnerabilities.

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.

For example, Apple released a software update to address over 35 issues related to vulnerabilities in iOS version 15.5 that had potential effects ranging from remote code execution to UI spoofing and user activity tracking. Not upgrading to this release puts organizations at greater risk of a data breach due to a successful cyber attack.

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 be aware of and 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.

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.

Android — 10 months after Android 12 release			
OS Version	**Percent of federal government devices**	**Percent of state and local government devices**	**Number of vulnerabilities in OS**
12	67.05%	54.51%	423
11	14.87%	15.65%	791
10	6.58%	9.8%	1116
9	3.98%	10.29%	714
8	6.69%	7.38%	1332

iOS — 10 months after iOS 15 release			
OS Version	**Percent of federal government devices**	**Percent of state and local government devices**	**Number of vulnerabilities in OS**
15	94.25%	70.9%	209
14	2.24%	23.68%	521
13	0.41%	1.68%	836
12	0.05%	1.12%	1083
11	0.01%	0.09%	1344

Reduce agency risk from mobile phishing and app threats

Government employees use iOS, Android, and ChromeOS devices every day 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 BYOD 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, 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 phishing attacks that steal credentials and deliver malware.

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, a guide that Lookout contributed to, 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)				
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.

Do you know your **data risk score?**

Today, data flows freely. As the places data can go continue to expand — from cloud apps to mobile devices — the challenge of keeping data secure will grow exponentially.

Knowing your risk is the first step to ensuring the protection of your data and your organization. In just a few minutes of your time, and with 15 questions, we will give you a high, medium, or low risk rating that helps you better understand your security posture.

GET STARTED

Lookout™

About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit **lookout.com**

Request a demo at **lookout.com/request-a-demo**

TX-RAMP CERTIFIED

FedRAMP™

AUTHORIZED & JAB StateRAMP