Lookout

# Feds: You have a BYOD program whether you like it or not

"We don't have a BYOD program."

This statement, referencing mobile device usage in the workplace, will likely sound familiar to federal government employees. Many agencies believe they aren't actually subject to cyber-threats from mobile devices because, simply, they don't currently allow personal mobile devices to access their networks. Ultimately, however, this posture puts the government and its data at risk because federal agencies have a BYOD program whether they like it or not.

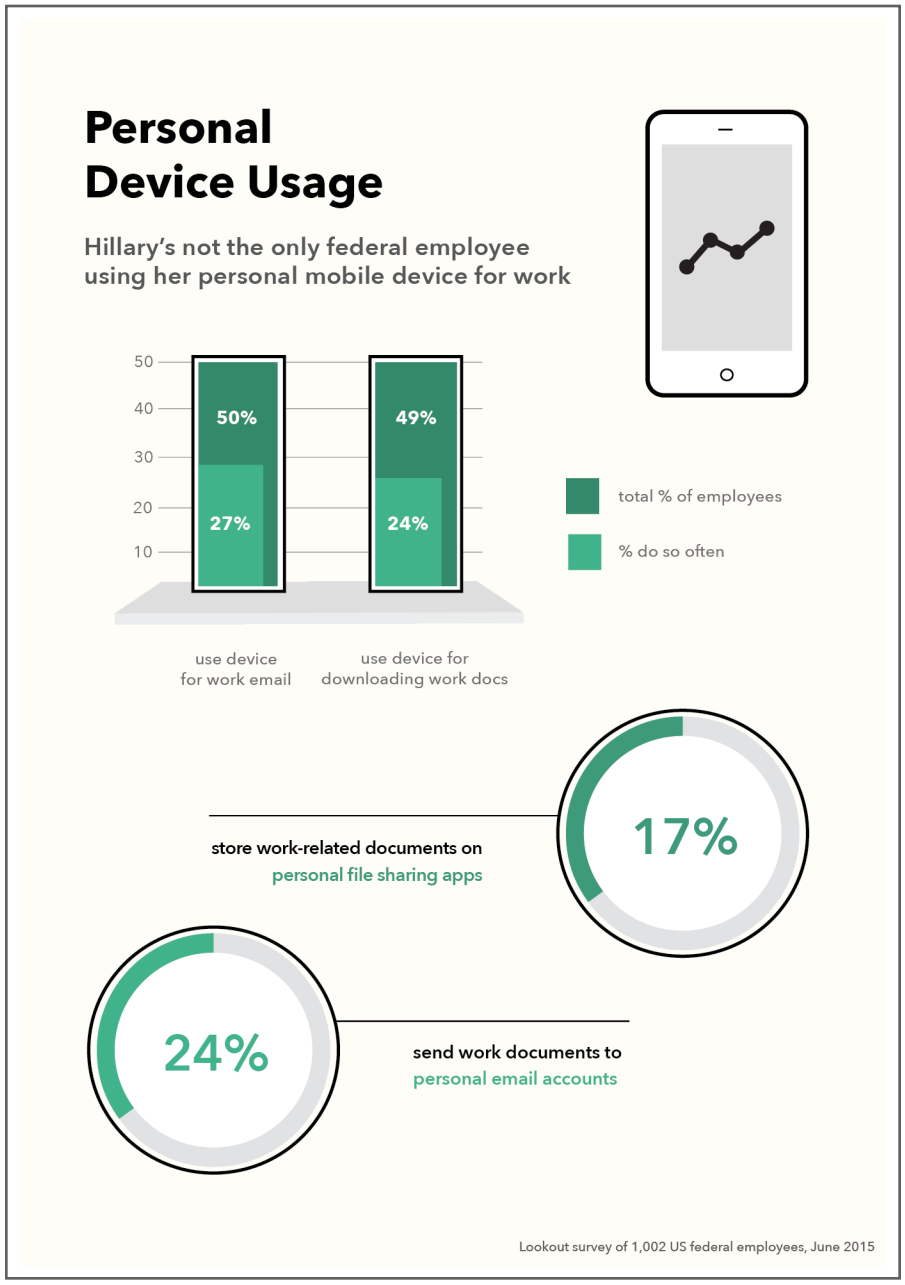
Need a little convincing? After analyzing 20 federal agencies, Lookout discovered 14,622 Lookout-enabled devices associated with government networks. That means people are connecting their phones to your systems. What's more is that the frequency of serious mobile threat encounters per year among these devices was high: 11 percent.

The problem is "Shadow BYOD," a reference to unmanaged or unknown mobile devices accessing a network. Similar to Shadow IT, Shadow BYOD introduces a risk of sensitive data leakage due to the lack of visibility and control of this access.

In an effort to better understand what's going on here, Lookout surveyed over 1,000 federal government employees to identify their behaviors on mobile and suss out whether that behavior puts sensitive government data at risk. The answer is unequivocally "yes."

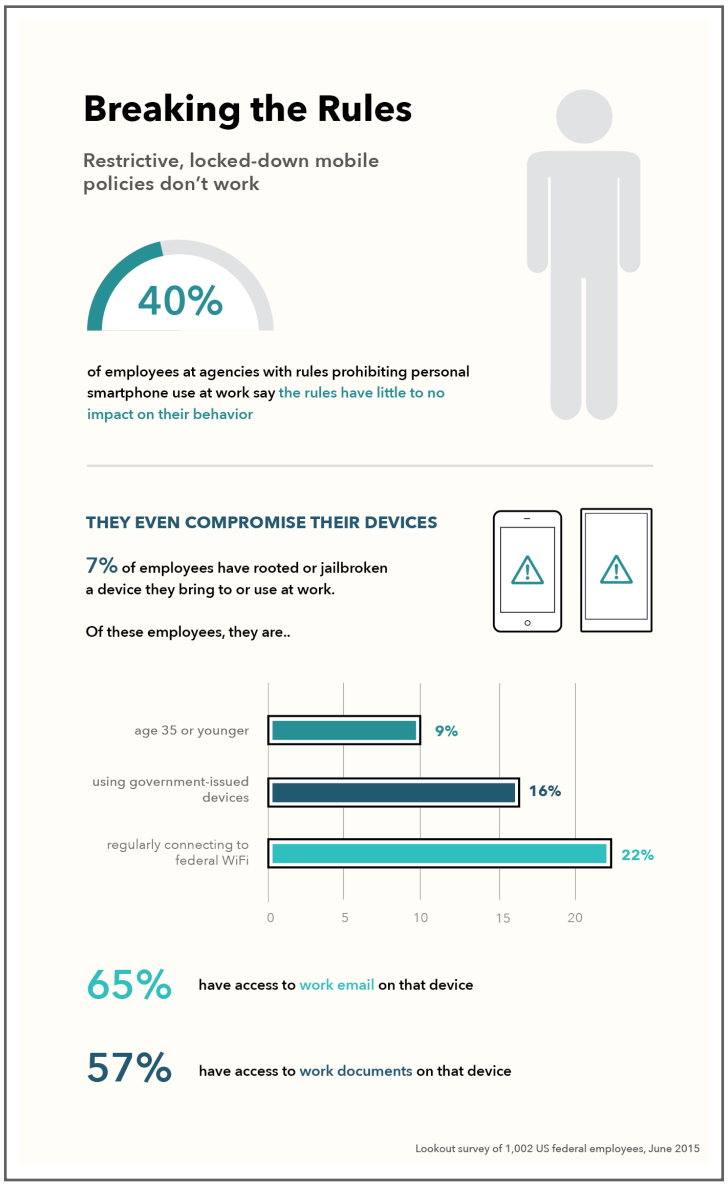
## Hillary isn't the only one using her personal device for work

Whether they realize it or not, federal employees are taking their work home with them -- something your agency might not allow. A whopping 50 percent of federal employees access work email from their personal device, and another 49 percent use their personal device for downloading work documents. This is only one example of the significant amount of data movement between personal and work accounts. Any organization -- federal or not -- should strive for visibility and control over where its data goes.



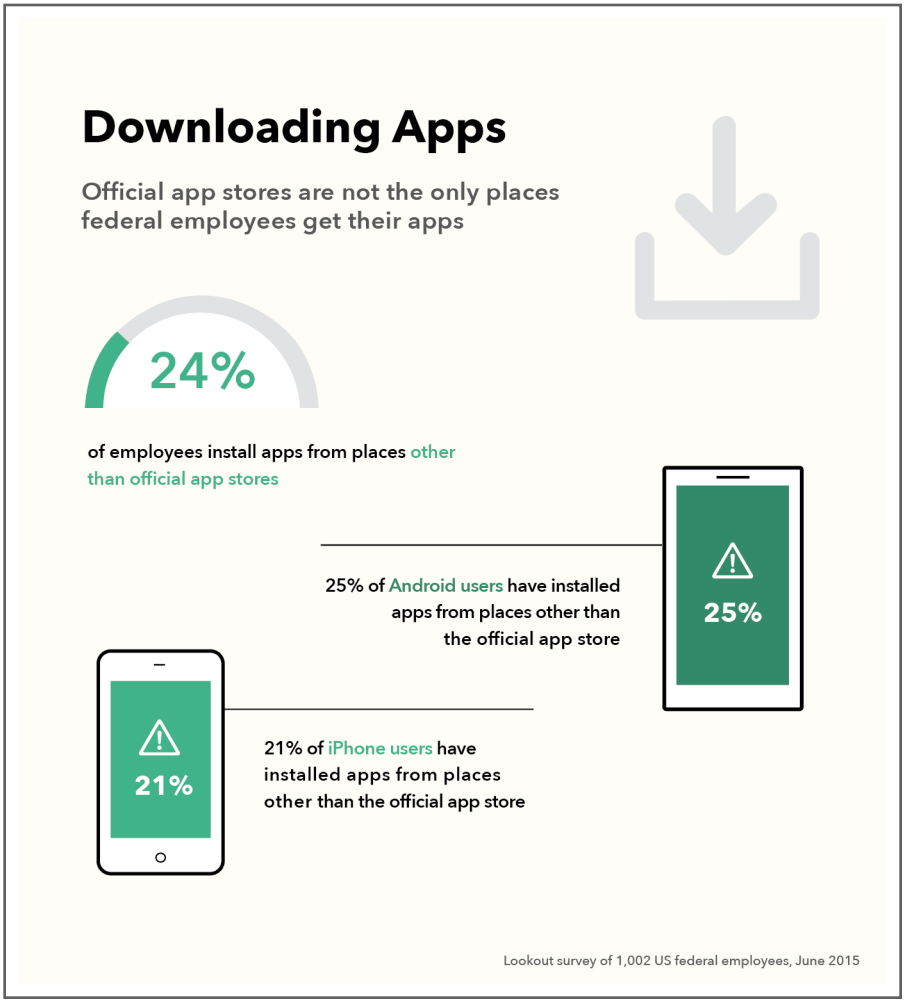
## It's not that hard to fundamentally change the security of your smart-device

A large percentage of government employees are accessing their work documents and communications on personal devices, but quite a few employees are also attempting to customize their device through jailbreaking or rooting. In fact, around seven percent of federal employees claim they jailbreak or root a device they bring to or use at work. That percentage is large enough to indicate that it's not just the tinkerers or the tech-y folks who are jailbreaking or rooting their devices, and it's not just Android users. Six percent of our survey's iPhone respondents reported jailbreaking their device, compared with the around eight percent of Android respondents who reported rooting their device. The problem is, while jailbreaking and rooting can be great for the security-saavy, it could expose operating systems to unpatched vulnerabilities and encourage downloading apps from third-party marketplaces known to have malicious apps.



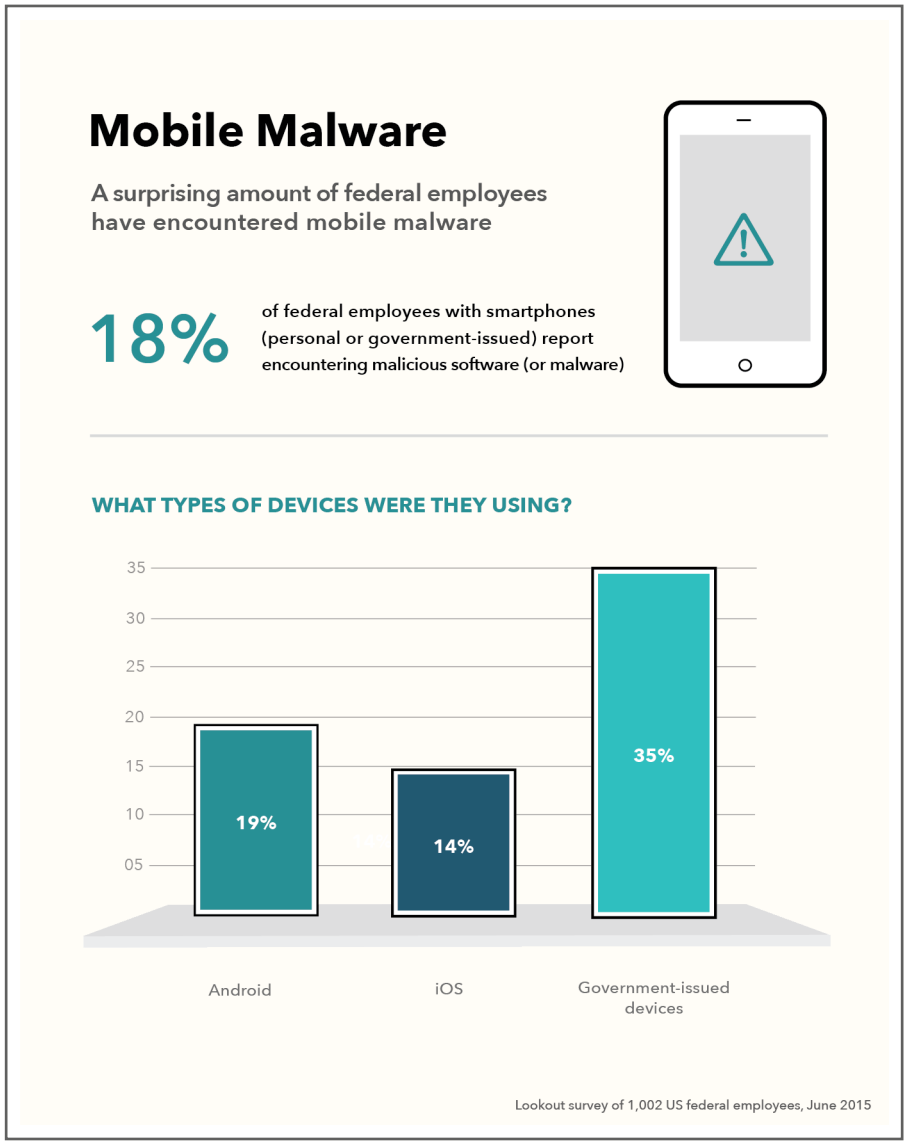
## There are potentially unvetted and unsecure applications connecting to your network

A surprisingly high amount of federal employees, 24 percent, are downloading applications from outside of official app stores, such as Google's Play Store and the Apple App Store. This can put a phone at risk because apps from outside of these stores are not guaranteed to have gone through the same vetting rigors that Google and Apple put their published apps through. This also highlights the myth that you can only download apps to an iPhone through an official app store, when, in fact, it's very easy to download an app to an iOS device through a website or link.



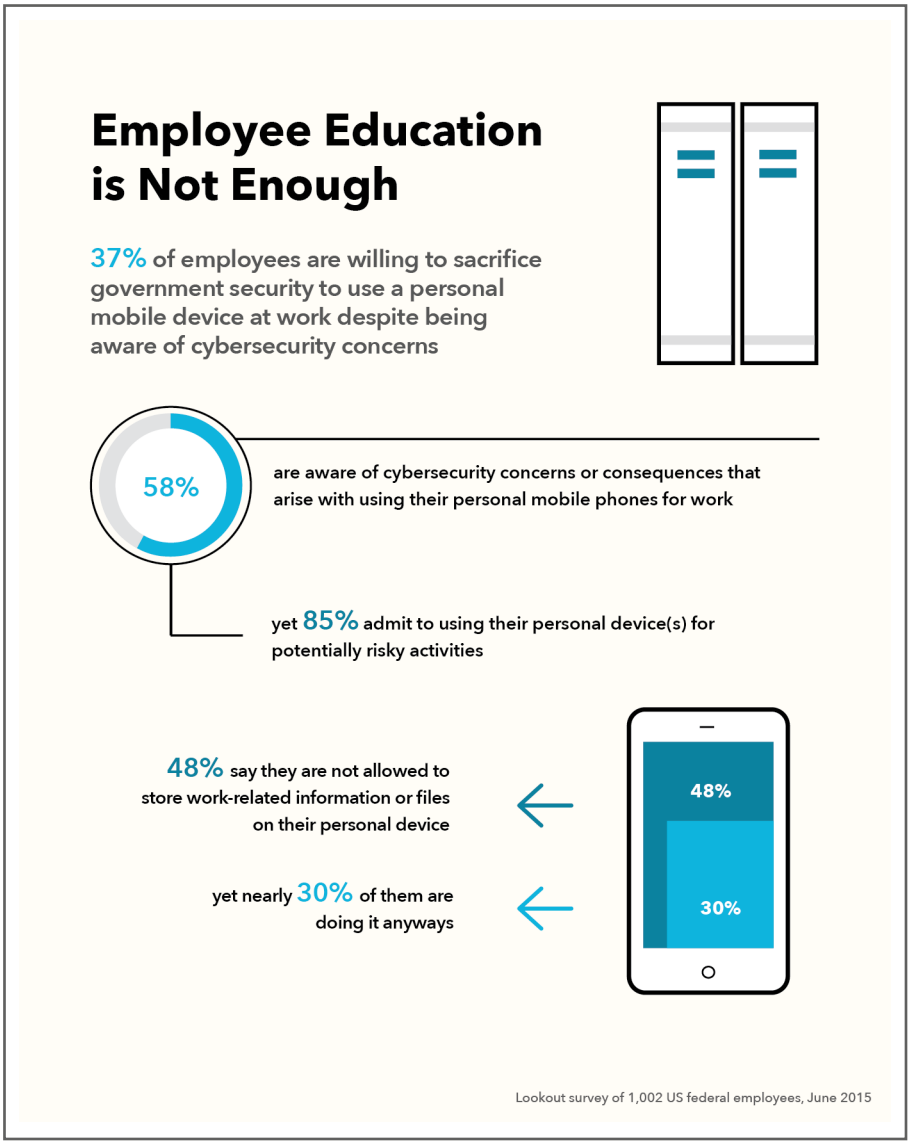
## The threats are real

A high percentage -- 18 percent -- of federal employees claim to have encountered malware on their mobile devices, including both personal and government-issued devices. While 19 percent of those were Android users, and 14 percent were iPhone users, these percentages are surprisingly higher than the 7 percent average Android malware encounter rate Lookout reported for 2014. Keep in mind that survey respondents are self-reporting and they might misinterpret their experience with potentially malicious software. Despite this reported encounter rate, however, 49 percent of federal employees still don't have a security app or solution installed on the mobile devices they use at or bring to work.



## Just teaching your employees about mobile security issues won't save your data

As it turns out, despite being aware of cybersecurity issues, federal employees are willing to sacrifice government security to use a personal mobile device at work. Fifty-eight percent of respondents report being aware of the security consequences of using their personal mobile phones for work, yet 85 percent of them will use their phone for potentially risky activities anyway. People value their convenience very highly and usually will take the path of least resistance to accomplish their goals -- risky or not. Employee education is important, but federal agencies need technology to back them up when education falls through.



## Conclusion

Employees increasingly expect to use their mobile devices in all aspects of their lives, and many organizations are struggling with how to balance that expectation with the need to secure sensitive data.

Many government agencies do not have a formal BYOD program, but this survey makes one thing abundantly clear: the lack of a formal BYOD program puts sensitive data at risk because employees are getting around the rules and using their devices anyway.

Progressive organizations have increasingly embraced personal devices in the workplace, taking advantage of today's device management and security solutions. Moreover, they view security as a holistic effort, of which mobile is a key component due to the prevalence of agency data being accessed.

Shadow BYOD should be a major security consideration for the federal government. To forget mobile when securing an agency is to leave the agency unsecured. The federal government needs to consider the devices that are on its networks because they are accessing data, whether they like it or not.

*Methodology: The survey was conducted on Lookout's behalf by Market Cube between June 19, 2015 and June 26, 2015 among 1,002 United States federal employees. The margin of error is 3.1 percent.*