Three Ways Employees Are Putting Your Organization At Risk

Employees in government organizations use iOS, Android and ChromeOS devices to stay productive and increase productivity as they telework. This makes them targets for cyberattackers because their devices are a treasure trove of data and a gateway to government infrastructure. You need to be aware of the risks inherent to a BYOD, remote, and mobile workforce.

1

RISK: 99% of Android users are running out-of-date operating systems. Failure to maintain the most current updates exposes your organization to hundreds of vulnerabilities. That's because mobile devices now provide the same access to your sensitive data and confidential information as traditional computer endpoints.

What you can do: You need to have mobile vulnerability and patch management capabilities in order to alert on outdated operating systems and identify the corresponding security patches. This will allow you to know where weaknesses exist and when they need to be updated.

2

RISK: Nearly 25% of state and local government employees use personal unmanaged devices. As a result, these employees are frequently exposed to phishing sites that put your organization at risk of credential harvesting and malware delivery.

What you can do: The first line of defense against phishing is an employee's ability to spot a phishing message. Your mobile endpoint security solution should contain in-app education so that employees are notified and educated every time a threat on their device is detected. Training should evolve beyond desktop and email to include challenges related to mobile phishing.

3

RISK: Cybercriminals are targeting your employees' mobile devices as an entry point for executing more invasive and personal attacks. In fact, credential theft attacks against federal agencies increased at a rate of 90 percent in 2020.

What you can do: Government agencies need mobile security that includes endpoint detection and response capabilities to proactively hunt for threats which have penetrated the environment via mobile attack vectors.

Summary:

Whether your employees' devices are managed, BYOAD, or BYOD, protecting these modern endpoints requires an approach that is built from the ground up for mobile. Only a modern endpoint protection solution can detect mobile threats in apps, operating systems and network connections while also protecting against credential harvesting and malware delivery attacks on your government employees.

Learn more about protecting your government agency today.

Lookout is FedRAMP JAB ATO and proud to serve federal government agencies.