

The four biggest security threats in financial services

Most financial services employees and customers today rely on tablets and smartphones to do business and conduct transactions. The apps they use are in the cloud, where the services and infrastructure are accessible from anywhere at any time.

But ensuring security and privacy for users, devices, apps, and data – and controlling who gets access to what – can pose formidable challenges. And reluctance to take on these challenges puts financial services organizations at serious risk.

Here are the dangers and what you can do about them:



RISK: Managed or not, mobile devices are at risk. The average quarterly exposure to phishing attacks against mobile devices increased by an imposing 125 percent from 2019- 2020*.

What to do: Ensure that employees and customers are keenly aware of the risks of mobile phishing attacks and explain how they are both different and more successful than attacks on desktop computers.



RISK: Mobile app threats are trending upward. The average quarterly exposure rate to app threats on mobile devices increased by approximately 15 percent throughout 2020*.

What to do: Understand the function and purpose of all apps in your mobile fleet and build access policies around them to protect data from cyberthreats and comply with data privacy laws.



RISK: Employees are exposed to hundreds of known vulnerabilities. About 27 percent of Android 11 devices and 79 percent of iOS devices had more than 50 vulnerabilities*, giving cyberattackers exploitable paths to steal financial data through mobile devices.

What to do: Reliable mobile vulnerability and patch management capabilities provide visibility into endpoints and apps, showing where security gaps exist and when to update them.



RISK: Protect the customer experience. In 2020, cyberattackers used complex malware, screen overlays, device rooting, and reverse engineering to steal customer login data on mobile devices*.

What to do: Be sure that software developers integrate security into customer-facing financial services apps. This reduces the risk attacks that can result in fraud, account takeovers and theft.

Summary:

With mobile as a catalyst for digital transformation in financial services, it's incumbent upon organizations to secure all users, devices, apps, and data –from endpoints to the cloud. Doing so with end-user privacy in mind enables financial services organizations to build and maintain a stronger security posture from endpoint to cloud without violating corporate and international data privacy and compliance laws.

Learn how to protect your financial services organization, employees, customers, and data.
lookout.com/solutions/financial-services



* Lookout Data, January 2020-December 2020