Mobile devices have been growing in importance, even as clouds and on-premises IT continue to dominate enterprise computing environments. 

Key findings from the Verizon Mobile Security Index 2021

Mobile devices have been growing in importance, even as clouds and on-premises IT continue to dominate enterprise computing environments. Mobile devices make it easy for businesses and individuals to communicate and access data, but they also introduce risks. The report is based on a comprehensive analysis of data collected from the Verizon Security Cloud platform through millions of customers, covering an annual period from January 1, 2020, through June 30, 2020.

Get actionable insights and recommendations to help keep your organization safe. Read the MSI 2021 report ➤

The bad news…

Security breaches remain a top concern for businesses, yet breaches are on the rise.

A too 'appy user can be a threat to your business.

Insecure networks remain a serious threat to mobile device security.

Fifty-three percent said the consequences they suffered from a mobile-device-related security compromise were major.

Ninety-seven percent consider remote workers to be at more risk than office workers.

Rules weren’t made for breaking.

People may make mistakes. They may lose things. Add in potential rule-breaking behavior, and it could create some very tempting targets.

Users and behaviors

Apps

Devices and things

Networks and cloud

Seventy-nine percent saw remote working increase as a result of COVID-19.

Forty-eight percent of those that sacrificed security said that one of the reasons why was dealing with the COVID-19 crisis.

Forty-nine percent of workers had allowed friends or family to use their work devices.

Three-quarters said their reliance on cloud-based apps is growing.

Ninety-three percent of Android® devices were running an out-of-date version of the OS.

Ninety-two percent weren’t taking any technical measures to block the use of public Wi-Fi, despite the risks.

There’s no such thing as free Wi-Fi.

Eighty percent of employees say they would use a public Wi-Fi network if it was available to them.

Twenty-seven percent of organizations that ban (but don’t block) the use of public Wi-Fi were aware that employees used it anyway.

One in 25 apps were found to leak credentials.

Ten percent of employees say they would use a public Wi-Fi network if it was available to them.

Forty-five percent of those that prohibit the use of social media on company devices were aware that employees used it anyway.

Three-quarters relaxed restrictions on installing new apps as part of their response to COVID-19.

Ninety-two percent of users were aware that their personal use of Wi-Fi is tracked and monitored by mobile devices.

Out of sight shouldn’t mean out of mind.

Users and devices connected to the Internet often travel with the end user, and attackers can take advantage of this to steal information or introduce malware. "Out of sight doesn’t mean out of mind."...