# Out of sight shouldn't mean out of mind.

## Key findings from the Verizon Mobile Security Index 2021

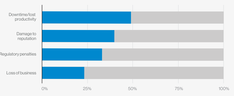

**71%**

**The majority of respondents to our survey said that mobile devices are "very critical to their business."***

* Answered 8 or more on the scale 1 (not at all critical) to 10 (extremely critical)

Mobile devices have been growing increasingly crucial to agility and productivity for years. And following COVID-19, that trend has accelerated rapidly.

When mobile devices suffer a compromise, the consequences can be severe and not just limited to data loss.





Now in its fourth year, the Mobile Security Index (MSI) offers a view into the threats facing mobile and IoT devices, as well as organizations' defenses and how often those fail. The report is based on responses from a survey 856 professionals responsible for the procurement, management and security of mobile devices, plus insights from 13 security companies and law enforcement agencies.

## The bad news...

**40%**

**Forty percent of respondents said mobile devices are the biggest IT security threat.**

**53%**

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

## Your home is no castle.

**79%**

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

But a big increase in mobile work can bring a big increase in potential risk.

**97%**

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

**48%**

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

### Users and behaviors

## Rules weren't made for breaking.

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

**54%**

**Fifty-four percent of companies that experienced a compromise attributed it, at least in part, to user behavior.**

**364%**

**increase in phishing attempts in 2020 versus 2019[1]**

**45%**

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

**600%**

**increase in visits to websites hosting adult content (on devices used for work)[2]**

### Apps

## You can be too 'appy.

The number of apps, especially web-based apps, used by organizations continues to grow. And more apps can mean more risk.

**75%**

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

**31%**

**Thirty-one percent relaxed restrictions on installing new apps as part of their response to COVID-19.**

**1 in 25**

**One in 25 apps were found to leak credentials.**

### Devices and things

## It's not always good to share.

Modern organizations rely on more and more devices. Many employees admit to allowing friends or family to use their company-issued devices.

**49%**

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

**56%**

**Fifty-six percent were worried about device loss or theft.**

**93%**

**Ninety-three percent of Android® devices were running an out-of-date version of the OS.[3]**

### Networks and cloud

## There's no such thing as free Wi-Fi.

Insecure networks remain a serious threat to mobile device security.

**92%**

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

**27%**

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

**Get actionable insights and recommendations to help keep your organization safe.**

**Read the MSI 2021 report >**

verizon

1 Lookout, analysis of all enterprise users covering January 2019 to December 2020.
2 Netskope, analysis based on anonymized data collected from the Netskope Security Cloud platform across millions of users from January 1, 2020, through June 30, 2020.
3 Lookout, based on analysis of all active Android devices, January 6, 2021.