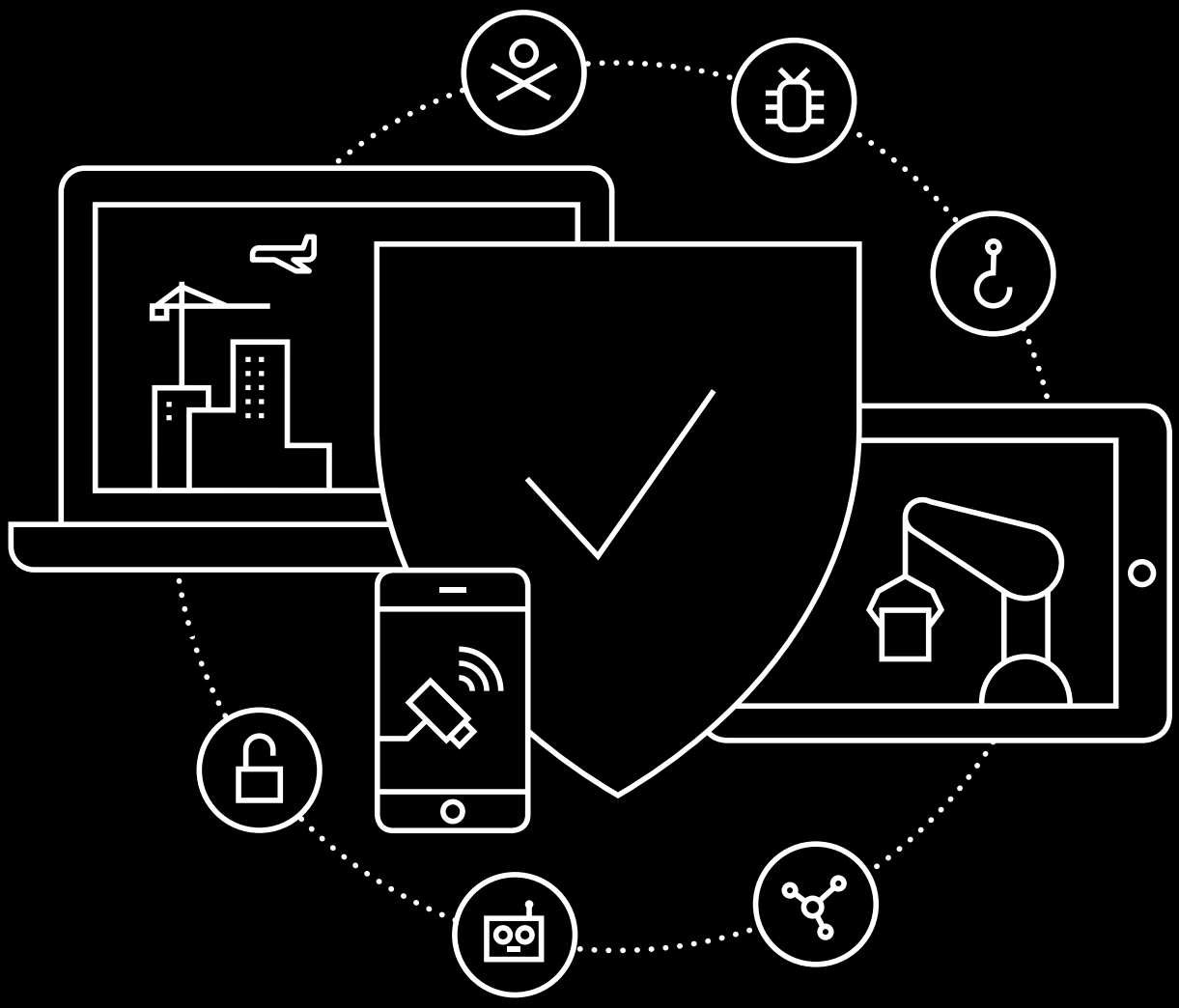
It's time to tackle mobile security.

Mobile Security Index 2019
Executive summary



verizon business ready

Be ready

Cybersecurity was all over the headlines again in 2018. There were many large and damaging compromises affecting retailers, airlines and credit rating companies, to name just a few. Many organizations weren't prepared and had sensitive data stolen or suffered downtime of key systems. Are you ready?

But largely absent from the headlines were compromises directly attributed to the vulnerability of a mobile device – such as a smartphone, tablet, laptop or connected device. Yet, we found that the number of companies admitting that they'd suffered a compromise in which a mobile device played a role went up – from 27% in the 2018 report to 33% this time around. So, where's the disconnect?

The answer lies in how little is normally made public about major incidents. We learn about the consequences, but not the details of how it happened. Often, attacks will start with phishing, getting an unsuspecting user to click on a malicious link. But that part of the story rarely makes it into print, never mind whether it was actually a tap on a mobile screen rather than the click of a mouse. You could say that none of the biggest breaches have been publicly attributed to mobile vulnerabilities; but a mobile element hasn't been ruled out either.

> Attackers are adapting to the mobile-first world and expanding their arsenals. 51% of sophisticated actors identified in the last 12 months were found to be targeting mobile devices as well as desktops[1].

Mobile devices now have access to much of the same valuable corporate data – customer lists, bank details, employee personal data, billing information and much more – as those using fixed connections. This means that the compromise of a mobile device can now be just as great a risk to your customer data, intellectual property and core systems.

That explains why our survey found that so many companies suffering a mobile-related compromise rated them as very serious. More than two fifths (41%) of those affected described the compromise as “major with lasting repercussions,” and even more (43%) said that their efforts to remediate the attacks were “difficult and expensive.”

Governments are starting to intervene to get organizations to take cybersecurity across all endpoints more seriously. Our research shows that this is starting to focus attention – the threat of multi-million, even multi-billion, dollar penalties tend to have that effect. But cybersecurity, and mobile device security in particular, cannot wait for regulation.

Read on to find out more about why you need to be ready, and how to improve your defenses.

More organizations were hit.

33%

A third of organizations admitted having suffered a compromise that involved a mobile device – up from 27% in our 2018 report.

And they were hit harder.

62%

And these weren’t trivial incidents. More than three fifths of those affected described the compromise as “major.” And 41% described it as “major with lasting repercussions.”

Mobile devices remained a weak spot.

67%

Two thirds of organizations said they are less confident about the security of their mobile assets than other devices.

And yet companies failed to put defenses in place.

45%

Less than half of organizations had mobile endpoint security in place. And the figures for other key protections – like anti-malware and mobile threat defense – were even worse.

And they continued to cut corners.

48%

Nearly half of companies admitted to sacrificing security to "get the job done." Those that did were nearly twice as likely to say they'd suffered a mobile-related compromise – 46% versus 24%.

The perception gap

Companies think that they are doing ok.

84% of organizations rated their existing mobile security measures as “effective," including a third (33%) that thought they were “very effective.” Almost four in five (79%) said that they're confident they’d spot a compromised mobile device quickly. And a similar percentage (77%) were confident that they would spot misuse by employees promptly.

This sentiment is not matched by events or actions.

But many aren't doing as well as they think.

A third (33%) of organizations admitted that they have experienced a compromise that involved a mobile device – up from 27% in the 2018 report.

Companies of all sizes were hit by mobile compromises

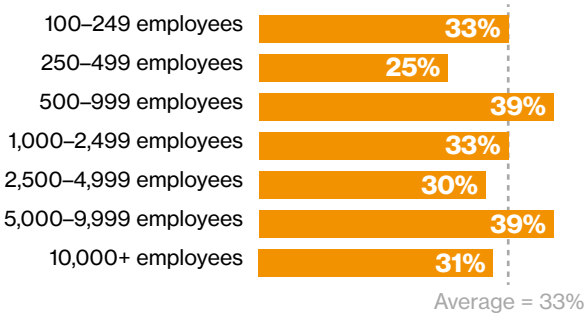


Figure 1. [Have you] experienced a security breach involving mobile devices during the past year? A breach is any security incident that resulted in the loss of data or system downtime.

Organizations across all sectors were affected

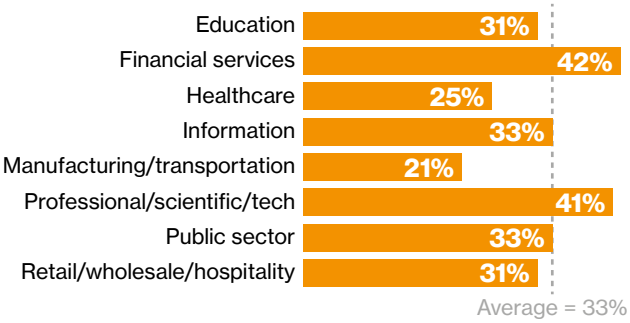


Figure 2. [Have you] experienced a security breach involving mobile devices during the past year? A breach is any security incident that resulted in the loss of data or system downtime.

This can't be accounted for solely by lost devices and relatively harmless things like adware infections. 62% of those that experienced a compromise described the event as “major,” and two fifths (41%) said that it had lasting repercussions.

Most companies found out from a third party

Figure 3. In which of the following ways were you made aware of the breach?

Refuting the belief that problems would be spotted quickly, the majority of organizations were made aware of a compromise by a third party.

Based on an analysis of privacy and security settings, 38% of mobile devices introduce unnecessary risk into the organization[2].

The bad actors keeping IT up at night.

While organizations are concerned about professional criminals, hacktivists and state-sponsored actors, they're even more worried about threats from within.

At 38%, employees topped the list of actors that respondents were most concerned about. Members of staff frequently expose their organizations to risk, both knowingly and unknowingly. Included in this number is the issue of negligence – employees making careless errors, losing their devices, using public Wi-Fi or circumventing security rules.

Organized criminal groups weren’t far behind. These groups are constantly adapting. As one device or platform becomes less vulnerable, they will move on to another. And they are constantly finding new ways to make money from their efforts. While “smash and grab” attacks are still common, there are much more sophisticated attacks too.

The tactics companies are concerned about.

We’ve broken threats and vulnerabilities into four layers: user behavior based, app based, device based and network based.

Malware was foremost amongst respondents' concerns

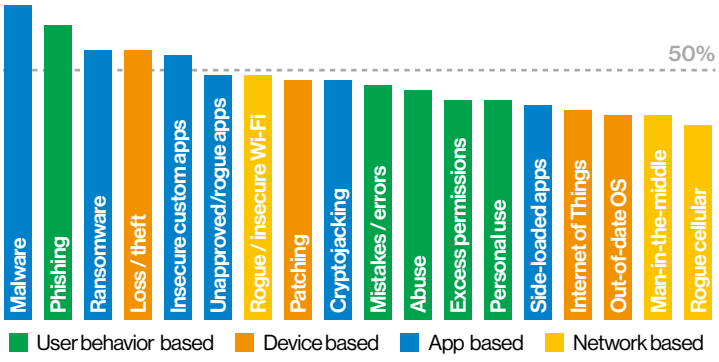


Figure 4. For each of the following mobile threats/vulnerabilities, please indicate whether you are aware of it, and concerned about it.

We look at these threats in more detail on the next two pages.

User behavior threats

Many threats come down to things that users do. This might be breaking policy, using a device for personal use, clicking on a malicious link, or installing an app and giving it permissions it doesn't need.

Phishing/business email compromise

Attackers often play a numbers game. They use automated tools and botnets to test the defenses of many thousands of devices. But some attackers take a more targeted approach. "Spear phishing" and business email compromise, also called CEO fraud, require more effort, but can be extremely effective.

> The FBI's Internet Crime Complaint Center (IC3) reported that victims of internet crime lost over $1.4B in 2017. 48% of that was due to business email compromise[3].

Users are more vulnerable to phishing on a mobile device. Many of the protective measures people typically take are not as easy: Who looks for the padlock, or hovers over the link to see the underlying URL? And mobile devices are much less likely to have endpoint protection installed.

> Enterprise users are three times more likely to fall for a phishing link when on a small screen (Android or iOS device) than when using a desktop OS, like Windows or macOS[4].

But it's not just email you need to think about – in fact, 85% of phishing attacks seen on mobile devices take place outside of email. While many organizations have filtering in place to block email-based attacks, far fewer have similar protection in place for these other routes[5].

Abuse/personal use

Defining what constitutes misuse of corporate resources can be tricky. For example, some companies will frown on the use of social media, but many others encourage employees – especially salespeople – to use it to do their job more effectively. How can companies differentiate between watching a cute cat video and an interview with the CEO of a customer?

Excess permissions

We all know that few people read the lengthy terms and conditions when upgrading the OS on a device or installing a new app. The page that lists what permissions an app wants is typically much shorter, but do users still just click "Ok" anyway? This could be exposing you to more risk than you think.

App threats

It's not just obviously questionable apps and websites that organizations need to worry about. App threats come in many forms. Even mainstream enterprise apps downloaded from the manufacturer's app store can be compromised or suffer from poor coding practices.

Malware

Malware remains at the top of the list of threats that companies are most concerned about. As well as "traditional" malware, our contributors have noticed an increase in attacks targeting two-factor authentication apps.

> During the first half of 2018, MobileIron identified known malicious apps on 3.5% of Android devices. Over 80% of the apps found with malware had access to internal networks and were scanning nearby ports[6].

Ransomware

This doesn't just affect personal computers and servers, there are mobile-specific forms of ransomware. In the past, these were seen to favor the Android platform as it presented fewer obstacles for app developers. But this is changing, at least one form of ransomware targeting iOS has been identified[7].

> Over 40% of all successful malware-based attacks involved ransomware[8].

Unapproved/rogue apps

Only two fifths (40%) of organizations said they limit users to installing apps from a recognized app store (like the Google Play store or the company's internal one). And just 3% totally blocked users from installing apps.

The official app stores aren't perfect. There have been several instances of rogue apps getting through, including some masquerading as popular messaging apps. But at least they have a degree of policing, unlike the Wild West of the internet.

Cryptojacking

In 25% of companies, at least one mobile device has encountered cryptojacking[9]. Infections are typically invisible and don't steal data or hijack credentials. But they aren't harmless.

The impact of even an "innocuous" infection can be severe. The disruption of reacting to the attack can be significant. But obviously the consequences of letting an infection through, even if it looks relatively innocuous, could be much worse.

Device threats

Devices can be subject to all kinds of vulnerabilities. And with numerous device types, multiple OSs, and numerous apps, keeping everything patched can be a daunting challenge – especially if you don't have the right tools in place.

Device loss and theft

There doesn't need to be any malicious intent for companies to suffer a loss of data and even downtime. People lose stuff. They leave smartphones, tablets and even laptops on planes, trains, taxicabs and ride shares. This shouldn't be too big a security threat, everybody uses the freely available precautions, right?

Wrong. Less than a third (31%) of companies use whole disk encryption and up to 5% of devices don't have a lock screen configured[10].

Internet of Things (IoT) devices

Over three quarters (76%) of respondents said that they think IoT devices are the greatest cybersecurity threat facing organizations. A lot of the issues with protecting IoT devices stem from difficulties accessing and managing them.

Many IoT devices don't have the storage or processing capacity to run traditional methods of protection. And because they often operate in remote locations, they can be susceptible to physical tampering and be harder to patch.

As IoT becomes more integrated with business processes and companies come to rely on it more, the damage a compromise could cause grows. Nearly two thirds (64%) of those that said they'd suffered a mobile-related compromise said that the consequences included downtime.

Out-of-date operating system and unpatched apps

It's not just about major versions – like iOS 12 and Android Pie. With new threats and vulnerabilities emerging all the time, even being a few minor versions behind could pose a significant risk.

In 2018, 693 Android and iOS entries were added to the CVE database*. Over two fifths (43%) of these had a CVSS** score of 7 or greater, indicating they were severe and exploitable[11].

Except in very special circumstances, each device has only one OS. Most have tens or even hundreds of apps, making keeping them up to date a much tougher challenge.

Network threats

To paraphrase a famous saying, there's no such thing as free public Wi-Fi. At best, users are swapping privacy for convenience. At worst, they could be compromising credentials to other systems and exposing devices – not just the one they're using, but every one it can connect to – to malicious code.

Insecure networks

Employees connect to an average of 12 Wi-Fi hotspots per day[12]. Unfortunately, not all access points can be trusted. Nearly 2% of mobile devices have connected to a rogue access point (one set up to imitate a legitimate network)[13].

Employees are taking risks, even when told not to

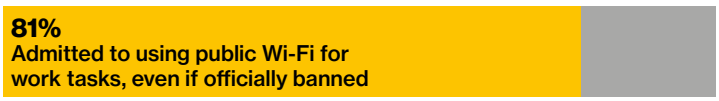


Figure 5. Do you use public Wi-Fi for work purposes?

Four fifths of respondents (81%) admitted to using public Wi-Fi for work, even when many know it's prohibited. When you look at just those respondents responsible for managing the security of devices, that figure is even higher (82%).

This suggests that even the most savvy users let convenience take precedence over what they know is right, and they are prepared to risk the consequences. This supports our observation that actions don't match concerns.

Interception attacks

One of the most serious types of threat involves the interception of all network traffic. This can be achieved by creating a rogue access point or using a man-in-the-middle (MitM) attack. These techniques enable attackers to capture any data transmitted, including credentials, emails and data submitted to web forms.

And yet, just half of companies had a solution in place to encrypt all traffic to protect users from this kind of attack:

- 28% were using an over-the-top (OTT) or SSL VPN
- 27% were using a mobile private network
- 21% were using a mobile web gateway

In the first half of 2018, more than one in seven (15%) protected devices detected an MitM attack[14].

* Common vulnerabilities and exposures system maintained by The National Cybersecurity FFRDC, funded by Homeland Security.
** Common vulnerability scoring system, https://nvd.nist.gov/vuln-metrics/cvss

What's being done?

For over a decade, year after year, the Verizon Data Breach Investigations Report (DBIR)[15] has found that many companies are taking the same gambles – and losing. Many are failing to take even basic precautions, and as a result, they are exposing themselves to greater risk of downtime and massive damage to their reputation.

It's worrying that our data shows that attitudes to protecting mobile devices are much less sophisticated than those of defending servers and personal computers.

What will drive companies to take mobile security more seriously?

2018: The year of regulation.

Governments are doing more to regulate privacy and data security. The big news of 2018 was clearly the General Data Protection Regulation (GDPR). It is by far the most ambitious and wide-ranging data protection law yet enacted. And while it's a European Union (EU) regulation, legislated by the 28 member nations, it has a global impact – any organization doing business in the EU, whether based there or not, is covered.

In fact, we found that over three quarters (78%) of the US-based organizations that we surveyed said they had changed IT security policies in light of it. The well-publicized scale of potential penalties was almost certainly a driving factor.

The threat of increased penalties has driven increased spend

Figure 6. Do you agree with the statement "The threat of increased regulatory penalties has been a major driver of increased security spending over the past year"?

GDPR wasn't the only new kid on the block. As of March 2018, all 50 states in the US have mandatory breach notification laws in place. Several updated their regulations during 2018, and several are actively considering more wide-ranging laws.

But cybersecurity is moving too fast to wait for regulation. Companies need to take responsibility for their data and the privacy of their customers and take action now.

Sadly, many aren't.

Companies aren't doing enough.

Mobile devices are prone to many of the same attacks as other devices. Most phishing attacks and badly coded sites can affect them equally, mobile users might even be more vulnerable. And there are also mobile-specific exploits – like malicious apps and rogue wireless hotspots.

And yet again this year, we found that many companies are failing to protect their mobile devices. And we're not talking about some almost-impossible-to-achieve gold standard. We're talking about companies failing to meet even a basic level of preparedness.

Confidence in mobile device security is lower

Figure 7. Do you agree with the statement "I'm less confident about the security of our mobile devices than other systems"?

Two thirds (67%) of organizations said they are less confident about the security of their mobile assets than other devices. A fifth (21%) strongly agreed with that statement.

This isn't surprising. As we've seen, many organizations don't have even the most basic protections in place – despite mobile security spend going up.

Most (64%) saw their spend rise in the past year – this could be additional remediation costs as more faced dealing with compromises. Even more (69%) expect their spend to rise in the next 12 months. Only 24% won't have seen an increase over the two year period.

Money's not the problem.

Budget was cited as a significant barrier by just 28% of respondents. And as in the Mobile Security Index 2018, lack of C-level support came at the bottom of the list of barriers to improving mobile security. The top three answers offered all revolve around expertise, or lack of it.

Respondents said that their organization lacks sufficient understanding of the threats and the skills to tackle them, and their users aren't adequately prepared.

Are you ready?

Companies need to put in place measures across the whole security cycle: assess, protect, detect and respond. And they should implement systems to enforce the rules and spot non-compliance automatically. Many companies already take this approach for other IT systems, lots more are working towards putting it in place. It's time to include mobile devices in the plan.

See our Baseline, Better, Best matrix on the next page for some suggestions on how you can get started or move up to the next level of mobile device security.

And see the back page for links to the full Mobile Security Index 2019, industry-specific snapshots and other publications.

Mobile security: Baseline, Better, Best.

		Baseline	Better	Best
Assess Understand your devices, your data, who has access, and what the threats are.	Implement	• Ensure mobile is included in all your security plans and policies • Understand risk factors including geolocation, industry, size, and critical data streams • Understand and manage your employees' data usage	• Take a full accounting of your assets to determine risks and potential exploits • Track updates and patches and coordinate deployment • Define guidelines for acceptable use, including file transfer	• Measure your environment against applicable regulatory frameworks • Establish a security-first employee focus and culture • Implement a risk evaluation and scoring framework
	Maintain	• Regularly assess defenses to confirm that detection capabilities meet set standards	• Test employee mobile security awareness at least once a year	• Perform regular, at least quarterly, 360° reviews of mobile threat landscape and security posture
Protect Harden assets, protect data and secure the emerging mobile perimeter.	Implement	• Deploy a device enrollment policy • Implement a strong password policy and verify adherence • Limit Wi-Fi to approved networks • Prevent employees from installing apps downloaded from the internet • Establish formal policies for corporate-liable/BYOD detailing employees' responsibilities	• Implement a unified endpoint management (UEM) system to pre-configure devices with approved apps, limit additions to company app store and set/manage policies • Deploy a private network solution to any device that gathers or accesses sensitive data • Leverage voice, messaging and file encryption solutions	• Implement device segmentation, keeping personal and work data and applications separate • Change device procurement policies to favor cellular over Wi-Fi • Develop governance policies for the transfer of data between IoT devices
	Maintain	• Regularly review access to systems and data	• Identify users who are out of compliance or misusing assets	• Use activity-based monitoring to block malicious behavior
Detect Identify vulnerabilities and anomalies quickly to enable speedy response to reduce impact.	Implement	• Deploy mobile threat detection software to scan for vulnerabilities • Implement log monitoring to spot signs of attacks and device misuse	• Introduce a solution to identify and prevent complex phishing attacks – including those happening outside email • Implement processes to identify devices that are out of compliance	• Introduce data visibility and content control tools • Deploy secure productivity apps to protect collaboration • Implement secure IoT device visibility and management platform
	Maintain	• Provide regular security training on the dangers associated with mobile devices and how to spot warning signs of an incident	• Review apps to identify anomalies such as excessive permissions and potentially dangerous behavior like scanning corporate networks	• Use data loss prevention (DLP) tools to limit data transfer, provide early warning and enable forensics
Respond Remediate issues, recover operations and enable forensic analysis.	Implement	• Implement policies to contain attacks by locking down private information and isolating infected, lost or stolen devices	• Create an incident response plan that informs employees of what to do in the event of an incident • Implement push messaging to tell users and admins what to do in the event of an incident	• Automate corrective actions to reduce response time and limit exposure • Implement employee-friendly policies and solutions tailored to BYOD security
	Maintain	• Remind employees how to report any suspicious activity – make it an easy-to-remember email address or phone number	• Exploit the complete range of UEM capabilities to identify full range of threats and trigger responses	• Run regular response exercises on areas of concern (e.g., phishing)

About Verizon

Verizon is a global leader in technological innovation, from mobility and networking to business communications. Our 4G LTE network is the largest in the US, and it's now available in more than 500 markets from coast to coast.

As one of the largest network providers, we draw on the experience of our cybersecurity experts and help to protect valuable information for organizations of all sizes. Our global Network Operations Centers and Security Operations Centers process more than one million security events every day, so we understand the rapidly changing nature of cyber threats.

We're the only provider recognized by industry analyst firm Gartner as a leader in both Network Services and Managed Security Services in its 2018 Gartner Magic Quadrant reports.

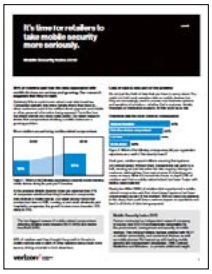
We offer world-class products to secure mobile devices, content, and applications. With Verizon, you can choose the security solution to best meet your business needs.

Learn more >

More on mobile security.

Mobile Security Index 2019
The full version of this report, packed with additional findings and insight. This is written for security professionals and those responsible for procuring, managing and securing mobile devices for their organization.

Read the full report >



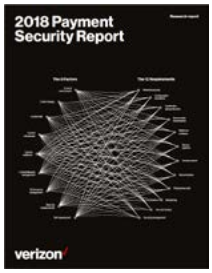
Industry snapshots
Detailed insights into the state of mobile security in finance, healthcare, public sector, manufacturing, and retail organizations, as well as at small companies (up to 499 employees).

Read our snapshots >

Other Verizon security publications.

Data Breach Investigations Report
For over a decade, Verizon's Data Breach Investigations Report (DBIR) has been one of the IT industry's most respected security publications. It's based on analysis of thousands of confirmed data breaches and tens of thousands of security incidents.

Download the latest edition >



Payment Security Report
Almost half (47.5%) of organizations that achieve PCI DSS compliance fail to sustain it until their next annual assessment. Read the Payment Security Report to discover which controls they failed to maintain, and how you can avoid the same fate.

Download the latest edition >

References

1. Lookout analysis of data aggregated from its 70M+ corpus of apps and 170M+ users of its mobile endpoint products between October 2017 and October 2018.
2. MobileIron, Global Threat Report Mid-Year 2018, 2018, Based on analysis of privacy and security settings like whether a device has "developer options" enabled, is jailbroken or rooted, has necessary security settings like encryption and PIN codes disabled, has code signing deactivated, has apps from unknown sources or harbors malicious profiles.
3. https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718
4. Analysis by Lookout between October 2017 to October 2018
5. Wandera Mobile Threat Research, Mobile phishing report 2018, May 2018
6. MobileIron, MobileIron Global Threat Report Mid-Year 2018, 2018
7. https://www.wandera.com/beware-ios-malware/
8. Verizon, 2018 Data Breach Investigations Report, April 2018, https://enterprise.verizon.com/resources/reports/dbir/
9. Over a one-year period (November 2017 to October 2018) Wandera Mobile Threat Research identified that 25% of organizations within their mobile-enabled user base experienced a mobile cryptojacking incident. Cryptojacking scripts were observed in web pages, mobile ads and in connected mobile apps.
10. Wandera Mobile Threat Research. Analysis of common configuration vulnerabilities. Covered enterprise mobile devices in production environments during a one-year period (November 2017 to October 2018).
11. MobileIron analysis of CVE data.
12. Wandera Mobile Threat Research, Mobile Wi-Fi Security Report, 2018
13. MobileIron, Global Threat Report, mid-year 2018
14. MobileIron, Global Threat Report, mid-year 2018
15. Verizon, Data Breach Investigations Report, 2018, https://enterprise.verizon.com/resources/reports/dbir/

verizon business ready