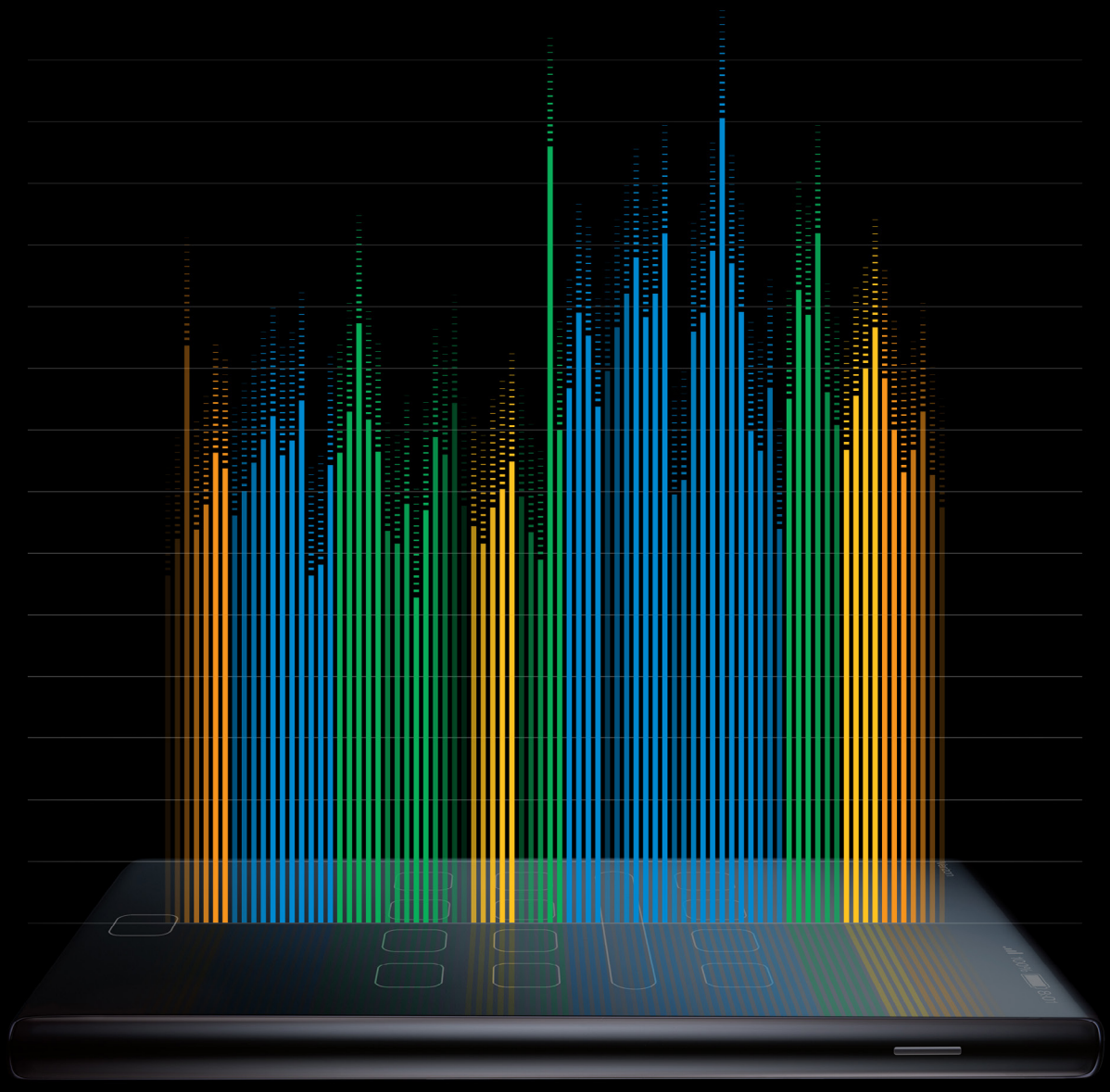
Mobile Security Index 2021

Public Safety Spotlight

A deep dive into mobile security in local, state and federal government agencies



verizon

The future of mobile security

A successful mission is at the heart of every public safety leader. The drive these leaders feel toward supporting their communities or nation has led to the creation of new strategies, devices and processes by this practical and forward-looking group. Technology and information are accelerating with the adoption of purpose-built devices, advanced connectivity, devices designed to public safety specifications, artificial intelligence, cloud services, virtual reality and more. In turn, these innovations have transformed first response in important and exciting ways.

As the adoption of technology grows, so does the exposure to cyberthreats.

> **"All of the planning and preparation that goes into being ready to respond to events can be thwarted by cyberattacks that bring you to your knees."**
>
> —Jerome Hauer, Ph.D, Former Commissioner, New York State Division of Homeland Security and Emergency Services

Consider that more than one-third* of public sector organizations report having 1,000 or more Internet of Things (IoT) devices in use and 7% had 10,000 or more. The ability to monitor the location of people, assets and vehicles; track physical facilities; and enable digital services for constituents have driven IoT adoption. This will only increase further as 5G opens up new use cases. But new endpoints mean more opportunities for hacking by malicious individuals or groups.

Attacks on the public safety community are not unique; all digitization efforts—whether public or private—attract threats. Securing the public safety community has always been an issue to grapple with. The public safety community must deal with "hacktivist" attacks driven by social or political agendas; an increase in remote working; the increased value of personally identifiable information (PII); and perceived weaknesses in security and defense measures. But the stakes are higher when life, property and safety are on the line. Plus, cybersecurity breaches also can erode community confidence and trust.

* All statistics are from the Verizon Mobile Security Index 2021 report unless otherwise noted.

Our research found that, like other sectors, public sector organizations sacrifice security due to budget constraints, resource constraints, concerns around speed and efficiency, and pressure to deliver new user and constituent experiences quickly. Furthermore, public safety leaders may mistakenly believe they are not at risk, thinking hackers have more lucrative prospects.

Mobile users, cameras, IoT devices and edge sensors connected to mobile wireless networks are the norm in public safety. Two-fifths of public sector respondents said that mobile devices are "10 - extremely critical" to the efficient operations of their organization. And, nearly three-quarters (72%) scored the importance as "critical"—8 or more on the 10-point scale. As more and more mobile devices are connected to wireless networks, it will become increasingly difficult for public safety IT teams, which are already strapped for resources, to protect every endpoint. This can create both new ways and more opportunities for hackers to carry out attacks.

More than 25% of public sector organizations admitted to having had a security compromise involving a mobile device in the past year. And remediation can be painful, expensive and time-consuming, with 68% of public sector organizations reporting it to be complex and expensive. Perhaps more detrimental are the hits to community and citizen confidence. For example, 70% of public sector respondents to our survey said that a security compromise could put people's lives at risk by impacting critical or emergency services.

Now is the time for public safety leaders to have an honest look at security protocols and processes to ensure that as leaders, they are taking a hard stance against threats. Like all successful response efforts, planning is essential. Here are some ways you can better support your mobile security goals.

> **"There are a lot of investment decisions that need to be equalized in order to have the right tools, network and technology for responding. In doing so, part of that investment has to be in better digital security."**
>
> – Ellis Stanley, Former Director, Atlanta-Fulton County Emergency Management Agency, and Former General Manager, Emergency Preparedness Department, City of Los Angeles

> **"Digital security is not a nice-to-have, it's a must-have for building and sustaining trust and credibility."**
>
> – Scott Thomson, Former Chief of Police, Camden County, NJ

Plan of action

1. **Stay tuned for the release of the Verizon Mobile Security Index 2021 report and read the report**
2. **Visit our website to learn more about Verizon Frontline and our commitment to the first responder community**
3. **Contact one of our sales representatives, who can answer questions and provide a security assessment for all your security needs**
4. **Share this report with your peers**
5. **Follow us on Twitter and LinkedIn**

Could a compromised mobile device put your staff and constituents at risk?

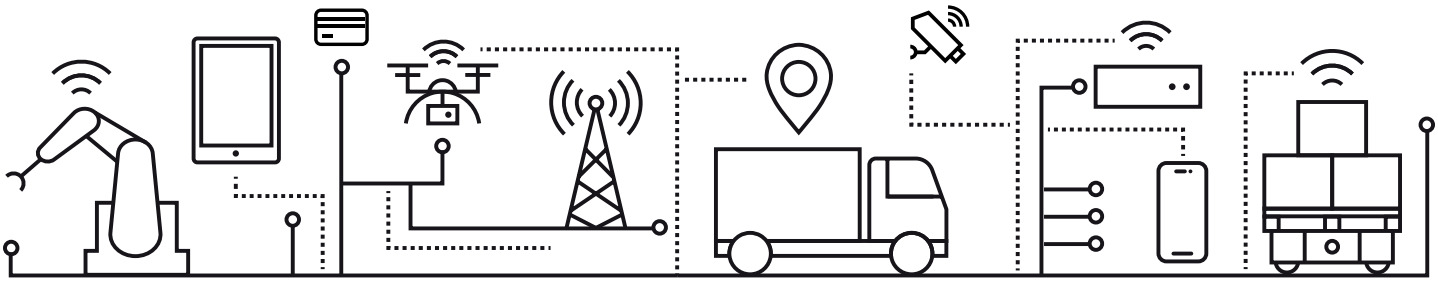
The remit of public sector organizations ranges from the everyday to matters of life and death. Like private sector organizations, they are under pressure to make services easier to access, but the pressure on budgets is often more severe and the potential consequences much higher. Mobile devices are key to improving service delivery, but they could be exposing infrastructure, constituents, employees and data to greater risk.

Mobile technology, including IoT devices, is crucial to enabling local, state and federal government organizations to help improve service delivery. It's empowering staff to serve constituents more effectively, even when they're unexpectedly forced to work from home. And mobile technology is providing constituents with easier access to important services and functions, from policing to planning applications and from providing education to offering business grants.

70%

A large majority of public sector organizations said that a security compromise could put people's lives at risk, by impacting critical or emergency services.

In 2020, we contracted with an independent research company to survey senior professionals responsible for the procurement, management and security of mobile devices. In total, 856 people responded; close to a quarter of them (23%) were from public sector organizations. Unless stated otherwise, all data in this report is from this survey.



One in four suffered a compromise.

When it comes to cybersecurity, public sector organizations have a lot at stake. Government entities often hold extensive data on the lives of their constituents—including information most people wouldn't share with private companies, such as their tax details and Social Security numbers.

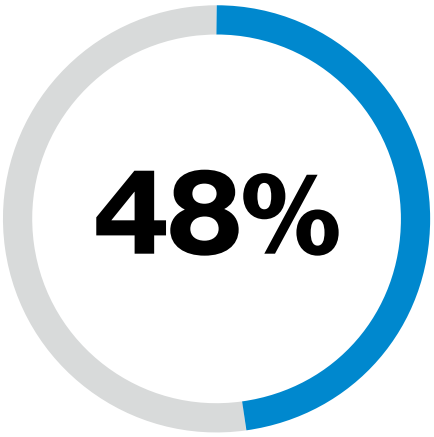
A quarter (25%) of public sector respondents admitted to having suffered a compromise involving a mobile device in the past year.

Local, state and federal organizations were all affected. State government bodies fared best, with less than one in eight (12%) reporting they'd been hit; conversely, nearly one-third (32%) of local government agencies were aware of having been compromised.

Most said the consequences were major.

Nearly half of the respondents that said that their public sector organization had experienced a mobile-related compromise said that the effects were major, and 63% of those said that the repercussions were lasting.

The top three consequences of a compromise that public sector organizations were concerned about were loss of data (53%), disruption to operations (38%) and increased risk to employee safety (37%).



Nearly half of the respondents that said that their public sector organization had experienced a mobile-related compromise said that the effects were major, and 63% of those said that the repercussions were lasting.

Remediation was often difficult and expensive.

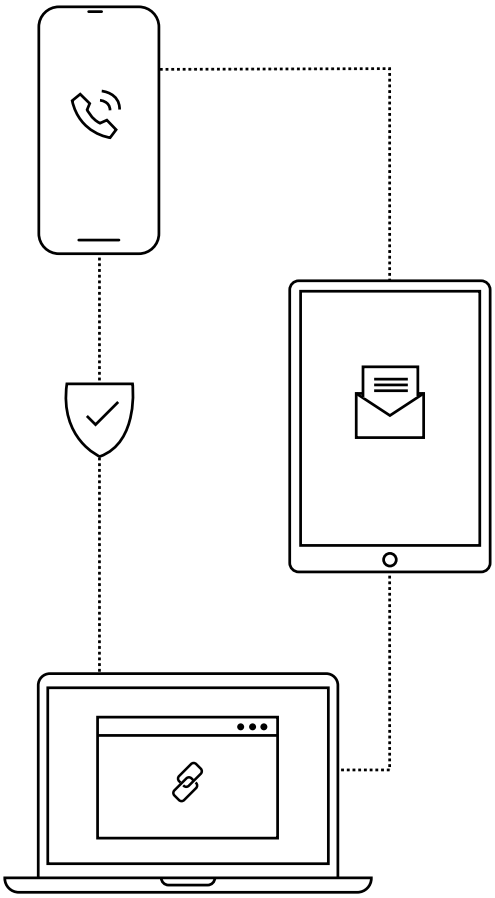
In 2018, the City of Atlanta reportedly spent over US$2.7 million on putting things right following an attack.[1]

In our survey, 68% of public sector organizations that had suffered a mobile-related compromise said that remediation was not "simple and cheap"; 29% said it was "difficult and expensive."

But public sector organizations still cut corners.

Despite the likelihood of being compromised and the consequences when it happens, 35% of public sector respondents admitted they had sacrificed mobile security to "get the job done." This is about the same as last year (36%) and noticeably lower than what we found across all public and private organizations (45%).

The two most commonly cited reasons for sacrificing security were expediency (40%) and coping with the COVID-19 crisis (45%).



40%

Two-fifths of public sector respondents said that mobile devices are "10 = extremely critical" to the smooth running of their organization. Nearly three-quarters (72%) scored the importance as 8 or more on the 10-point scale.

82%

More than four out of five public sector organizations said employee expectations for remote or flexible working were forcing them to reevaluate how they operate.

70%

Seven in 10 public sector organizations said the public's expectations for increased online services are putting greater pressure on their budgets.

The biggest concerns in the public sector

Public sector organizations are concerned about mobile device threats; 84% rated the risk to their organization as moderate to significant. They're worried about a diverse range of threats, but many think their existing defenses are adequate.

The five most common concerns for public sector organizations

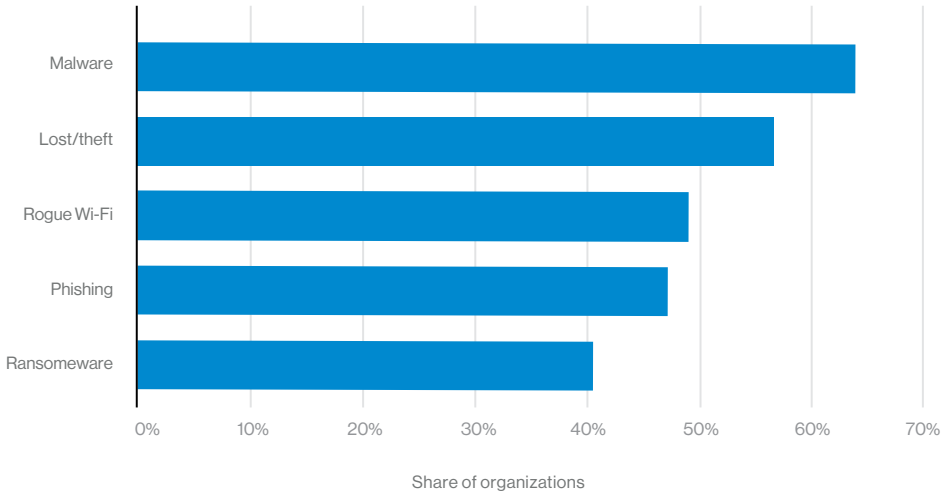


Figure 1. Please indicate which of the following threats/vulnerabilities you're concerned about—which you think is a threat and feel unprepared to handle.

Malware

Malware topped the list of threats and vulnerabilities that public sector organizations were most concerned about. In reality, mobile-device users are 26 times more likely to click on a phishing link than they are to encounter malware.[2]

Based on data from Wandera, the encounter rate for malware dropped year-over-year since the previous edition of this report. In 2020, over 8% of organizations had at least one malware incident. That's down from 10% in 2019, but up from 2% in 2018.[3]

Lack of employee awareness is a problem. Nearly 30% of U.S. workers said they thought that malware is a type of hardware that boosts a Wi-Fi signal. This serves as an important reminder that what might seem obvious to those working in IT and well-read on cybersecurity may be a mystery to many others. There's still a lot to do in educating employees about the threats and how to counter them—both in their personal lives and as government officials.

Loss/theft

People lose stuff. They leave phones, tablets and laptops in taxis, on trains, at restaurants—the list goes on and on. Some of these will end up in a lost-and-found box, and others will find a new owner—or rather a new owner will find them.

Loss/theft is one of the types of compromises that's easiest to mitigate. Protections like device encryption and remote wipe are now standard with most types of user devices and mobile device management (MDM). But that doesn't mean that people are using them.

One-third of organizations had at least one device without a lock screen enabled.

Rogue Wi-Fi

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 and exposing other systems—not just the device that they're using, but everything it can connect to—to malicious code.

The dangers of public Wi-Fi are increasing as mobile devices are used for more tasks. Nearly two-fifths (38%) of public sector organizations that admitted to having suffered a mobile-related compromise said that public Wi-Fi played a role in it.

Phishing

Lookout, a mobile security company, saw a 364% increase in the number of mobile phishing attempts in 2020 versus 2019.[4] With many employees working from home, cybercriminals have adapted their techniques. And many have taken advantage of the disruption.

Cloud-based applications can make phishing attacks more effective and facilitate business email compromise (BEC) attacks, which are the leading cause of financial loss in cyberattacks. The extensive control granted to users by Microsoft 365 and similar services can give attackers in possession of stolen credentials a critical foothold inside the target organization.

Ransomware

There has been extensive media coverage of successful ransomware attacks on public sector organizations in recent years.

In September 2020, the Clark County School District in Las Vegas, the U.S.'s fifth largest, was hit by a ransomware attack targeting the personal data of the district's 320,000 students.[5] But it's not just data that's at risk. In November 2020, Baltimore County Public Schools, another of the biggest school districts in the U.S., was closed for three days following a ransomware attack.[6]

This publicity has both elevated ransomware as a concern and driven organizations to improve their defenses. "White hat" hackers have also published tools to decrypt computers affected by attacks using common ransomware kits and variants. In response, attackers have adapted their tactics.

Instead of simply locking the files on the infected device, newer variants target files you have stored in online services like Google Drive and Microsoft 365. An even more alarming variation is doxware (or leakware), where the hacker increases the incentive for the target to pay up by threating to publish the affected files online.

Security shouldn't be a burden.

Our data suggests that, in addition to worrying over budget constraints, decision makers are also concerned about the impact security measures can have on productivity and efficiency.

It's true that poorly designed or implemented security policies can be bad for the employee experience and organizational performance. Something as simple as a password policy could impede productivity, increase support costs (due to more resets) and potentially increase risks (by driving employees to circumvent the rules).

On the other hand, well-implemented security solutions can dramatically reduce risk and remain largely transparent to users. Effective tools can also help reduce the burden on IT teams, provide better reporting and increase visibility into user adherence with policies—including users working from home.

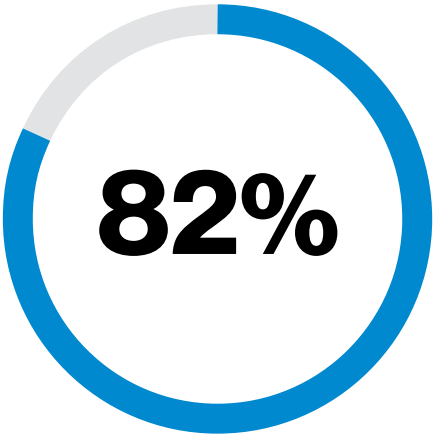
88%

The majority of public sector respondents said that being able to take a future crisis in stride was key to their planning and investment.

> **"We know that cybercriminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the coronavirus outbreak."**
>
> —Paul Chichester, Director of Operations, National Cyber Security Centre (NCSC)

9%

Public Wi-Fi can be dangerous, but less than 1 in 10 public sector organizations blocked its use. A further 22% have a policy banning its use, but 47% of those are aware that employees use it anyway.



Nearly five out of six public sector respondents said they think that organizations like theirs need to take mobile device security more seriously.

Public sector IoT: Increase of threat?

The volume and variety of devices using wireless connectivity has grown massively. Smart IoT devices are transforming public services, enabling smart city infrastructure and improving support for the armed forces. But cyberattackers see innovation as an opportunity.

36%

Over a third of public sector organizations said that they had 1,000 or more IoT devices in use. Over 7% had 10,000 or more.

The safety of people and assets topped the list of purposes public sector respondents said they're using IoT for:

- **Movement (36%):** Monitoring the location of people, vehicles and other assets
- **Security (36%):** Monitoring the physical security of buildings and other property
- **Experience (29%):** Enabling services like digital signage

To investigate the risks of IoT, we interviewed an additional group of professionals responsible for the procurement, management and security of these devices. Just short of half (49%) of these respondents said that their organization was at significant or high risk from attacks on their IoT devices. And 26% said they had already suffered a compromise involving an IoT device.

49%

Nearly half of the IoT respondents in our survey said that these devices posed a high or significant risk to their organizations.

Despite their fears, 67% of respondents said they had sacrificed IoT security to "get the job done." Why are they cutting corners?

- Responding to COVID-19 (43%)
- Need to meet profitability targets (40%)
- Expediency or time pressures (39%)

In the drive to meet targets, security often takes a back seat. Three-fifths (61%) of our respondents said IoT device security isn't a priority for version 1.0; it's something they can "worry about later."

Securing your IoT devices

Fortunately, there's a lot that can be done to improve IoT security. In addition to following our recommendations for all mobile devices, implementing these four IoT-specific best practices could help you protect your organization:

1. Review security before you buy anything.
Whether you are buying off-the-shelf solutions or components to build your own IoT devices, ask potential vendors to supply details about the security measures they take and review them for robustness. Pay particular attention to their authentication, encryption and patching policies. Seventy-six percent of respondents said they had IoT devices in remote or difficult-to-access locations. Use over-the-air (OTA) updates to help keep these devices secure.

2. Harden all devices before attaching them to your network.
Make sure that the device itself is tamper-resistant and tamper-evident. Then make sure you change all default or vendor-supplied passwords. Also, reduce exposure by shutting down anything you don't need—if you're not using a port or protocol, block it.

3. Encrypt data in transit and at rest.
Eighty-three percent of respondents said that they are collecting PII, and 25% of those weren't encrypting it. Encrypting data can make it useless to hackers and help you mitigate the risk of a reputation-destroying data breach.

4. Use an IoT platform.
Choose an IoT platform that enables you to monitor and manage all your devices remotely and easily. This can help you reduce vulnerabilities by implementing digital certificates and other security features. An IoT platform can also help mitigate attacks by limiting the potential damage of SIM theft by binding SIMs to devices.

Recommendations

Don't wait until you discover a breach to reprioritize mobile security. Some simple steps can help reduce your exposure.

Users and behaviors:

- Establish a formal acceptable use policy (AUP) that specifies responsibilities for bring-your-own-device (BYOD) users, what networks can be used and what apps users can install
- Adopt a security-first focus, give all employees regular training and make sure users know how to report anything suspicious
- Set and communicate a password policy covering strength, reuse and two-factor authentication

Apps:

- Restrict access to data on a need-to-know basis
- Limit employees to installing apps from vetted sources and block those downloaded from the internet
- Ensure that all patches are installed promptly

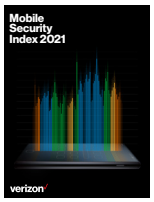
Devices and things:

- Change all default and vendor-supplied passwords—and avoid reusing the same ones
- Implement policies to lock down and isolate vulnerable, infected, and lost or stolen devices
- Use an MDM solution to simplify patch management and enforce your AUP, including authentication policies
- Deploy mobile threat detection software to regularly scan for vulnerabilities

Networks and cloud:

- Encrypt all data sent over unsecured networks
- Educate users on the dangers of public Wi-Fi and block the use of unknown or insecure Wi-Fi networks
- Consider adopting a zero-trust approach
- Restrict the use of unvetted cloud apps, especially file-sharing ones
- Limit access to cloud services to devices that use trusted networks or virtual private networks (VPNs)

Next steps



MSI 2021 main report

This Public Sector Spotlight is an offshoot of the full Mobile Security Index (MSI) report. The extended report provides more detailed statistics and analysis of the threats facing mobile devices.

MSI 2021 security assessment tool

This online assessment tool uses insight from the MSI report to rate your organization's mobile security maturity in four key areas: understanding, perception of risk, exposure and preparedness. Use it to identify where to focus to improve your security posture.

MSI 2021 Acceptable Use Policy Guide

This 10-step guide can help you build a comprehensive AUP that helps your employees understand what is, and isn't, acceptable when using mobile devices. This can help mitigate the risk of threats like malware and phishing.

For more information, visit verizon.com/mobilesecurityindex

About Verizon's Mobile Security Index

Now in its fourth edition, the MSI is a leading source of information on mobile security. This year, we commissioned an independent survey of 856 professionals responsible for buying, managing and securing mobile and IoT devices for their organization. Almost a quarter (23%) of these were from U.S. public sector organizations—federal, state and local. To add further insights, we worked with Asavie, IBM, Check Point, Lookout, MobileIron, NetMotion, Netskope, Qualcomm, Proofpoint, Thales, VMware and Wandera, all leaders in mobile device security. They provided additional information, including incident and usage data. The FBI, the U.S. Secret Service and Europol also made valuable contributions. We'd like to thank all of these organizations for their assistance in helping us present a more complete picture of the threats impacting mobile devices and what is being done to mitigate them.

verizon

1 "Cost of City of Atlanta's Cyber Attack: $2.7 Million—and Rising," The Atlanta Journal-Constitution, April 2018.
2 Wandera, analysis of data from entire global customer base between January 1 and December 31, 2020.
3 Wandera, analysis carried out in January 2020. Data from enterprise user base.
4 Lookout, analysis of all enterprise users covering January 2019 to December 2020.
5 "Ransomware Attack on Nevada School District Highlights Newest Hacker Targets," The National Law Review, October 2, 2020.
6 "Baltimore County Schools Will Reopen Wednesday After Being Closed Due to Cyber Attack," CNN, December 1, 2020.