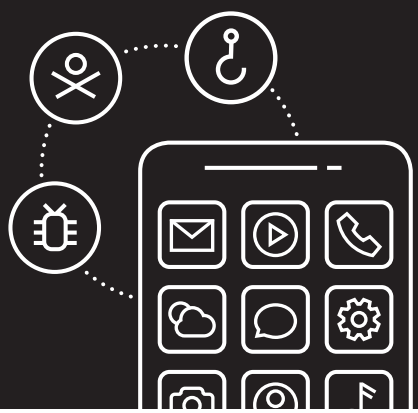
Cyberattacks on mobile devices are on the rise.

Article



5G networks promise increased security, but organizations need to implement their own mobile security measures. Are you ready?

Cyberattacks on mobile devices are increasing. Yet many organizations still aren't taking the problem seriously.

It stands to reason that attacks are becoming more common. Mobile device use is now the norm, not the exception. Employee-liable and corporate-liable devices alike are regularly used to conduct business, even if it's just to read and respond to email. And in the case of employee-liable devices, often without IT approval or governance.

Each year, the *Verizon Mobile Security Index*[1] provides an in-depth look at the scale of mobile threats and incidents, and what organizations are doing to improve mobile security. The 2019 *Index* shows an increase in reported incidents involving a mobile device—from 27 percent in 2017 to 33 percent in 2018. However, organizations rarely share details about how breaches occur, so it's possible that mobile devices were the entry point in considerably more incidents.

Who is doing the hacking? How? And why?

Cybercriminals are adapting nicely to the mobile-first world, evolving their tools and techniques to exploit undefended gaps in mobile security, and weaponizing security technologies like encryption to conceal their actions. Forty-eight percent of the sophisticated cyber actors identified by Lookout Mobile Security in the past year were found to have the tools and techniques for attacking both mobile and desktop devices.

The *Mobile Security Index 2019* categorizes threats into four layers:

- **User behavior:** Phishing/business email compromise, mistakes/errors, abuse, personal use, excess permissions
- **App-based:** Malware, ransomware, insecure coding, unapproved/rogue apps, cryptojacking, side-loaded apps
- **Device-based:** Loss and theft, patching, Internet of Things, out-of-date OS
- **Network-based:** Rogue and insecure Wi-Fi, man-in-the-middle, rogue cellular and base station

That's a lot of opportunities for cybercriminals to gain entry. And for employees to accidentally (or otherwise) open up the organization to attack.

So who are these cybercriminals, and why do they attack organizations?

The people behind cyberattacks and security breaches can also be broken down into four categories:

- Professional criminals
- Hacktivists
- State-sponsored actors
- Employees

As far as motivation goes, personal gain tops the list every time, as evidenced by over a decade of *Verizon Data Breach Investigations Report* (DBIR) results. However, some cybercriminals are acting on a grudge, others on ideology. And still others hack for fun, or are committing espionage for an organization or government.

But the fact is, a large number of data breaches are caused by employees. Some intentionally. Many not. How many of your employees have accidentally clicked on a phishing email, lost their device, or used public Wi-Fi? Probably more than you know.

Mobile device users are much more vulnerable to phishing than desktop users and are less likely to have endpoint protection.

What are the consequences of a breach? And which industries are vulnerable?

While the consequences of a security compromise will be different for every organization, the most common impacts are reputational damage, data loss, financial loss, downtime, penalties and fines, loss of additional equipment, and insurance policy increases.

verizon✓

Eighty-five percent of employees feel that their organization needs to take mobile device security more seriously.

Of course, not every organization will suffer all of those impacts, but of those reporting a compromise in the *Mobile Security Index 2019*, 62 percent described it as "major." And 41 percent described the compromise as "major, with lasting consequences."

Just how major are we talking? In 2018, the average cost of a data breach in the United States was $3.86 million, with a per capita cost of $148 per record.[2]

Though the cost can be higher or lower, depending on the industry, of those most at risk—healthcare, hospitality, public sector, retail and finance (per DBIR)—resolution costs for healthcare are the highest, costing an average of $408 per record. That's followed by financial services, with an average cost of $206 per record.

That's pretty major. Particularly when the number of records compromised reaches into the thousands. Or millions. Or even billions.

What's being done about mobile security?

So what are organizations doing about the increase in mobile threats?

As it turns out, not nearly enough.

Many are failing to meet even a basic level of preparedness. In fact, only 12 percent of *Mobile Security Index 2019* respondents had the following baseline protections in place:

- Encryption
- "Need-to-know" access
- Two-factor authentication
- No default passwords

Not surprisingly, 85 percent of employees feel that their organization needs to take mobile device security more seriously.

What your organization should do right now

For many organizations, money isn't the barrier to better mobile security: It's a combination of not understanding mobile threats and not knowing how to mitigate them. And even those with a good handle on internal IT security may find creating, implementing and managing a mobile program daunting.

Still, it's time to overcome whatever it is that's holding you back. Because, according to Ponemon Institute's 2018 Cost of a Data Breach Study,[2] the odds of experiencing at least one incident in the next two years are more than one in four. Those are great odds if you're buying a raffle ticket. Not so much if you're facing a potentially devastating data breach.

If you're unsure where to begin, see the "10 basic steps to better mobile device security" sidebar.

Additionally, the *Mobile Security Index 2019* includes a handful of self-assessment tools, as well as a "Baseline, Better, Best" matrix that includes steps you can take to improve your mobile security stance, whatever your current level of preparedness.

Another critical step in the journey to better mobile security is partnering with the right network. Because when it comes to security, the network matters.

4G, 5G and what they mean to mobile security

Security has improved with each successive wireless network evolution. For example, with 2G it was possible to intercept mobile phone calls as they passed over the radio waves. From 3G onward data has been encrypted, making interception much more difficult.

In fact, 4G LTE encrypts both data and signaling, to prevent it from being overheard on the radio access interface. 4G LTE also provides secure storage, mutual authentication, integrity protection and stronger encryption.

And the next-generation network, 5G, will deliver even more robust security for mobile devices,[3] thanks to:

- **Communication security**
  5G will encrypt signaling traffic and inherits well-proven security algorithms, such as separation of keys, backward and forward security for keys at handovers, idle mode mobility and secure algorithm negotiation. New features will include automatic recovery from malicious algorithm mismatches and fast synchronization of security contexts in access and core networks
- **Identity management**
  With secure identity management and a new authentication framework, 5G will allow more flexible and robust authentication. It will also facilitate reuse of existing public keys and certificate infrastructure for network access authentication
- **Privacy**
  Subscriber privacy for data traffic, phone calls and text messages will be included in 5G, by using state-of-the-art encryption. The devices and the network will mutually authenticate each other and use integrity-protected signaling
- **Security assurance**
  This will help ensure that network equipment meets security requirements and is implemented following secure development and product life-cycle processes

5G is also expected to be more resilient to cyberattacks and non-malicious incidents, thanks to a core network architecture designed to support network slicing, continuous secure connectivity for mobile devices and lower latency.

The best way to capture the full security potential of 5G is to start incorporating the best 4G LTE connections and technologies into your business. The Verizon 5G Ultra Wideband network will be paired with the nation's best 4G network, Verizon 4G LTE Advanced, and the networks will interoperate seamlessly, providing secure, reliable connectivity for years to come.

You'll find an always-current list of cities with Verizon 5G Ultra Wideband at verizonwireless.com/5g/coverage-map/

For information on 5G Home availability, visit verizonwireless.com/5g/home/

Threats are escalating: Is your organization ready?

It's time for organizations of all sizes and across all industries to start taking mobile security seriously.

While security will continue to improve with each generation of the network, millions more devices are projected to connect to the 5G network, providing hackers with more targets than ever.

That's why it's crucial to implement the strongest possible security measures for your organization's mobile devices. Because with the right security in place, you'll be more resilient to both cyberattacks and inadvertent exposures. And you'll be ready to harness the power of 5G, with its game-changing speed, performance and security.

10 basic steps to better mobile device security

1. **Gain an understanding of the risk factors for your organization, location and industry**
2. **Ensure that mobile is included in all of your security plans and policies**
3. **Take a full accounting of mobile assets and users**
4. **Understand and manage employee data usage**
5. **Establish formal policies for corporate-liable and employee-liable device**
6. **Deploy a device management program and consider a private network solution**
7. **Implement a strong password policy and ensure adherence**
8. **Limit the use of Wi-Fi to approved networks**
9. **Prevent employees from downloading apps from the internet**
10. **Regularly review access to data and systems**

Let's talk cybersecurity

We help protect organizations of all sizes and types against security threats. We will work with you to identify vulnerabilities and then design a cybersecurity strategy that addresses them. No wireless carrier does security better than Verizon.

To learn more, contact your Verizon Wireless business specialist.

Take the Verizon 5G Readiness Assessment survey: https://info.verizonwireless.com/b2b-5g-assessment-tool.html#/

Read the *Mobile Security Index 2019* report here: solutionslab.vzw.com/presentation/mobile-security-index-2019-report-customer-presentation

Learn more about your 5G opportunity at verizon.com/about/our-company/5G

verizon

1 The Mobile Security Index is conducted by an independent research firm on behalf of Verizon. Unless otherwise noted, all stats are from Verizon's Mobile Security Index 2019.

2 2018 Cost of a Data Breach Study, Ponemon Institute.

3 https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system