



You're ready for anything

Is your mobile security?

The Verizon 2025 Mobile Security Index delivers mobile threat intelligence that can help you build a strong defense for your organization — and the people you serve.



Here's what you need to know.

What happens if critical services go dark?

In mobile security, the stakes are high for businesses—but for Public Sector organizations, they're even higher. Because public services are vital, a single breach can disrupt essential operations, erode trust and even put lives in danger.

79%

of Public Sector respondents say a security breach could put people's lives at risk.

50%

of all respondents had a mobile or Internet of Things (IoT) security incident resulting in data loss.

46%

of all respondents had a mobile or IoT security incident resulting in downtime.

63%

of all respondents that suffered downtime from a cyberincident had major repercussions, up from 47% in the previous year.

Artificial intelligence (AI) is rewriting the playbook for attackers.

77%

of respondents believe AI-assisted attacks involving deepfakes and short message service (SMS) text phishing are likely to succeed.

93%

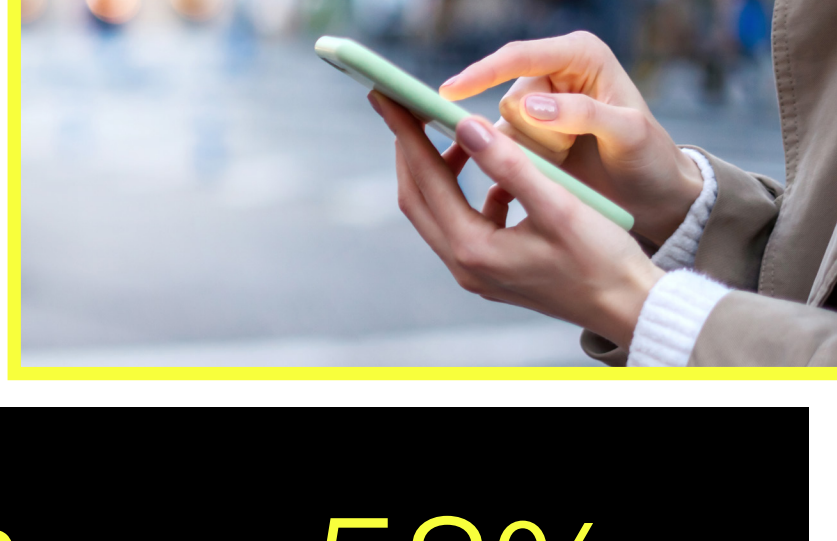
of respondents report that their employees are using generative AI (genAI) tools on mobile devices.



Human error is still part of the story.

64%

of respondents see data compromise from employees entering sensitive information into genAI as their top mobile device risk.



Proactive governance can change the outcome.

58%

of Public Sector respondents have defined and enforced genAI usage policies vs. 50% for other industries.

84%

of Public Sector respondents say the public's expectations for self-service require additional mobile cybersecurity defenses.

The attacks of choice:

phishing

and smishing

Almost everyone's a target.

One click can open the door.

Defenses are lagging.

80%

of all respondents reported experiencing mobile phishing attempts targeting their employees.

39%

of all respondents running smishing simulations reported that between a quarter and half of their employees clicked a malicious link when tested.

42%

of Public Sector respondents have adopted mobile threat defense vs. 48% for other industries.

Secure mobile access controls = enhanced mobile security

Self-service technology should meet the public's expectations for availability and safety. Strong mobile access controls protect sensitive information, helping the community feel confident in every digital interaction.

53%

of respondents report using passwordless or passkey access; 52% say they use advanced multifactor authentication.

62%

of respondents report using AI-powered software to automatically revoke mobile access privileges based on risk signals.

62%

of respondents have adopted biometric authentication to strengthen mobile identity security.

60%

of respondents use role-based access control to manage access to mobile devices.

Protect what matters from core to edge.



The 2025 Mobile Security Index shines a light on the evolving mobile threat landscape. The report can help you turn those insights into a defense plan tailored to your organization—helping you safeguard your data, operations and community.

Talk to your Verizon Representative to get started.



Read the report at [verizon.com/mobilesecurityindex](https://www.verizon.com/mobilesecurityindex).