T-Mobile Opens Up on Its Cybersecurity Transformation in New Report

November 2, 2026

Over 99% fewer phishing-related credential compromises among employees, over 99% fewer successful SIM swap attacks on customers, and the story of how T-Mobile got here

BELLEVUE, Wash.--(BUSINESS WIRE)--Nov. 2, 2026-- T-Mobile US, Inc. (NASDAQ: TMUS):

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20261102608714/en/

T-Mobile published Advancing Cybersecurity at T-Mobile, a report on how the company rebuilt its security program and what that work has delivered. T-Mobile is showing its work, including what's changed, what's held up when tested and what's next — because trust has to be earned and verifiable.

- What's the news: T-Mobile published Advancing Cybersecurity at T-Mobile, a report on how the company rebuilt its security program and what that work has delivered.
- Who it's for: Customers and businesses that rely on T-Mobile's network, and the industry and government partners working to secure America's communications infrastructure.
- Why it matters: Telecom networks are high-value targets for nation-state actors and criminals. T-Mobile is showing its work, including what's changed, what's held up when tested and what's next — because trust has to be earned and verifiable.

T-Mobile (NASDAQ: TMUS) today published *Advancing Cybersecurity at T-Mobile*, an inside look at how one of America's largest wireless providers rebuilt its security program, what held up when that program was tested and where the work goes next.

It's a story about speed, scale and a willingness to be uncomfortable. Facing relentless pressure from nation-state actors and financially motivated criminals, T-Mobile asked its employees, contractors and partners to change how they work, from how they prove who they are to how they connect to systems. Two things were non-negotiable: customers' wireless service had to keep working, and stores had to keep opening. Almost everything else was on the table.

"At T-Mobile, protecting customers is fundamental to who we are. Our industry connects families, businesses, first responders and communities every day, so the security of our networks is a responsibility that extends beyond any single company," said Jeff Simon, EVP & Chief Information Officer, T-Mobile. "With stakes that high, we couldn't work at the normal pace. The attackers never stop moving, so our teams skipped the pilots and the multi-year rollouts and moved at a speed most companies wouldn't try. Today, phishing-related credential compromises among our people are down more than 99%. This report shows what it meant to move that fast, and what we learned along the way."

Inside the report

Over a recent 12-month period, T-Mobile observed a 37% increase in attempted intrusions, even as credential-based attempts decreased 35%, highlighting how quickly adversaries are adjusting their tactics. Customers feel the pressure too: T-Mobile continues to identify hundreds of millions of scam and spam calls every week, and in 2025 saw nearly 50% more scam and spam messages than in 2024. That's why T-Mobile is sharing the progress and investments behind its cybersecurity program, including:

- **Cutting phishing-related credential compromises among employees by more than 99%.** Each team member verifies who they are with a selfie and a government-issued ID before any credential is issued. T-Mobile also eliminated passwords, one of attackers' most common ways in, replacing them with phishing-resistant FIDO2 hardware security keys that never transmit a password for criminals to intercept. Nearly 100% of T-Mobile's workforce is now passwordless.
- **Reducing successful SIM swap attacks by more than 99% since 2022.** Layered authentication measures including biometric ID verification, SIM Protection and Port-Out Protection help protect customer accounts against these attacks.
- **Defending against a nation-state attack.** In late 2024, Salt Typhoon, a state-sponsored threat actor, targeted U.S. telecommunications providers. The attackers came through a third-party wireline provider and impersonated a trusted router at the edge of T-Mobile's network, a technique the company had not seen before. T-Mobile's layered defenses contained the attackers before they could access sensitive customer data, including calls, voicemails or texts, and the team shared what it learned with federal partners and industry peers.
- **Deploying zero trust in six months.** Hybrid zero trust assumes no user, device or application is trusted by default, so an attacker who gets in can do far less. T-Mobile rolled out zero trust across its workforce in just six months — a process that typically takes years — and its platform has blocked more than 6 million online threats since launch.
- **Building security in, not bolting it on.** T-Mobile was first in the world to deploy a nationwide 5G standalone network, with security designed in from the ground up. 5G Advanced takes that foundation further, with more capabilities to help protect customers' sensitive data and shrink attack surface.
- **Protecting customers automatically, at scale.** Today, 100% of T-Mobile customers get core network-level protection that

works across calls, texts and web browsing to help block scams and spam in real time. Since March 2017, Scam ID and Scam Block have helped protect customers from more than 160 billion unwanted calls, and in 2025 alone T-Mobile blocked nearly 3 billion scam and spam texts before they reached customers.

- **Defending 24/7, with people at the core.** T-Mobile's workforce completed more than 200,000 cybersecurity trainings in 2025. The new Cyber Defense Center brings monitoring, threat hunting, digital forensics and incident response under one roof, and AI-driven threat detection deployed at scale helps teams detect, disrupt and respond to threats in real time.
- **Helping businesses of every size strengthen their security.** T-Mobile offers business and enterprise customers ways to identify cyber risk, secure access and protect distributed workforces, including Risk-Based Vulnerability Management, Patch Management, SASE with zero trust access, secure SIM authentication and mobile threat defense solutions.

Advancing Cybersecurity at T-Mobile also highlights T-Mobile's Bug Bounty program , which has drawn more than 1,400 valid submissions from the global security community. And no one company can tackle these threats alone, so T-Mobile partners with CISA, is a founding member of the C2 ISAC and the CTIA 5G Security Test Bed and shares what it learns to raise the bar across the industry.

"What stands out in this report is the specificity," said Jason Leigh, Senior Research Manager, IDC. "Many companies merely provide a litany of cybersecurity abbreviations or footnote security in financial filings with minimal detail on specific cybersecurity actions. T-Mobile is elevating the conversation with a level of detail that signals a security program built for operational maturity."

What comes next

Advancing Cybersecurity at T-Mobile is a marker of T-Mobile's cybersecurity work, not a final word on it. The report looks ahead to AI-enabled fraud, non-human identities such as AI agents and bots and quantum computing. T-Mobile is already preparing, from adversarial testing of AI systems to a honeypot program that studies attacker techniques.

In a note to T-Mobile employees today, Mark Clancy, SVP, Information Security Officer, thanked team members across the company for embracing the changes and making security a shared mindset. "Ultimately, cybersecurity is about protecting people," said Clancy. "We pushed to modernize our systems and strengthen how we detect and respond to threats. With tighter collaboration across our teams and partners, our defenses became stronger and our response faster than ever before. There's no finish line in cybersecurity. The threat landscape will keep evolving, and so will we."

T-Mobile's guiding principle is that security must be seamless, equitable and grounded in the needs of the people and businesses the company serves — and it's fundamental to how T-Mobile builds, operates and continually strengthens America's Best Network.

Read the full report, *Advancing Cybersecurity at T-Mobile* on T-Mobile's Newsroom. To learn more about online safety, cybersecurity and tools for customers, head to T-Mobile's Trust Center and Privacy Center.

Follow the T-Mobile Newsroom on X and Instagram to catch the latest company updates.

Cybersecurity metrics are based on T-Mobile internal data as described in the report. Cyber threats continue to evolve, and no security measures can prevent all threats or incidents.

About T-Mobile

As the supercharged Un-carrier, T-Mobile US, Inc. (NASDAQ: TMUS) is powered by an award-winning nationwide 5G Advanced network that connects more people, in more places, than ever before. With T-Mobile's unique value proposition of best network, best value and best experiences, the Un-carrier is redefining connectivity and fueling competition while continuing to drive the next wave of innovation in wireless, broadband and beyond. Headquartered in Bellevue, Wash., T-Mobile provides services through its subsidiaries and operates its flagship brands, T-Mobile, Metro by T-Mobile and Mint Mobile. For more information, visit https://www.t-mobile.com.

View source version on businesswire.com: https://www.businesswire.com/news/home/20261102608714/en/

Media Contact
T-Mobile US, Inc.
MediaRelations@t-mobile.com

Investor Relations Contact
T-Mobile US, Inc.
Investor.Relations@t-mobile.com
https://investor.t-mobile.com

Source: T-Mobile US, Inc.