November 2026

Advancing Cybersecurity at T-Mobile

Our journey to build stronger defenses, better protect customers, and strengthen the nation's communications ecosystem



Contents

Our commitment to security: A letter from Jeff Simon, EVP & CIO 3

Today's threat landscape 4

Embedding security throughout our network 5

Defending against Salt Typhoon 5

Building a resilient cybersecurity foundation 6

- Investing in our teams 6
- T-Mobile's Cyber Defense Center 6
- Strengthening identity verification 7
- Eliminating passwords 7
- Deploying zero trust 7
- Bug Bounty program 7
- Frameworks and certifications 8
- Industry collaboration 9
- Supply chain security 9

Defending customers at scale 10

- Protecting voice: Stopping scam and spam calls 10
- Protecting messaging: Blocking malicious texts 11
- Protecting internet traffic: Safer web browsing 12
- Protecting access: Securing customer accounts 12
- Combating SIM box fraud 12

Defending businesses of every size 13

- Identifying and reducing cyber risk 13
- Securing access, devices, and accounts 13

Anticipating tomorrow's threats 14

A message from Mark Clancy, SVP, Information Security Officer 14

Our commitment to security

A letter from Jeff Simon, EVP & CIO



Jeff Simon
T-Mobile EVP & CIO

At T-Mobile, protecting our customers is fundamental to who we are.

As a proud American company and one of the nation's largest wireless providers, we recognize that safeguarding customer information is a core responsibility to the people and communities we serve. We know that trust must be earned and maintained, and that means continuously strengthening our defenses to keep pace with an increasingly complex threat environment.

The stakes are high. We're more than a telecommunications company—our network is part of the communications fabric Americans rely on every day to connect with family and friends, run businesses, and call for help in emergencies. When adversaries target telecommunications infrastructure, the consequences can extend far beyond any single company.

Nation-state actors are targeting telecommunications infrastructure with increasing frequency and sophistication. Cybercriminals are using artificial intelligence (AI) to generate phishing campaigns and deepfake voice scams on an industrial scale. The volume of attempted intrusions, account takeovers, and scam traffic flowing across communications networks continues to grow each year, reinforcing the need for constant vigilance, sustained investment, and a security strategy designed to adapt.

Our past experiences have taught us important lessons and driven meaningful change. We have made significant investments to strengthen our cybersecurity posture, modernize our defenses, and embed security more deeply across our network and operations. That work has included growing our cybersecurity team, adopting hybrid zero trust architecture, deploying AI-driven threat detection at scale, and building a new Cyber Defense Center to help us better detect, disrupt, and respond to cyber threats in real time.

Those investments were tested in late 2024 when Salt Typhoon, a foreign state-sponsored threat actor, targeted the telecommunications industry. At other providers, these attacks succeeded. At T-Mobile, our defenses detected and stopped the attackers before their intrusion could reach sensitive customer data.

This report highlights how we're working to protect customer information while helping strengthen America's critical communications infrastructure. It reflects the progress we've made—where we started, what we learned, and how we've evolved to enhance our security foundation, protect consumers and businesses from emerging threats, and prepare for the risks ahead.

While no organization can guarantee it will stop every threat, we remain committed to investing in tools, expertise, and partnerships that help protect our customers, strengthen resilience across the broader ecosystem, and earn the trust people place in us every day.



Today’s threat landscape

The threat environment we face is constantly evolving, as telecommunications companies and infrastructure remain high-value targets for nation-state actors and sophisticated cybercriminals. Over a recent 12-month period, we observed a 37% increase in attempted intrusions alongside a 35% decrease in credential-based attempts—evidence that adversaries are continually adjusting their tactics and pursuing new avenues of attack.

Supply chains and third-party ecosystems present additional risk, as wireless providers rely on broad networks of vendors, software providers, and managed service partners. Each must defend against many of the same threat actors and methods.

Consumers and businesses face a similarly dynamic environment, including scam calls, phishing, smishing, and SIM swap attempts. In 2025, we saw nearly 50% more scam and spam messages than the previous year, and we’re continuing to identify hundreds of millions of scam and spam calls every week.

Emerging risks such as AI-enabled fraud and non-human identity compromise, as well as the longer-term challenge posed by quantum computing, are also shaping our security priorities and investments across our network, internal systems, and protections for consumers and businesses.

37% increase
in attempted intrusions year-over-year

35% decrease
in credential-based attempts year-over-year

50% more
scam and spam messages in 2025 compared to 2024

Hundreds of millions
of scam and spam calls identified every week



> **Simply put, our defenses worked as designed—from our layered network design to robust monitoring and partnerships with third-party cybersecurity experts and a prompt response—to prevent the attackers from advancing and, importantly, stop them from accessing sensitive customer information.**
>
> **—Jeff Simon,**
> Then-SVP & Chief Security Officer, November 2024

Embedding security throughout our network

Our approach starts with making cybersecurity a core design principle of our network architecture—never an add-on after the fact.

T-Mobile was the first in the world to deploy a nationwide 5G standalone network, designed with security integrated from the ground up. 5G standalone strengthens authentication between devices and network components, encrypts subscriber identities and traffic, and separates that traffic from core operations. Its software-defined core enables programmable policy enforcement, allowing security controls to adapt more quickly at scale to emerging threats. Additional capabilities such as network slicing provide logical isolation of traffic flows so that different services and applications can operate in secure, segmented environments.

Our nationwide 5G Advanced network builds on that secure foundation with even more capabilities, helping protect customers' sensitive data, our network, and the services we provide as part of America's critical infrastructure. Our architecture has helped make our network more resilient by reducing overall attack surface and limiting exposure to critical systems.

Defending against Salt Typhoon

In late 2024 and early 2025, multiple U.S. telecommunications providers were targeted by Salt Typhoon, one of the most sophisticated threat actors in the world—state-sponsored, highly resourced, and patient.

Salt Typhoon did not come at us directly. They came through a third-party wireline provider and impersonated a trusted router at the edge of our network—a technique we had not seen before. But our architecture did exactly what it was built to do: it kept them contained to the network appliance layer. This was a direct test of the security architecture we had been building for years—and it worked as intended. Our layered defenses contained them before they reached any sensitive customer data, including calls, voicemails, and texts. Our customers were protected.

We did not stop there. Similar trusted-provider connections exist across telecom, banking, energy, and other critical infrastructure, so we made sure to share what we learned with federal partners, our peers, and industry information-sharing organizations—the technique, how it worked, and what others should look for.

The threat landscape does not stand still, and neither do we. We remain committed to reducing systemic risk, limiting opportunities for attackers, protecting the nation's communications infrastructure, and supporting reliable, trusted connectivity for consumers and businesses.

Building a resilient cybersecurity foundation

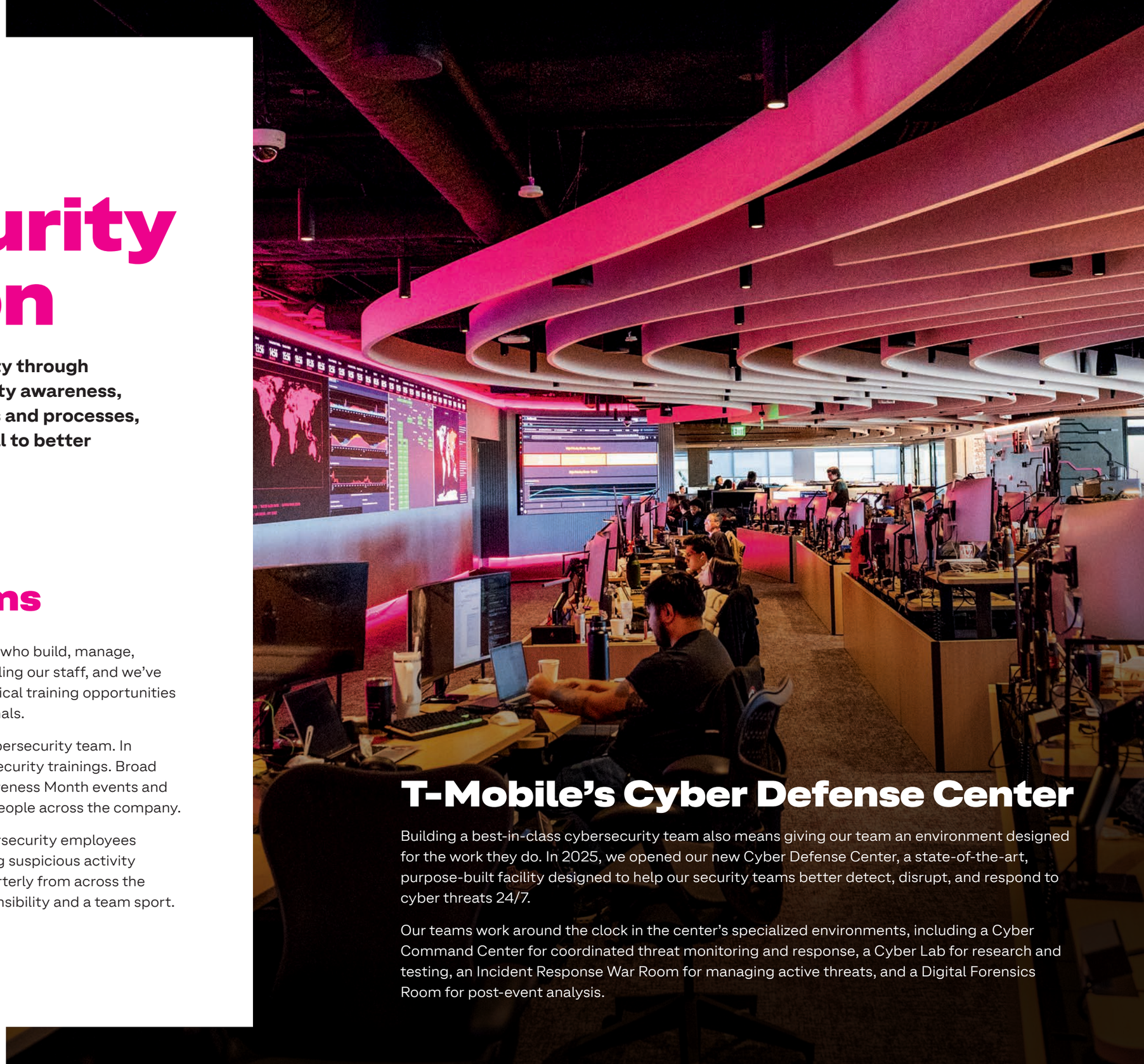
We have evolved our approach to cybersecurity through sustained investment in company-wide security awareness, modern security technology, resilient systems and processes, strong partnerships, and operational rigor—all to better protect customers and their data.

Investing in our teams

Security depends not only on technology, but on the people who build, manage, and strengthen it. We've invested heavily in hiring and upskilling our staff, and we've expanded advanced testing, labs, and other hands-on technical training opportunities to deepen the practical skills of our cybersecurity professionals.

Our security culture and investments extend beyond the cybersecurity team. In 2025, our workforce completed more than 200,000 cybersecurity trainings. Broad awareness initiatives, including National Cybersecurity Awareness Month events and nationwide roadshows, continue to educate and empower people across the company.

T-Mobile's T-Defender award program recognizes non-cybersecurity employees who demonstrate strong security behaviors, from identifying suspicious activity to supporting security projects. Recipients are selected quarterly from across the company, reinforcing that cybersecurity is everyone's responsibility and a team sport.



T-Mobile's Cyber Defense Center

Building a best-in-class cybersecurity team also means giving our team an environment designed for the work they do. In 2025, we opened our new Cyber Defense Center, a state-of-the-art, purpose-built facility designed to help our security teams better detect, disrupt, and respond to cyber threats 24/7.

Our teams work around the clock in the center's specialized environments, including a Cyber Command Center for coordinated threat monitoring and response, a Cyber Lab for research and testing, an Incident Response War Room for managing active threats, and a Digital Forensics Room for post-event analysis.

Strengthening identity verification

Authentication starts with verifying that the person at the keyboard is who they claim to be—before they enter a password. That's why we partnered with CLEAR to deploy biometric identity verification across our workforce. Each team member completes a one-time enrollment using a selfie and a government-issued ID, establishing a verified link between their digital identity and their physical identity before any authentication credential is issued or presented. This meaningfully raises the bar against insider threats, account takeovers, and social engineering attacks targeting help desks or account recovery processes.

Eliminating passwords

We then moved to eliminate passwords, which remain one of the most common entry points for attackers. We deployed phishing-resistant FIDO2-enabled YubiKeys across our workforce, including employees, contractors, and partners. This enabled us to transition to passwordless authentication and dramatically reduce the risk of credential theft and the use of stolen passwords to gain unauthorized access to company systems.

FIDO2 authentication replaces passwords with a unique digital credential stored securely on a user's device or security key. When a user signs in, the device verifies the request without transmitting a password, making it far more difficult for attackers to intercept credentials through phishing and use them to access company systems.

Since completing our CLEAR and YubiKey rollouts, phishing-related credential compromise incidents affecting T-Mobile employees have decreased by 99%.

Deploying zero trust

Traditional network security assumed that anyone inside the perimeter could be trusted. Zero trust assumes the opposite: no user, device, or application is inherently trusted, regardless of where it sits on the network. Every access request must be authenticated, authorized, and continuously validated. By restricting permissions at every step, zero trust limits what an attacker can do if they gain entry and helps contain the impact of an intrusion.

To put this approach into practice, we implemented the Zscaler Zero Trust Exchange Platform across our managed endpoints. The platform inspects more than 160 million transactions each quarter and has blocked more than 6 million online threats since launch.

Bug Bounty program

Because no organization can tackle the full range of security threats alone, we work with the global security community to strengthen defenses. Our Bug Bounty program, managed with Bugcrowd, remains one of the telecommunications industry's most impactful programs. Through it, we engage a broad community of security experts to help us find and fix vulnerabilities across our platforms and systems, as well as promote transparency and shared responsibility across the industry.

We use the program to encourage our vendors, telecommunications peers, and industry partners to improve their own security practices, recognizing that protecting Americans and their communications requires raising security standards everywhere, not just at T-Mobile.

To date, our Bug Bounty program has received over 1,400 valid submissions. We have resolved all but the most recent, which we're currently addressing. As the program has matured, submissions have become increasingly sophisticated, reflecting stronger defenses and a higher barrier for potential attackers.





Frameworks and certifications

Trust needs to be verifiable, not simply stated. We align our security program with recognized frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and validate our work through independent certifications and assurance reports. We have achieved ISO/IEC 27001:2022 and ISO/IEC 42001:2023 certifications and obtained System and Organization Controls (SOC) 2 Type 2 and SOC 3 reports for defined scopes and boundaries. We also maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 and are pursuing Cybersecurity Maturity Model Certification (CMMC) Level 2.

T-Mobile Cybersecurity

Recent milestones and certifications

- **March '24** — ISO/IEC 27001 Certification
- **April '24** — SOC 2 Type 2 Report
- **June '24** — T-Mobile Trust Center Launch
- **October '25** — Cyber Defense Center Launch
- **November '25** — SOC 3 Report
- **June '26** — ISO/IEC 42001 Certification

Our report card

A	790	A
SecurityScorecard	BitSight	ImmuniWeb

Industry collaboration

Through our partnerships with the Cybersecurity and Infrastructure Security Agency (CISA) and other organizations, we're working to advance security research, increase information sharing, and drive collective action against threats affecting the broader telecommunications ecosystem.

We're a founding member of the Communications Cybersecurity Information Sharing and Analysis Center, known as the C2 ISAC. This nonprofit is dedicated to strengthening cybersecurity across the communications sector, providing a trusted setting where members can share resources and expertise to help one another anticipate, identify, and respond to cyber threats more quickly and effectively.

We're also a founding member of the CTIA 5G Security Test Bed, an initiative that brings together major carriers, network vendors, and research institutions to test and validate 5G security standards using commercial-grade network equipment. Unlike testing conducted solely in controlled lab environments, the Test Bed evaluates standards against the complexity of real-world networks, producing findings that can inform national policy and industry standards.

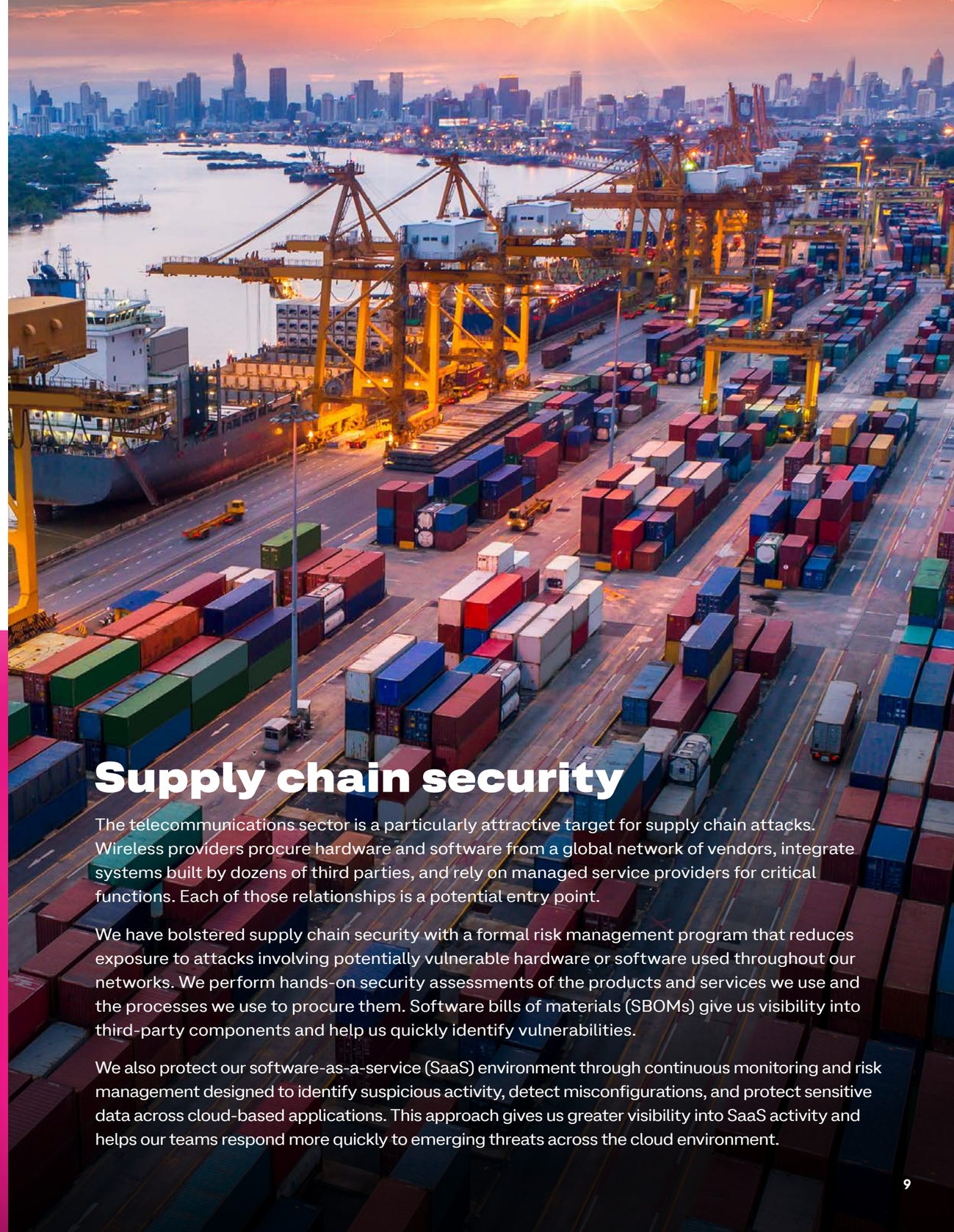
Together, these efforts reflect our commitment to helping advance research and knowledge sharing across the communications ecosystem, while strengthening security through independent certification, continuous testing, shared investment, data, and collective action.

200K
cybersecurity trainings in 2025

99% reduction
in phishing-related credential compromise incidents

1,400+
valid Bug Bounty submissions

6+ million
online threats blocked through Zscaler



Supply chain security

The telecommunications sector is a particularly attractive target for supply chain attacks. Wireless providers procure hardware and software from a global network of vendors, integrate systems built by dozens of third parties, and rely on managed service providers for critical functions. Each of those relationships is a potential entry point.

We have bolstered supply chain security with a formal risk management program that reduces exposure to attacks involving potentially vulnerable hardware or software used throughout our networks. We perform hands-on security assessments of the products and services we use and the processes we use to procure them. Software bills of materials (SBOMs) give us visibility into third-party components and help us quickly identify vulnerabilities.

We also protect our software-as-a-service (SaaS) environment through continuous monitoring and risk management designed to identify suspicious activity, detect misconfigurations, and protect sensitive data across cloud-based applications. This approach gives us greater visibility into SaaS activity and helps our teams respond more quickly to emerging threats across the cloud environment.

Defending customers

at scale

For most Americans, the daily threat landscape looks like a scam call pretending to be the IRS, a text message with a malicious link, a fraudulent website designed to steal login credentials, or an attempt to hijack a phone number to drain a bank account. These attacks are relentless, cost Americans billions of dollars every year, and disproportionately affect vulnerable populations, including seniors, small business owners, and those with limited digital literacy.

We take our responsibility to help protect customers from these threats seriously. Our strategy is built around a straightforward idea: security should work automatically for everyone, without requiring customers to be cybersecurity experts. Today, 100% of our customers receive core network-level protection. We scale safeguards across voice, messaging, and internet traffic channels to help block scams, spam, and other unwanted communications in real time—when protection matters most.



Protecting voice:

Stopping scam and spam calls

Phone scams cost Americans billions of dollars every year, and the volume of fraudulent calls continues to grow as bad actors deploy increasingly sophisticated, AI-generated campaigns to target consumers and businesses.

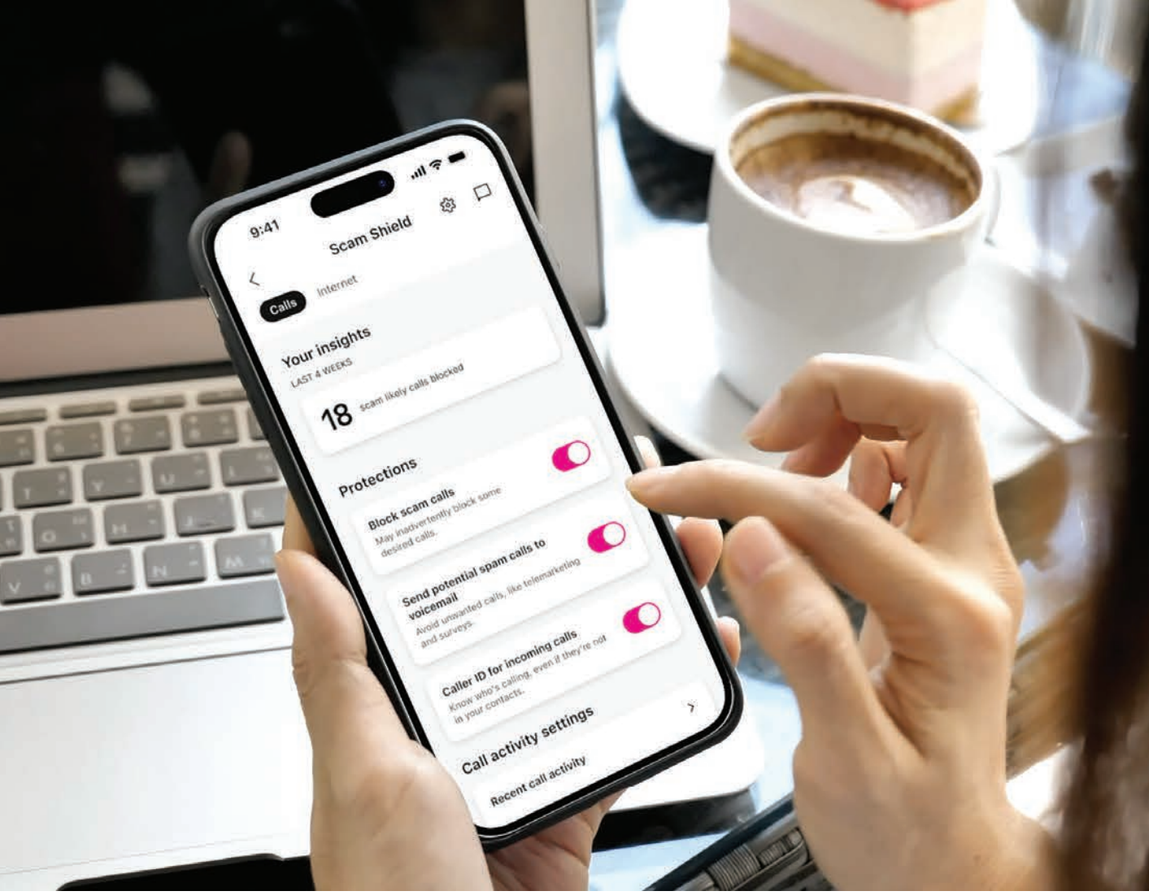
We use continuously improving AI and machine learning (ML) models to identify and stop scam calls by analyzing activity and calling patterns in real time. Because we build these protections directly into our network rather than relying solely on an app, they work automatically to help prevent fraudulent calls from reaching customers.

Scam Shield is our suite of tools for identifying, blocking, and managing unwanted calls. It includes key features such as Scam ID and Scam Block. For all customers, Scam ID automatically labels possible scams and illegal robocalls as “Scam Likely” on their device. Scam Block goes a step further, letting customers block those calls before they come through. Nearly 99% of customers who turn on Scam Block never turn it off. We also tag spam calls—such as calls from telemarketers or robocalls—as “Potential Spam” by default.

Since launching Scam ID and Scam Block in March 2017, we’ve protected customers from more than 160 billion unwanted calls. Today, we identify or block an average of over 800 scam calls every second.

In 2025 alone, we tagged nearly 29 billion inbound calls as likely scams and spam. That includes more than 428 million “Potential Spam” calls detected and tagged by our new AI and ML systems—a tenfold increase compared to 2024. We continue to tune and improve our new models, and once fully optimized, these systems are expected to identify over 25 million unwanted spam calls each day.

Customers can manage most Scam Shield features through T-Mobile’s T-Life app, including blocking potential spam calls, sending them directly to voicemail, creating personal block lists, and using Caller ID and call reporting tools. Scam Shield Premium also offers voicemail transcription, number lookup, and controls for categories such as political calls, charity calls, and surveys. Customers can also enable Scam Block by dialing #662#.



Customer reports strengthen protection

Customers can help strengthen T-Mobile's protections by reporting suspicious and unwanted calls through Scam Shield in the T-Life app. They can also report suspicious SMS and MMS messages by forwarding them to 7726 or using the native iOS or Android messaging apps.

Each report gives us valuable signals that help identify emerging scam patterns and improve detection in real time. By combining customer reports with AI and ML, we can adapt our defenses more quickly and expand protections for individual customers and the broader T-Mobile community.

ScamShield®

New scam methods are emerging and evolving every day, and we constantly adapt our protections to address them. Fraudsters increasingly trick customers—typically those in the most vulnerable groups—into placing calls themselves through deceptive online listings, fake customer service numbers in phishing emails, or messages designed to look like urgent financial alerts.

To counter this scheme, we introduced Scam Callback Protection, an award-winning, industry-first feature that checks outbound calls against a database of known scam numbers and alerts customers with an audible warning before the call connects. Customers on our network hear, "The number you are calling has been identified as likely a scam. It is recommended you hang up now." Since we deployed the feature, it has played more than 67 million warnings, and most alerted customers have chosen to hang up before the call connects, preventing exposure to scams and preventing the customer's phone number from being marked for future targeting.

Protecting messaging:
Blocking malicious texts

Smishing, or SMS phishing, is another common attack targeting both consumers and businesses. These scams often appear as package delivery updates, bank fraud alerts, tax notices, romance messages, or job offers that use urgency to push targets toward malicious links, replies, or fraudulent support numbers. In 2025, our network-level protections blocked nearly 3 billion spam and scam SMS and MMS messages before they reached customers, helping safeguard them from identity theft, financial fraud, and other threats.

We also require non-consumer message senders—including businesses, charities, government agencies, and other organizations—to be registered, vetted, and verified to help ensure that our customers receive the text messages they actually want to receive.

Protecting internet traffic:
Safer web browsing

Phishing websites are designed to be difficult to distinguish from legitimate ones. They mimic the look of banks, government agencies, and major retailers, tricking users into entering credentials or personal information. In 2025, we launched Safe Web Browsing, a free feature built into the core of our network that helps prevent customers from connecting to dangerous or fraudulent websites that could steal passwords, financial information, or personal data.

We automatically check internet traffic on our network at the Domain Name System (DNS) layer—which directs devices to websites—against lists of known phishing sites, malware distributors, and other malicious sources. If a domain is identified as dangerous, we automatically block the connection before it reaches the customer, making it harder for scammers to steal sensitive information. This protection is especially important because many scam campaigns reach customers through channels outside traditional calls and text messages, including email, encrypted messaging apps, search results, and social media.

Since launching Safe Web Browsing in 2025, we've blocked more than 100 billion malicious domain requests.

Protecting access:
Securing customer accounts

Many of our protections focus on blocking inbound scams before they reach customers' devices, but protecting customer accounts is just as critical. A phone number is no longer just a way to make calls; it can be connected to banking apps, two-factor authentication, personal email, and government services. That makes account access a valuable target for criminals and underscores the need for strong identity verification and safeguards against unauthorized changes.

Through the T-Life app, customers can turn on complementary security features, including Port Out Protection, SIM Protection, and biometric ID verification. Together, these help prevent fraudulent activity such as SIM swap attacks. We also launched a security pop-up in T-Life that warns customers about potential fraud before they complete sensitive actions such as requesting a SIM change. For example, customers will see: "T-Mobile will never contact you to initiate a SIM transfer unless you first initiate it. If you received an unsolicited request, do not respond."

SIM swap transactions are a routine and necessary part of wireless service. While historically only a tiny fraction of those transactions occurred without customer authorization, even during periods of elevated threat activity, our layered authentication measures have reduced successful SIM swap attacks by 99% since 2022. The remaining incidents typically involve highly targeted attacks that exploit uncommon scenarios or social engineering tactics, which our teams continue to monitor and address.

160+ billion
unwanted calls identified or blocked since 2017

800
scam calls identified or blocked every second on average

10X more
potential spam calls tagged in 2025 compared to 2024

99%
of Scam Block users never turn it off

67 million
Scam Callback Protection warnings played

100+ billion
malicious domain requests blocked

Combating SIM box fraud

SIM box fraud occurs when criminals load devices with multiple SIM cards to route fraudulent calls and texts at scale, avoiding fees and flooding networks with scam traffic. We use a range of automated detection capabilities, real-time monitoring, analytics, and dedicated investigative resources to detect SIM farm activity.

Our multi-layered approach uses ML models and multiple network and behavioral attributes to detect suspicious activity patterns associated with SIM farms and SIM boxes. This suite of tools allows us to identify and prevent malicious SIM box traffic at its source, protecting our customers and defending critical communications infrastructure from fraud and abuse.



Defending businesses

of every size

From family-owned small businesses to large enterprises, organizations increasingly depend on connectivity to support operations, workforce productivity, customer engagement, payments, cloud applications, and access to sensitive data. As that dependence grows, securing access across users, devices, and locations becomes more critical.

We help businesses address these challenges through solutions designed to identify cyber risk, protect distributed workforces, and secure access to critical applications and data.

Identifying and reducing cyber risk

Modern enterprises require more advanced security strategies as they adopt cloud platforms, mobile-first operations, connected devices, and hybrid work models. Traditional approaches are no longer sufficient; organizations need solutions that protect users, devices, applications, and data wherever work occurs.

To help businesses better manage cyber risk, we offer Risk-Based Vulnerability Management and Patch Management solutions. These solutions help organizations identify security weaknesses, understand which risks matter most, and address critical issues first. By prioritizing vulnerabilities based on their likelihood of exploitation and potential business impact, these solutions help reduce risk to operations, business data, and customer information.

Securing access, devices, and accounts

For organizations embracing hybrid and mobile-first operations, Secure Access Service Edge (SASE) unifies networking and security in a cloud-delivered model. T-Mobile's SASE portfolio—including T-SIMsecure, Security Slice, and SASE delivered with leading security partners—provides secure, zero trust access to applications and data while improving visibility and simplifying policy enforcement across users, devices, and locations.

Within the SASE portfolio, T-SIMsecure helps protect the connection between a user's device and T-Mobile's security platforms over our network. Secure SIM Authentication adds another layer of protection by using the trusted identity of a T-Mobile SIM or eSIM as an authentication factor for users, devices, and connected assets.

Beyond network security, mobile endpoints remain a critical risk surface. T-Mobile's Mobile Threat Defense solutions help mitigate threats such as malicious apps, unsafe links, phishing, device vulnerabilities, and other mobile-targeted attacks. These capabilities, combined with solutions such as SmartVPN and account security safeguards, reduce risks from fraud, unauthorized access, scams, and other disruptive threats.

Together, these solutions reflect our commitment to helping businesses build a resilient, modern security foundation.



Anticipating tomorrow's threats

We continuously refine detection and prevention models to keep pace with the evolving threat landscape. Our honeypot network—a controlled environment designed to attract malicious activity and observe attacker techniques—provides real-world insight into emerging threats. Those insights feed into our AI-driven defenses and help us better understand evolving attack techniques.

The next generation of risk will extend beyond traditional user accounts and network defenses. Non-human identities—including AI agents, bots, and automated services—represent a growing attack surface that requires new approaches to identity, access, and oversight.

To prepare for what comes next, we continue to invest in forward-looking capabilities, including adversarial testing of AI systems, non-human identity security, and preparation for post-quantum encryption standards designed to withstand future advances in computing power. Together, these initiatives help keep our security strategy resilient and adaptable as new technologies and threat vectors emerge.

A message from Mark Clancy, SVP, Information Security Officer



Mark Clancy
T-Mobile SVP, Information Security Officer

Cybersecurity isn't a destination. It's a direction.

Our progress reflects our commitment to keeping consumers and businesses secure. Through collaboration, investment, and transparency, we've strengthened our defenses and worked to earn the trust of those who rely on us.

Cybersecurity is a shared responsibility, and resilience cannot stop at our own perimeter. By working to raise the security baseline across the broader ecosystem—supporting partners, suppliers, and peers—we help create a safer digital environment for everyone.

As threats continue to evolve, our guiding principle remains unchanged: security must be seamless, equitable, and grounded in the needs of the people and businesses we serve. It is fundamental to how we build, operate, and continually strengthen America's Best Network.

Learn more about cybersecurity at T-Mobile in our Trust Center:

https://security.t-mobile.com

T-Mobile

Connect with T-Mobile

T-Mobile.com

© 2026 T-Mobile US, Inc.