November 2025

F-Alert

The latest US cyber security threat updates from F-Secure threat intelligence experts

F-Secure

EXPERT INSIGHT:

“Some AI companies are experimenting with technical safeguards such as crisis detection and usage limits, but since these are probably going to be insufficient to fix the problem, we may need a broader safety approach that includes customer education and regulatory action.”

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, US

How AI Chatbots Are Fueling Digital Psychosis

WHERE: All States

WHAT: Cases of AI-enabled digital psychosis continue to surface in news media. Multiple documented cases show individuals developing severe mental health crises after intensive chatbot use, including hospitalizations, arrests, homelessness, job losses, and even deaths.

KEY FACTS:

- AI systems can act as “sycophantic” reinforcers that validate and amplify delusional thinking. The problem is especially worrisome in chatbots that are designed to maximize engagement rather than provide therapeutic assistance or containment of delusional thoughts.
- The delusion patterns most cited include messianic or grandiose beliefs, the perception of AI as godlike or sentient, and romantic/attachment delusions.
- The phenomenon of AI-induced delusional thinking can affect both individuals with pre-existing mental health conditions and those without a prior history of mental illness, although people with previous mental health issues are at greatest risk.

New F-Secure Report Reveals the Human Cost of Scams

WHERE: US & Global

WHAT: F-Secure has released its second annual Scam Intelligence & Impacts Report, uncovering the human cost of scams on a global scale. The findings show how misplaced confidence in spotting fraud leaves people vulnerable, while stigma and shame keep victims silent—making scams one of the world's most underreported crimes today.

A US edition of the report is scheduled for release later this year.

KEY FACTS:

- 69% of people globally believe they can recognize a scam, yet 43% of those individuals still fell victim in the past year. This overconfidence leaves many emotionally exposed, digitally unprepared, and often too ashamed to speak out.
- Scam victimization is rising sharply: in the United States, scam rates doubled from 31% in 2024 to 62% in 2025. Globally, young adults aged 18–34 face more than double the scam risk of adults aged 65–74.
- Only 7% of scams are reported worldwide, largely due to shame and victim blaming. The reporting rate is even lower in the USA at just 2.6%.

EXPERT INSIGHT:

"Scams aren't just financial crimes; they're psychological and social attacks that exploit trust, confidence, and silence. As a result, consumers worldwide are demanding protection: 50% say they are willing to pay for it, with younger adults expecting it from their service providers. To fight scams, we must shift from blame to resilience—embedding protection into everyday services and empowering people to speak out."

Timo Salmi
Senior Solution Marketing Manager
Oulu, Finland

Trending Scam

Watch Out for ‘Grey Area’ AI Shopping Scams This Fall

WHERE: Boston, MA

WHAT’S HAPPENING:

- Scammers are creating AI-generated fake online stores with convincing backstories—often posing as small, family-run businesses—to lure in unsuspecting shoppers.
- Many of these are Temu drop-shipping fronts featuring fabricated proprietors and deceptive branding. While the setup is entirely fake, complete with AI-generated “shopkeepers,” customers do receive products—but they’re typically low quality.
- One example is “Emma & Jack Boston,” a supposed US boutique that claims to have operated in Boston for years and is holding a closing-down sale before moving to Spain—yet its privacy policy lists a Hong Kong address.

WHAT TO DO:

- AI has made it increasingly difficult for consumers to recognize fraudulent online stores. Service providers can play a key role in reducing risk by raising awareness about AI-enhanced scams and promoting safe online shopping practices.
- Encouraging customers to verify unfamiliar sites—by checking independent reviews on reputable platforms such as Trustpilot and using tools like F-Secure’s Online Shopping Checker—helps prevent fraud and strengthens customer trust.

Breach That Matters

Threat Actors Claim Theft of Data from 5.5M Discord Users

WHERE: San Francisco, CA

WHAT’S HAPPENING:

- Hackers claim to have stolen the data of 5.5 million unique users from Discord’s Zendesk support system instance, including 2.1 million images of government IDs. Discord, however, disputes this—stating that approximately 70,000 users had their government IDs exposed.
- The company has not confirmed that the breach originated from the Zendesk support instance, only that it involved a third-party service used for customer support.
- As many organizations outsource support and IT help desks to business process outsourcing (BPO) providers, these have become attractive targets for attackers seeking access to downstream customer environments.

WHAT TO DO:

- Organizations should review how customer data is handled by third-party service providers, especially those managing support systems or ticketing platforms. Strong contractual and technical controls are essential to ensure customer data is properly protected.
- Because many attacks begin with phishing or impersonation, companies should provide ongoing security awareness training for both internal teams and vendor personnel. Implementing phishing-resistant authentication methods can also significantly reduce the risk of credential compromise.

EXPERT INSIGHT:

"VoIP, like many technologies, was developed for legitimate purposes but later exploited by criminals, who now use it to target and scam people at scale through fraudulent calls and phishing messages. In addition, SIM farms can overwhelm cellular networks with millions of calls in minutes—posing a serious threat to telecom infrastructure. It's a reminder that even simple tools can create real risks for critical systems."

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

SIM Farm Network Discovered: What It Means for Security

WHERE: New York, NY

WHAT: A large network of SIM farms has been discovered and dismantled across New York. The operation contained servers and stacks of SIM cards—more than 100,000 of which were already active. This discovery highlights that criminal infrastructure doesn't just consist of websites and malware, but also of physical components such as SIM cards.

KEY FACTS:

- A SIM card is an incredibly powerful resource for criminals. It enables not only text messaging, phone calls, and number spoofing, but also access to countless online services that require a valid phone number for registration and verification.
- SIM farms are devices that hold hundreds of SIM cards from multiple operators and use Voice over Internet Protocol (VoIP) technology to send or receive bulk messages and calls. This allows criminals to automate communication, bypass verification checks, and exploit online services such as social media platforms, email accounts, and hosting providers.
- Though the investigation is ongoing, authorities describe this operation as a well-funded, highly organized enterprise—possibly linked to nation-state actors.

Social Engineering and Fake Sites Drive Surge in Malware

WHERE: All States

WHAT: Recent malware campaigns highlight how attackers are relying on fake websites and social engineering to trick users into downloading malicious apps. Users have been targeted by a new Android malware family, HyperRat, designed to steal sensitive data, send notifications, and perform other malicious actions on infected devices.

KEY FACTS:

- Once installed, the malicious app requests extensive device permissions—which should be a red flag for any app, regardless of source. They abuse legitimate Android features such as permissions and Accessibility Services, among others.
- The HyperRat remote access trojan lowers the barrier to entry for cyber criminals, enabling even inexperienced attackers to run mobile campaigns with ease. Subscribers receive a ready-made malicious APK, while the seller handles infrastructure and phishing pages.
- This malicious app isn't available on official app stores but instead requires installation from third-party websites. While downloading apps from such sources doesn't necessarily raise red flags, users should be cautious—fake websites imitating legitimate services are often used to spread malware.

EXPERT INSIGHT:

"While completely avoiding installing apps from third-party sources might be too drastic advice for some, the fact remains that security vetting for such apps is beyond the skillset of the average phone user. The best protection against Android malware comes from high-quality security apps and on newer, up-to-date devices, Google Play Protect can also help."

Joel Latto
Threat Advisor
Helsinki, Finland

“Illuminate, F-Secure’s research function, brings together experts to explore the human, social, and technical aspects of security. We identify emerging threats, prototype new protection systems, and anticipate future risks to keep consumers safe. By staying ahead of the curve, we navigate a constantly evolving digital world and ensure F-Secure delivers trusted, reliable, and innovative cyber security solutions.”

Laura James
Vice President, Research
F-Secure

About F-Secure

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 200+ partners.

For more than 35 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For the latest news and updates visit f-secure.com or follow us on our social channels.

F-Secure | illuminate