November 2025

F-Alert

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

F-Secure

2025 US Cyber Threat Recap: Key Lessons for the Year Ahead

In 2025, US consumers lost $64.8 billion to scams, with 70% of American adults experiencing at least one. Across this year's F-Alerts, scams and AI-driven threats dominated, followed by malware risks and a growing focus on stronger consumer protections.

Key trends in 2025:

1. Gen Z is now the most at-risk age group

- US consumers aged 18–24 face 1.6 times the scam risk of adults aged 55–74—and almost half (49%) receive scam attempts every week. Digital fluency doesn't equal digital safety.
- A larger digital footprint, frequent online activity, openness to new tech, and parasocial trust dynamics all increase their exposure.
- This is also why younger adults are most willing to pay for scam protection—61% of 18–24-year-olds, compared to just 46% of adults aged 55–64 and 48% aged 65–74.

2. AI-driven scams primarily use AI for content generation

- Our 2025 analysis of AI-enabled scams identifies four core uses of AI: identifying victims, building attack tools, personalizing scam bait, and engaging with targets.
- In 89% of cases, AI was used to generate content—from phishing messages to voice cloning and deepfake impersonation.
- Two emerging concerns stand out: using AI to analyze data and rank high-value targets and deploying AI chatbots to conduct long-term romance or investment scams.

3. Humans have become the weakest entry point

- Cyber criminals once depended on malware to break into systems. Today, the most vulnerable point isn't technology—it's the human mind.
- Social engineering has become the most reliable method for compromising victims, using psychological manipulation rather than technical exploits.
- Scammers take advantage of cognitive biases by posing as distressed family members, promising fake financial relief, or exploiting people's need for connection.

Sources: GASA State of Scams in the United States of America, 2025; F-Secure Consumer Market Survey, January 2025 (US data); Sample derived from news media reports, industry analysis, and other external and internal intelligence sources, 2025

Key takeaways for 2026:

- Empower consumers through continuous education. Share simple, regular security guidance—especially around trending scams and emerging AI threats. Teach not just red flags, but the emotions and behaviors scammers manipulate.
- Advocate for proactive scam protection. Tools matter when human judgment fails. While 80% of US consumers believe they can spot scams, 60% of those confident individuals still fall victim—a gap that technology can help close.

Discover more 2025 consumer insights in the F-Secure US Scam Intelligence & Impacts Report

Sources: F-Secure Consumer Market Survey, January 2025 (US data),

Online Reviews in Crisis: Can 5-Stars Be Trusted?

EXPERT INSIGHT:

“We're facing a fundamental trust crisis in online commerce that platforms have been very slow to address. It may be time for both customers and legitimate businesses to demand identity verification, purchase requirements, or other safeguards at the platform level.”

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, US

WHERE: All States

WHAT: Online review platforms are facing a crisis of credibility as AI-powered fake reviews, including both fraudulent 5-star promotions and 1-star attacks, have become virtually indistinguishable from genuine consumer feedback.

KEY FACTS:

- The Guardian reports that review sites like TrustPilot are full of fake 5-star reviews placed by scammers and brand impersonators.
- AI technology is helping scammers write fake reviews without traditional “tells” such as poor grammar and spelling. Recent academic research shows that consumers asked to differentiate between real and AI-generated reviews are only right about 50% of the time, or no better than a coin toss.
- It’s not just 5-star reviews that are fake. A CBS news investigation revealed dozens of New York City restaurants were battling extortionists who used 1-star reviews as weapons, posting fake, negative comments to Google Reviews unless the restaurants paid money to remove them.

Agentic Browsers: Innovation's Next Leap—And Its Cautions

WHERE: All States

WHAT: Agentic browsers are the latest evolution of AI-driven tools—web browsers that don't just find information but act on your behalf as a "buddy." Recent research from F-Secure's Abdullah Al Mazed and Tony Shepherd explores the benefits, drawbacks, and emerging risks of agentic browsers and one of their most anticipated use cases: shopping.

KEY FACTS:

- Major browsers are racing to integrate AI assistants directly into their interfaces. Microsoft Copilot now appears in Edge, while Gemini is embedded in Chrome. New agentic browsers are also entering the market, such as Perplexity's Comet and OpenAI's ChatGPT Atlas.
- Unlike traditional browsers, agentic browsers can perform actions automatically on behalf of users, carrying out complex workflows across multiple websites through human language instructions in a chat-like interface.
- One prominent use case is shopping automation—for faster decisions, price tracking, and acting when a product becomes available. But as with any new tech, agentic browsers bring vulnerabilities such as hacking, spoofing, and unknown risks.

[Read the full article here]

EXPERT INSIGHT:

"The promise of convenience from agentic browsers is real. However, their speed of deployment continues to outpace security. Even more concerning is that agentic browsers have access to data like our browsing history, greater exposure to untrusted content, and a broader ability to communicate externally. If exploited, they could become a powerful new tool for scammers. As users, we should balance caution with openness to innovation."

Abdullah Al Mazed
Head of Protection Concept Lab
Oulu, Finland

Trending Scam

Think Before You Click: ‘Tis the Season for Shopping Scams

WHERE: All States

WHAT’S HAPPENING:

- The foundation of many online shopping scams is a simple click on a malicious link. You receive a promotional email announcing new product drops—click to browse. You see a social media ad offering an exclusive discount—tap to buy. You get a text message about a delayed gift delivery—click to track.
- Once scammers hook users, they redirect them to fraudulent websites where they steal their credit card details, commit financial fraud, or spread malware.
- Online criminals rely on psychological manipulation to make people click without thinking. They exploit urgency (“Only 2 left!”), fear (“You missed your delivery”), and FOMO (“Don’t miss this offer—get it before it’s gone”).

WHAT TO DO:

- Help consumers stay safe this shopping season: warn them about hidden links in “buy now” or “click here” buttons and hyperlinks, and remind them to preview links before clicking—hover on desktop or press and hold on mobile.
- With AI making fake profiles harder to spot, the safest option is to go directly to the source instead of clicking links in ads or messages. Consumers can also use an online shopping checker to confirm if a site is safe before buying.

Breach That Matters

Hyundai AutoEver Breach Exposes Social Security Numbers

WHERE: All States

WHAT’S HAPPENING:

- Hyundai AutoEver America, an IT services affiliate of Hyundai Motor Group, is notifying individuals of a cyber breach affecting its internal systems. Hackers gained unauthorized access between February 22 and March 2 earlier this year.
- The company provides IT and digital manufacturing services across Hyundai and Kia operations, including vehicle connectivity, telematics, and business systems supporting millions of users and vehicles.
- Exposed information reportedly includes names, Social Security numbers, and driver’s license details, though it remains unclear whether the breach impacted employees, customers, or both. No ransomware group has claimed responsibility.

WHAT TO DO:

- **Monitor for identity theft or fraud:** Individuals notified should consider placing fraud alerts, freezing credit reports, and watching for suspicious financial activity.
- **Verify communications:** Be cautious of follow-up emails or calls referencing the breach. Hyundai AutoEver will not request sensitive data such as passwords or Social Security numbers via email.

Military Raid Shuts Down Forced-Labor Scam Center

EXPERT INSIGHT:

“Although this case was widely publicized, it’s unlikely to make much difference to the number of scams originating from the region. We expect to see more large-scale operations as governments work together to end not only widespread scamming, but also the humanitarian crisis that has developed alongside the highly organized cyber crime industry.”

Joel Latto
Threat Advisor
Helsinki, Finland

WHERE: Myanmar, with victims in the United States

WHAT: Myanmar’s military has shut down and demolished buildings belonging to a major scam operation in an effort to curb cross-border online fraud. The crackdown left hundreds of workers—many reportedly held under duress and originating from 28 countries—fleeing to Thailand.

KEY FACTS:

- Myanmar is widely recognized as a hotspot for large-scale cyber scam operations that lure foreign workers with false promises of legitimate employment, only to trap them and force them into criminal activity.
- The United States Institute of Peace estimates that hundreds of thousands of people work in scam centers like these across the region, many of them held in captivity.
- Although most of these scam centers are located in Southeast Asia, their operations target victims globally, including in the United States.

Tap, Relay, Steal: Inside NFC Malware's New Playbook

WHERE: Eastern Europe, with potential spread to the US

WHAT: Android malware abusing the platform's NFC permissions is on the rise. Threat actors are tricking victims into installing malicious apps that mimic well-known banking apps and exploit Android's Host Card Emulation (HCE) to steal payment data.

KEY FACTS:

- According to a recent report, threat actors are distributing malicious sideloaded Android APKs that impersonate major banks like Santander and ING. Victims are typically lured through phishing messages about bank impersonation, suspicious transactions, or other urgent prompts that direct them to download the fake apps.
- Early variants mainly requested access to the NFC module, but newer versions have evolved to target payment card data more aggressively, using multiple techniques to capture and transmit sensitive information.
- Attackers now exfiltrate EMV payment fields to Telegram channels, gather card details during voice calls, and install NFC relays on infected devices to pass payment credentials to their infrastructure.

EXPERT INSIGHT:

"Scammers are continuously evolving their tactics. As the use of NFC payments grows, so does the incentive to abuse these systems for illicit gain. The irony here is that near-field communication is being exploited by scammers who are often operating far away. They are always looking for novel techniques to make money—and as new payment methods become popular, their abuse quickly follows."

Amit Tambe
Senior Researcher
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