May 2025

F-Alert

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

F-Secure

The Future of US Consumer Protections May Be at Risk

EXPERT INSIGHT:

“By weakening independent consumer protection agencies, the administration risks creating a regulatory vacuum—a situation that scammers will be all too eager to exploit, leaving victims with fewer options for restitution.”

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, US

WHERE: All States

WHAT: The newly elected US presidential administration has launched a significant restructuring of federal agencies, including those central to consumer safety and scam protection. This overhaul carries serious implications for the future of consumer safeguards and efforts to hold scammers accountable.

KEY FACTS:

- The administration has taken steps to effectively shut down the Consumer Financial Protection Bureau (CFPB), an agency established in 2010 to protect consumers from financial fraud and scams. A back-and-forth between the judiciary and the administration over the legality of this is expected to continue for months.
- In February, the president signed an executive order aiming to extend presidential oversight over previously independent regulatory bodies, including the Securities and Exchange Commission (SEC), the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC). By reducing their autonomy, the order risks compromising their ability to safeguard consumer interests.
- Acting on the order, the administration has reshaped the FTC—formerly a bipartisan agency—raising concerns about its continued effectiveness. The FTC handles many consumer-facing responsibilities, including the enforcement of antitrust laws.

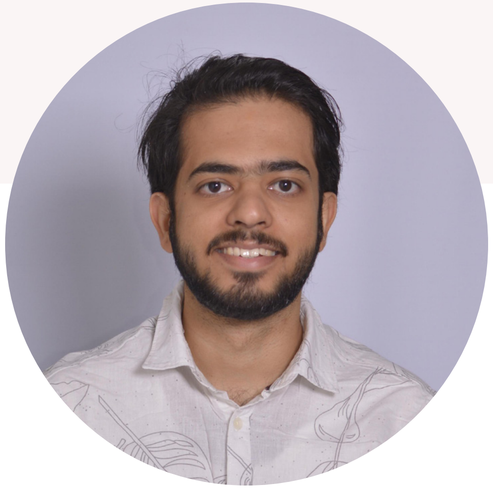
AI Studio Ghibli Art Trend Becomes a Privacy Nightmare

WHERE: All States

WHAT: A viral trend that transforms personal photos into Studio Ghibli-style art using AI tools is gaining momentum—but it also carries overlooked privacy risks. Many platforms ask users to upload images without explaining how the data will be used. Behind the fun lies a lack of transparency, with concerns about privacy, data storage, and image reuse.

KEY FACTS:

- Many uploaded photos contain hidden metadata—such as location and timestamps—yet most platforms provide vague terms of service. This lack of clarity leaves users uncertain about how their data is used, creating opportunities for misuse such as unauthorized image reconstruction or data profiling.
- The trend's surge in popularity—fueled by tools like GPT-4o—has also attracted malicious actors. Fake Android apps and phishing sites are now mimicking popular platforms to trick users into sharing personal data under false pretenses.
- Engaging visuals and seamless user flow often encourage uploads without informed consent. In some cases, these images may be stored, used to train AI models, or exploited for surveillance or targeted advertising without the user's knowledge.



EXPERT INSIGHT:

"This trend shows how viral tech can be both fun and risky. These tools tap into the fear of missing out: when something feels fast and exciting, people often click 'accept' without thinking. That's what scammers rely on—mass attention and low caution. Consumers should avoid sketchy links or apps and stay mindful of the data they share. Even seemingly harmless photos carry risks."

Apramey Bhat
Researcher
Helsinki, Finland

Trending Scam

New Wave of ‘Unpaid Toll’ Phishing Scams Target Consumers

WHERE: All States

WHAT’S HAPPENING:

- A new phishing campaign impersonating toll agencies—including E-ZPass, I-Pass, and FasTrak—is targeting consumers via SMS and iMessage.
- The messages—often sent using spoofed sender IDs—falsely claim that recipients owe unpaid toll fees and urge them to click links leading to phishing websites designed to steal personal and financial information.
- The campaign has been linked to a Chinese cyber crime group known as the Smishing Triad, which has registered more than 60,000 domains to support these attacks.

WHAT TO DO:

- Consumers who receive urgent messages requesting immediate payment or account verification should not engage. They should avoid clicking links in unsolicited messages—even if the sender appears to be a legitimate company.
- Instead, consumers should log into their account directly to check for alerts or contact the toll agency using an official number to verify the message.

Breach That Matters

Driver’s Licenses Stolen in Car Hire Company Data Breach

WHERE: CA, ME, TX & VT (currently)

WHAT’S HAPPENING:

- Car hire company Hertz Corporation has confirmed that customer data—including driver’s licenses and credit card information—was stolen in the Cleo zero-day attacks late last year. The breach affected customers of its Hertz, Thrifty, and Dollar brands.
- Additionally, the company stated that a “very small number” of individuals may have had more sensitive information exposed, including Social Security numbers, government IDs, passport numbers, and Medicare or Medicaid IDs.
- While Hertz has not disclosed the total number of affected customers, notifications have so far been issued in several states—including California, Vermont, Texas (more than 96,600 customers), and Maine (at least 3,400 customers). The total number of affected individuals is likely much higher.

WHAT TO DO:

- Consumers who suspect their personal information may have been compromised should monitor financial accounts regularly for signs of unusual activity.
- Hertz is offering affected customers two years of free identity monitoring and has advised them to remain alert for potential fraud.

EXPERT INSIGHT:

“Data doesn't get much more personal than this. Genome data can’t be changed like a leaked password. Once someone, willingly or not, gives access to that data, they can never truly get it back. And like any other data, it’s likely to be sold and resold. I strongly recommend consumers permanently delete their 23andMe data. Doing so means losing the account—but regaining some control over the fate of their sensitive information.”

Joel Latto
Threat Advisor
Helsinki, Finland

23andMe Bankruptcy: What Happens to Genetic Data?

WHERE: All States

WHAT: Genetic testing company 23andMe filed for bankruptcy on 23 March this year, raising urgent questions about the fate of the vast trove of genetic and health-related data it has accumulated. Privacy concerns grew further after a US judge ruled that the company could sell this highly sensitive data as part of the bankruptcy proceedings.

KEY FACTS:

- Upon signing up, users agreed to T&Cs and a privacy notice permitting the company to use their data for research, development, and third-party sharing. Many also submitted health data via surveys and saliva samples. But how many truly understood the scope of their consent—or that their data might be used or sold?
- This isn’t the first time 23andMe has faced scrutiny. In 2018, the FTC investigated the company and other DNA testing services over their genetic data-sharing policies.
- More recently, in October 2023, a data breach exposed the personal information of 6.9 million users. The incident raised alarms about the potential misuse of genetic data, particularly the risk of targeting individuals based on ancestry.

Are ‘AI Scam Agents’ the Next Big Threat to Consumers?

WHERE: All States

WHAT: So-called ‘AI agents’— autonomous systems capable of performing complex tasks on behalf of a user or another system—are emerging as the latest focus of AI hype. Some misleading claims suggest scammers are already using them, but we’ve seen no real-world evidence to support that. Here’s a look at the reality of AI’s potential for misuse.

KEY FACTS:

- While scammers increasingly use AI, they don't yet deploy fully autonomous agents. Instead, they use AI to generate deepfakes, text, and images, while much of the scam infrastructure—like building fake profiles, scripting conversations, making calls, and handling money transfers—remains manual.
- In a recent test, we explored AI’s potential for deception—specifically, whether it could be prompted to behave like a scammer. The results showed that an open-source LLM could be easily manipulated through fine-tuning and prompt engineering, turning it into a highly effective tool for social manipulation and fraud.
- Although the use of AI in scams is still largely manual, the automation of scam operations using AI agents could allow them to scale faster—enabling bots that not only interact with victims, but also perform account takeovers, and much more.

EXPERT INSIGHT:

“Are scammers using AI? Yes, absolutely. Are AI agents being used to scam people? Not yet, but this could change soon. For AI agents to become attractive tools for scammers, I believe they first need to become more popular and widely adopted. Right now, many scam tools are already simple to use—but AI agents could lower the barrier for less tech-savvy criminals to launch convincing scams at scale.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

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