June 2026

F-Alert

The latest U.S. cyber security threat updates from F-Secure threat intelligence experts

F-Secure

EXPERT INSIGHT:

“This is a meaningful step forward for Apple, especially since Android has supported the feature for many years. It’s even better that end-to-end encryption is enabled by default — as it always should be. This is an easy way to increase the privacy of non-technical users who may not use encrypted messaging apps as their main communication tools.”

Joel Latto
Threat Advisor
Helsinki, Finland

Apple Makes iPhone-to-Android Texting More Secure

WHERE: All States

WHAT: Apple has confirmed that its latest iPhone update, iOS 26.5, makes text messages between iPhones and Android phones more private and secure. The update improves Rich Communication Services (RCS) messaging, the newer texting standard used when iPhone and Android users message each other.

KEY FACTS:

- RCS already supports features like read receipts, typing indicators, and higher-quality photos and videos — similar to Apple’s iMessage. But with iOS 26.5, Apple has also added end-to-end encryption for RCS messages.
- This means only the sender and the recipient can read the messages. Nobody else — including Apple, phone carriers, or hackers — should be able to access their contents.
- Apple says the feature will work with mobile carriers that support it, and availability will roll out gradually. Although Apple still labels the feature as a “beta,” it became available to users when iOS 26.5 launched on May 11, 2026.

AI Model Mythos Could Make Cyber Attacks Easier to Launch

WHERE: All States

WHAT: New AI model Mythos has raised questions after reports claimed it was highly effective at finding serious software vulnerabilities, also known as “zero day” security flaws with no fix available yet. Cyber criminals and state-sponsored attackers can use them to secretly break into devices, steal data, or spy on users.

KEY FACTS:

- Mythos was developed by Anthropic and released privately to a small group of technology companies, including Nvidia, Microsoft, and Amazon, through its Glasswing program. The model is not currently available to the public.
- Some believe the discussion around Mythos may be overstated, but F-Secure's threat intelligence team anticipates that in the next 6–12 months, AI tools will become increasingly capable of finding vulnerabilities. While major tech companies have the resources to release security updates quickly, smaller software companies may be less prepared.
- Everyday users could be affected if AI-powered vulnerability hunting becomes more widespread. Consumer apps, games, utility software, cryptocurrency wallets, and smaller banking services could become targets for cyber criminals looking for easier ways to attack users or steal data.

EXPERT INSIGHT:

“There’s been a lot of hype around Mythos. The biggest concern isn’t necessarily major operating systems or browsers — it’s the huge number of smaller consumer software vendors that may not have the resources or knowledge to improve their security. If AI makes vulnerability hunting easier for cyber criminals, the most important thing consumers can do is keep their apps and devices updated as quickly as possible.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

Trending Scam

Google Used to Target Facebook Business Accounts

WHERE: All States

WHAT'S HAPPENING:

- Cyber criminals are abusing trusted Google services, including Google AppSheet and Google Drive, to send phishing emails that can bypass some security filters and appear more legitimate to victims.
- The scam emails often warn users that their Facebook Business account is at risk of being suspended due to fake copyright complaints or policy violations and pressure victims to act quickly and click malicious links.
- Researchers say more than 30,000 users have already been affected globally. Some scams use fake Facebook support pages to steal passwords, ID documents, and two-factor authentication (2FA) codes in real time.

WHAT TO DO:

- Be cautious of urgent emails claiming your Facebook account will be disabled or restricted, especially if they pressure you to act within hours.
- Always access Facebook Business accounts directly through the official Facebook website or app instead of clicking links in emails, even if the message appears to come from a trusted company like Google.

Breach That Matters

Amtrak Data Breach: 2.1 Million Customer Records Exposed

WHERE: All States

WHAT'S HAPPENING:

- A dataset linked to Amtrak has appeared online, with reports that hackers may have accessed more than 2.1 million customer records, including names, email and home addresses, and customer support information.
- Stolen support tickets and travel-related details could make phishing scams far more convincing — attackers may use real trip details, refund requests, or past customer service interactions to trick victims into sharing sensitive information.
- Reports suggest the attackers may have targeted cloud-based customer systems, which companies use to store large amounts of customer information in one place.

WHAT TO DO:

- Be cautious of emails, text messages, or phone calls claiming to be from Amtrak or travel companies, especially if they reference past trips, refunds, or account issues and ask you to click a link or share information.
- Change passwords for your travel and email accounts if you believe your information may have been exposed. Enable 2FA where possible.

AI is Putting Large-Scale Cyber Attacks Within Anyone's Reach

WHERE: All States

WHAT: Cyber security researchers have found that AI tools are making it easier for individuals with little or no technical background to carry out cyber attacks that previously required skilled hacker groups or organized criminal teams. This shift is happening as AI-powered coding tools become more advanced and more widely available.

KEY FACTS:

- Individuals are using AI tools to help develop malicious software, automate attacks, analyze stolen data, and create convincing phishing scams. In one case, a 17-year-old in Japan allegedly used malicious code to steal the personal data of more than 7 million users from internet café chain Kaikatsu Club.
- Another incident involved teenagers with no coding background using AI chatbots to target mobile services. Solo attackers have also used AI coding tools to extort at least 17 companies and compromise the Mexican government's systems.
- At the same time, cyber attacks are happening faster. Security researchers say the time between a software vulnerability being publicly disclosed and criminals attempting to exploit it fell from over 700 days in 2020 to just 44 days in 2025.

EXPERT INSIGHT:

"While AI is also helping security teams improve defenses, the biggest challenge is that AI tools are lowering the technical barrier to cyber crime. In the past, many of these attacks required highly skilled hacker groups. Now, individuals with very limited technical knowledge can use AI tools to help create malicious code, automate attacks, and quickly scale their operations. That's a meaningful shift in who can cause harm — and how fast."

Timo Salmi
Senior Product Marketing Manager
Oulu, Finland

Criminals Are Selling Tools to Bypass Bank Identity Checks

EXPERT INSIGHT:

“Facial recognition and liveness checks are no longer sufficient to establish identity. Banks and exchanges must now layer behavioral analytics, device integrity checks, and transaction monitoring on top of the face scans to stay ahead of criminals. This will add friction but will be necessary as AI-powered tools become more sophisticated.”

Dr Megan Squire
Principal Threat Intelligence Researcher
North Carolina, United States

WHERE: All States

WHAT: A two-month MIT Technology Review investigation uncovered an active black market on Telegram where criminals sell ‘bypass kits’ that trick the facial recognition and liveness checks used by major banks to verify customer identity.

KEY FACTS:

- A liveness check is a security step during identity verification that uses the mobile phone’s camera to confirm a real, living person is present in front of it. This software analyzes subtle cues like blinks, head movements, and the depth of a real face.
- These tools, often built around ‘virtual camera’ software that feeds fake images or deepfakes into banking apps, are being used by money-laundering operations tied to Southeast Asian scam compounds. Workers use the kits to open money mule accounts at mainstream banks and cryptocurrency exchanges.
- Reporters identified 22 public Telegram channels and groups openly advertising bypass kits for this type of liveness data and stolen biometric data — some with thousands of subscribers. Bank identity verification software providers estimate that virtual camera exploits were more than 25 times as common in 2024 than in 2023.

“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 is a human-first, AI-powered consumer cyber security experience company with 37 years of expertise in tackling digital threats. We help Digital Service Providers turn trust into a high-value growth engine — protecting their customers while enabling them to live their best digital lives in a world of relentless, AI-driven scams.

With billions of digital interactions secured each year, tens of millions of consumers protected globally, and over $10bn in partner value created, we deliver proven impact at scale.

To find out more visit f-secure.com/partners
or follow us on our social channels.

F-Secure | illuminate