April 2026

F-Alert

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

F-Secure

AI Just Made Online Anonymity Much Harder to Maintain

WHERE: All States

WHAT: Most people have long operated online under a simple assumption: posting under a username, rather than a real name, offers a degree of anonymity and makes it difficult to connect the two. However, new research shows that AI can now link anonymous accounts to real identities—cheaply, accurately, and at scale.

KEY FACTS:

- A team from ETH Zurich, MATS, and Anthropic has shown that LLMs can deanonymize accounts at a scale and speed that wasn't previously possible. Their system analyzes anonymous posts for signals—career details, location clues, interests, and writing patterns—then searches for matches across known identities and evaluates likely connections.
- When tested on Hacker News accounts matched against LinkedIn profiles, it correctly identified two-thirds of users at 90% precision. On Reddit, it linked users across communities and time periods, outperforming traditional methods.
- The system doesn't rely on obvious mistakes like sharing a real name or profile link. Instead, it uses "micro-data"—small details such as lifestyle details, locations, or niche interests. Combined, these signals form a unique fingerprint.

EXPERT INSIGHT:

"The implications are wide-ranging. Governments could link pseudonymous accounts to real identities for surveillance. Stalkers could automate their searches. Corporations could connect anonymous posts to customer profiles. Attackers could build profiles for targeted social engineering. For anyone posting under a pseudonym, assume your accounts can be linked to your real identity, with the risk increasing as more information is shared."

Dr Laura James
Vice President of Research
Liverpool, UK

EXPERT INSIGHT:

“The current scam landscape has removed many of the technical barriers traditionally associated with cyber crime. This makes scamming particularly appealing to young people looking for easy money, who may not fully grasp the seriousness of the crime. I do commend this public shaming tactic and can see other countries, including the U.S., taking their own ‘name and shame’ strategies a step further too.”

Joel Latto
Threat Advisor
Helsinki, Finland

Dutch Police Shame Scammers—Could It Work in the U.S.?

WHERE: All States

WHAT: Dutch police are taking a bold new approach to catching scammers: publishing their faces everywhere. Billboards, television, online ads—you name it. The large-scale ‘Game Over?!’ campaign aims to identify and bring in prolific criminals. This raises the question of whether similar measures could be used in the U.S.

KEY FACTS:

- In early March, Dutch police announced that 100 suspected scammers would have two weeks to surrender, or their faces would be made public. The campaign has a dual aim: to identify suspects and deter others from engaging in scam activity. And it appears to be working—21 suspects either came forward or were identified through tips.
- On March 23, the police followed through by publishing the faces of the remaining 79 suspects. The individuals are believed to be linked to around 13,000 scam cases, with total losses estimated at over $78 million.
- Public exposure tactics are not new in the U.S.—from the FBI’s Most Wanted list to televised policing and law enforcement footage—suggesting that while the Dutch approach is more direct, similar tactics already exist and could be expanded.

Trending Scam

Signal ‘Support Bot’ Scam Used to Hijack Accounts

WHERE: All States

WHAT’S HAPPENING:

- Dutch intelligence agencies warn that Russian state-backed hackers are using a phishing scam posing as a Signal ‘support bot’ to hijack accounts, tricking users into sharing verification codes or linking new devices.
- The attacks don’t exploit the apps themselves but rely on user trust in secure messaging apps. Once access is granted, attackers can silently read private messages and group chats without alerting the victim.
- Officials, journalists, and others discussing sensitive topics are primary targets, as trusted messaging apps have become key channels for high-value communications.

WHAT TO DO:

- Never share verification codes or follow instructions from unsolicited support messages—legitimate services will not ask for this information.
- Check linked devices, look out for duplicate accounts in group member lists, and treat unexpected account-related messages as potential phishing attempts.

Breach That Matters

Misconfigured Cal AI App Exposes 3M User Records

WHERE: All States

WHAT’S HAPPENING:

- Calorie-tracking app ‘Cal AI’ has reportedly exposed data from around three million users after a major security misconfiguration left its database accessible without authentication.
- The breach includes sensitive personal data such as email addresses, names, dates of birth, and detailed health information including weight history, eating habits, and exercise goals.
- Subscription and transaction data were also exposed, increasing the risk of targeted scams, phishing, and account abuse using personalized information.

WHAT TO DO:

- Be cautious of unsolicited emails, messages, or offers related to health apps, subscriptions, or fitness services—especially those that reference personal details.
- Review accounts linked to health or fitness apps, enable two-factor authentication where possible, and avoid reusing passwords across services.

Government-Grade iPhone Exploit is in Criminal Hands

WHERE: All States

WHAT: A government-grade iOS exploit kit known as "Coruna" has fallen into the hands of cyber criminals and is now being deployed at scale. The tool allows attackers to silently compromise iPhones simply by luring users to malicious websites—creating a new opportunity for scam operations to combine social engineering with device-level access.

KEY FACTS:

- The exploit kit contains 23 exploits and multiple attack chains, enabling attackers to fully compromise iPhones running iOS versions from 2019 through late 2023 just by getting users to visit a malicious or fake website.
- Scam sites—particularly fake cryptocurrency and financial platforms—have already been found embedding the exploit, turning routine social engineering lures into full device takeovers without visible signs to the victim.
- Once deployed, the malware can steal sensitive data, access photos and emails, and drain crypto wallets. Around 42,000 devices are estimated to have been impacted by financially motivated attacks.

EXPERT INSIGHT:

"When advanced exploit tools designed for government use enter the criminal ecosystem, they lower the barrier for large-scale attacks. For consumers, visiting a malicious website is no longer just a phishing risk—it can lead to full device compromise. Keeping devices updated and avoiding untrusted sites is now critical to staying protected."

Timo Salmi
Senior Product Marketing Manager
Oulu, Finland

U.S. Makes Scam Centers a National Security Priority

EXPERT INSIGHT:

“In today’s polarized political climate, cracking down on scams and fraud is something that everyone can agree is a good idea. Any disagreements with this executive order will likely hinge on execution, not the rationale behind it.”

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, USA

WHERE: All States

WHAT: In March, U.S. President Trump signed an executive order to make cyber crime and scam centers a national security priority. The order aims to coordinate a whole-of-government response to protect Americans from scams such as cryptocurrency investment fraud, phishing, and sextortion.

KEY FACTS:

- Cabinet-level departments have been given 60 days to review existing frameworks and 120 days to deliver an action plan identifying the transnational criminal organizations behind scam centers and proposing ways to dismantle them.
- The order also formalizes a Victims Restoration Program, giving the Attorney General 90 days to recommend how funds can be returned to victims.
- It calls for international consequences against nations that tolerate transnational criminal organizations, including sanctions, visa restrictions, trade penalties, and the expulsion of complicit foreign diplomats.

“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