February 2026

F-Alert

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

F-Secure

2026 PREDICTION

AI Agents Acting on Our Behalf Will Redefine Cyber Risk

EXPERT INSIGHT:

“When AI systems are trusted to act autonomously, the security challenge changes completely. It’s no longer enough to protect people from making bad decisions online. We now must protect AI systems that make those decisions for them, often at machine speed and without human intuition.”

Timo Laaksonen
President and CEO
Helsinki, Finland

WHERE: Global

WHAT: In 2026, agentic AI will fundamentally reshape the digital threat landscape. These systems will no longer just assist users, but act independently, making decisions, moving money, and interacting with services on our behalf.

KEY FACTS:

- This shift in the way we interact in the digital world introduces a new class of cyber risk, where software becomes both the operator and the victim.
- Agentic AI lacks the contextual judgment humans rely on to detect manipulation, deception, or social engineering. As adoption accelerates across consumer and business services, attackers will focus on exploiting decision logic rather than user behavior.
- Security, oversight, and clearly defined limits on AI autonomy are critical foundations for the next phase of digital life.

2026 PREDICTION

Scam Centers Will Become a High-Profile Security Threat

WHERE: United States & Southeast Asia

WHAT: In 2026, industrial-scale scam centers operating out of Southeast Asia will become one of the most visible and politically charged cyber security threats facing the U.S.

KEY FACTS:

- The newly formed Scam Center Strike Force—a joint effort between the U.S. Attorney's Office, DOJ, FBI, and Secret Service—has already seized more than $400 million in cryptocurrency and dismantled major scam infrastructure linked to Cambodia, Laos, and Myanmar.
- Last year, U.S. officials seized $15bn in bitcoin allegedly tied to scam mastermind Chen Zhi and charged him with fraud and money laundering. He was recently arrested by Cambodian authorities and extradited to China.
- While enforcement is accelerating, experts warn that lasting success will require sustained international cooperation and deeper public-private partnerships to stop platforms and internet services from being used to enable cyber crime.

EXPERT INSIGHT:

"These scam centers represent a massive wealth transfer from American families to organized crime. Nearly $10 billion is stolen from Americans every year, and what's different now is the coordinated effort to dismantle not just the scammers, but the entire ecosystem that enables them, including U.S.-based internet infrastructure."

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, USA

Trending Scam

"Truman Show" WhatsApp Scam Steals IDs and Selfies

WHERE: Global

WHAT'S HAPPENING:

- A new fraud operation dubbed the 'OPCOPRO scam' uses AI and bots to build fake communities and trust over weeks, drawing mobile users into a fabricated "Truman Show" style digital world.
- Victims are typically lured via SMS messages impersonating Goldman Sachs and then added to a WhatsApp "investing" group run by two AI-generated personas: Professor James and his assistant Lily.
- After several weeks, victims are pushed to download the OPCOPRO app, complete an identity check by submitting photo ID and a liveness selfie, and deposit funds with promises of 370%–700% returns. The app has no real trading functionality and simply shows fake figures to harvest money and personal data.

WHAT TO DO:

- Stolen IDs and liveness selfies can enable SIM swaps, workplace account takeover, and financial fraud.
- Treat unsolicited investment offers as scams, avoid links or investing groups from unexpected messages, and never submit ID or liveness checks unless independently verified through official channels.

Breach That Matters

Instagram Denies Breach as Reset Emails Alarm Users

WHERE: Global

WHAT'S HAPPENING:

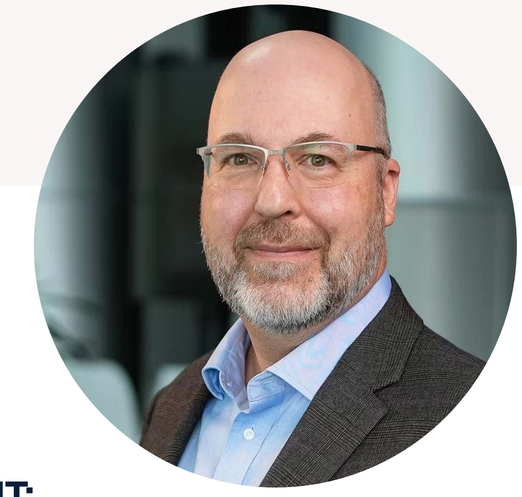
- Instagram continues to deny an alleged breach after many users reported receiving password reset emails. The reports come amid claims that data linked to more than 17 million accounts was scraped and leaked online.
- In response, the platform says it has "fixed an issue that allowed an external party to request password reset emails for some Instagram users" and that "people's Instagram accounts remain secure."
- At this stage, there's no confirmed evidence of a new breach. The activity could stem from API abuse, recycled or older data aggregated into a larger list, or unrelated password-reset activity misinterpreted as a hack.

WHAT TO DO:

- Enable two-factor authentication and stay alert for phishing emails, smishing texts, and social engineering attempts designed to steal passwords.
- Ignore and delete any password reset emails or SMS messages that were not requested.

2026 PREDICTION

AI Identity Fraud Will Reach an Industrial Scale



EXPERT INSIGHT:

“AI has made synthetic identity fraud far more convincing and scalable. Criminals can now generate fake documents, bypass video and photo ID checks, and build credit histories that appear legitimate across multiple systems.”

Bill Lott
Head of Marketing, Embedded Solutions
Atlanta, USA

WHERE: Global

WHAT: In 2026, criminals will increasingly use AI to generate synthetic identities by combining stolen real data with fabricated details, creating new personas that can pass verification checks, open bank accounts, and secure loans.

KEY FACTS:

- Research shows that individuals are willingly selling their identities, giving criminals legitimate credentials to exploit.
- The impact is already measurable: more than 6.4m identity theft and fraud reports are estimated to have been sent to the Federal Trade Commission in the U.S. alone over the last year.
- Financial institutions face mounting pressure to adopt multi-layered verification capable of detecting these hybrid identities. Meanwhile, individuals who sell their credentials risk legal liability for crimes and debts committed in their name, creating victims on both sides of the fraud.

2026 PREDICTION

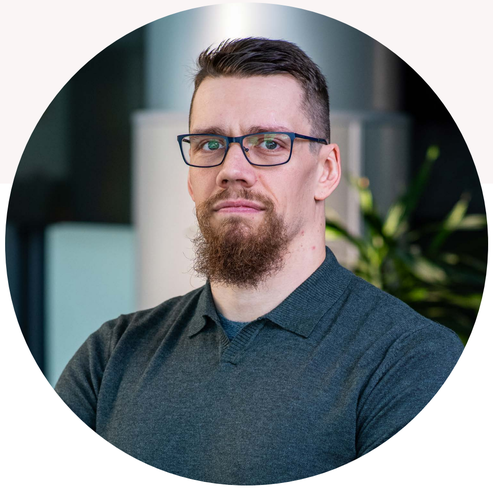
LinkedIn's Trust Signals Will Keep It a Target for Job Scams

WHERE: Global

WHAT: In 2026, LinkedIn will remain a major channel for employment scams. The platform's scale makes it a prime target—and its high-trust reputation can lend credibility to fraudulent job offers. Job market uncertainty, combined with anxiety about AI replacing roles, will only make conditions even more conducive for these schemes.

KEY FACTS:

- Scammers typically reach victims via direct messages or comments under popular posts. Their "job offers" may promise high pay for minimal experience, flexible hours, and fully remote work—so they never have to meet in person. Job titles may be vague, and the hiring process unrealistically fast.
- These scams often include obvious red flags, but they target people in vulnerable situations (for example, after a layoff), making victims more likely to engage.
- Once contact is established, scammers exploit victims by harvesting personal data for identity theft, attempting account takeover, requesting an "advance fee" for recruitment or onboarding, or running a fake equipment reimbursement scheme.



EXPERT INSIGHT:

"LinkedIn detects and removes tens of millions of fake accounts each year, but some still slip through. To spot these scams, check the sender's profile for low engagement and few connections, look for a verification badge and review its details, and run a reverse image search. If it seems too good to be true, verify the role independently by contacting the company directly."

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