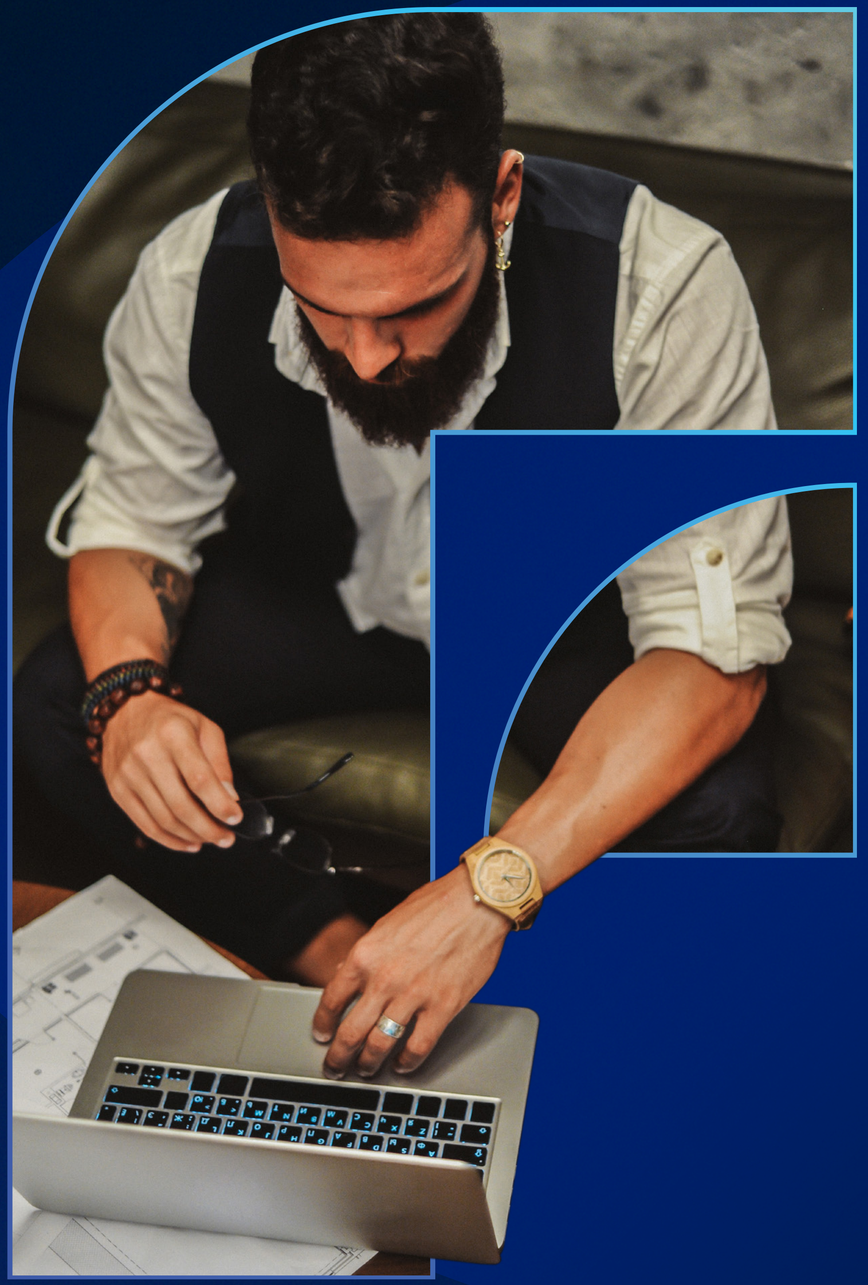
June 2025

F-Alert

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



F-Secure

Inside the Scammer ‘Flex’ Culture on Social Media

WHERE: Germany & Global

WHAT: A criminal network operating across Asia has been linked to fake delivery scams targeting consumers in Germany and around the world. These scammers don’t lurk in the shadows of the internet as you might expect—instead, they flaunt their stolen wealth openly on social media, showing off designer outfits and luxury cars.

KEY FACTS:

- Central figures in one of the world’s largest phishing networks have been identified—brazenly showing off their extravagant lifestyles online. But why do bad actors feel the need to flex? Ego plays a role, but it’s also a deliberate tactic. Flaunting wealth makes others believe they too could succeed—if only they buy into the scheme.
- In this case, this group lures victims through mass text messages claiming to provide “updated shipping information,” each linking to a fake website that closely mimics a legitimate delivery service. Globally, more than 900,000 people have entered their credit card details into these fraudulent sites.
- Scammers flaunting wealth online isn’t new. A recent TikTok video showed one flashing wads of cash, claiming he made his fortune by stealing Fortnite credentials. These can be monetized by selling rare-skin accounts, saved payment details, and more.

EXPERT INSIGHT:

“More and more, cyber criminals are openly flaunting how they make money through scams. Some are part of organized crime gangs, while others operate alone—yet most use aliases to conceal their identities. Yes, they flex online—but they still need to hide who they really are, because what they’re doing is illegal. At times, it seems these criminals believe the internet shields them from the law and makes them untouchable. But that’s simply not true.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

AI Makes Online Stalking Easier Than Ever—Here's How

EXPERT INSIGHT:

“AI’s ability to reveal internet users’ locations isn’t new. What is new is the unprecedented precision it now offers to online stalkers—without requiring any technical skill. Does this mean people should stop posting photos online? No. But users should post more mindfully, paying attention to what’s visible in the frame—especially public figures, those who have experienced stalking, or anyone concerned about privacy. Like everything else, AI is only going to get better at this.”

Joel Latto
Threat Advisor
Helsinki, Finland

WHERE: Global

WHAT: Thanks to AI, just about anyone can now act like a professional ‘geoguessr’ with zero skill—using location clues in photos to identify where an image was taken. All it takes is a single photo containing basic outdoor details, and AI can infer remarkably accurate location data. In the hands of a bad actor, this makes online stalking easier—and more precise—than ever before.

KEY FACTS:

- Large language models (LLMs) are not just good at describing what's in an image—they can also infer where it was taken. This can include altitude (e.g. floor level in a building), the time of day or year, and even directions on how to reach that location.
- In an urban stalking context, prompts can go even further: AI can suggest exactly where to stand to replicate a photo—down to the building, floor, cardinal or intercardinal direction, and even the camera height at which it was taken.
- What can be done to tackle this risk? Advocating for stricter AI guardrails is unlikely to be effective, as current AI systems can’t reliably distinguish between benign prompts (e.g. “I want to visit this place”) from malicious ones (e.g. “Where was this taken?” for stalking purposes). AI simply can’t interpret user intent.

Trending Scam

Scammers Spoof Google in Sophisticated Phishing Attack

WHERE: Global

WHAT'S HAPPENING:

- Phishing emails spoofing no-reply@google.com are passing DomainKeys Identified Mail (DKIM) authentication and claim a subpoena has been served to Google LLC.
- They allege that law enforcement "seeks retrieval of information contained in your Google Account," and includes a link to a fake Google Support Case.
- These messages mimic real Google alerts, and the phishing site closely resembles the genuine portal. The giveaway: real alerts use accounts.google.com, but this scam uses sites.google.com, Google's free website builder.

WHAT TO DO:

- This is a particularly sophisticated phishing scam, as the attackers spoofed Google's real email address (no-reply@accounts.google.com), making it appear immediately trustworthy. But even when an email looks authentic, users should remain cautious.
- It's always good practice to scrutinize unexpected messages—especially those that create a sense of urgency or request sensitive information. If something feels off, don't click any links.

Breach That Matters

Study Reveals 94% of Leaked Passwords Aren't Unique

WHERE: Global

WHAT'S HAPPENING:

- A new analysis of over 19 billion recently leaked passwords reveals troubling patterns in user behavior. Only 6% of passwords were unique, leaving the remaining 94% highly vulnerable to cross-account attacks.
- The study also found that most users rely on passwords between 8–10 characters, with 27% consisting only of lowercase letters and digits. Weak passwords like '123456', 'password', and 'admin' remain widely used—even in 2025.
- Despite decades of education around password security, user behavior remains unchanged—reinforcing the urgent need for more secure authentication methods.

WHAT TO DO:

- Multi-factor authentication (MFA) remains a critical line of defense. That's why it's essential for businesses to enable 2FA or MFA—ideally through biometrics or authenticator apps—across their digital services and customer-facing apps.
- While MFA significantly strengthens account security, consumers must also adopt better password habits—such as using a password manager to generate and store strong, unique credentials.

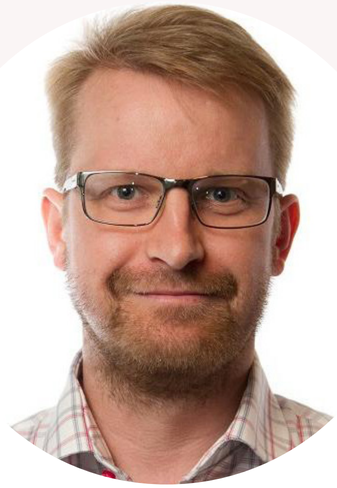
Investment Scams Are Lucrative—And Growing Fast

WHERE: Europe & North America

WHAT: Two scam centers behind investment fraud campaigns have been uncovered by security researchers. Nicknamed ‘Reckless Rabbit’ and ‘Ruthless Rabbit’, the groups use spoofed celebrity endorsements to promote the scams on social media and hide their operations behind traffic distribution systems.

KEY FACTS:

- Reckless Rabbit uses fake Facebook ads with fabricated celebrity endorsements. When users ‘register’ on a fake site, a web form captures their personal details. The group verifies this data and filters traffic by region. High-value victims are then sent to a scam investment platform or a page telling them to expect a call from an agent.
- Ruthless Rabbit runs a cloaking service to perform validation checks—making its infrastructure more resilient and harder to detect. Users who pass these checks are directed to a fake investment platform and prompted to enter financial details.
- Scam centers in Israel and Georgia have used similar tactics to defraud over 32,000 victims out of $275 million. One exposé reveals how they treat scamming like an office job—running Facebook ads, hiring staff, and celebrating tricked victims as if they were new clients.



EXPERT INSIGHT:

“The same tools and techniques used by everyday people are also exploited by scam centers. Like legitimate businesses, they have teams dedicated to attracting victims and keeping them engaged—with sales targets for different markets. Investment scams are lucrative, and these groups are relentless. Consumers should remain cautious online, especially when faced with offers that seem too good to be true—particularly those promoted on social media.”

Timo Salmi
Senior Solution Marketing Manager
Oulu, Finland

EXPERT INSIGHT:

“While this marks the first major victory against illegal spyware threatening the safety and privacy of all WhatsApp users, it also signals a potential shift in the tactics available to combat large-scale scam operations. Scam centers that operate under similar veils of plausible deniability and cross-border protection may eventually face similar consequences. This puts those currently acting with impunity officially on notice.”

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, US

WhatsApp Spyware Case Sets Cyber Law Precedent

WHERE: United States & Global

WHAT: Messaging platform WhatsApp has won a pivotal lawsuit against Israel-based spyware maker NSO Group, following its detection and interception of a spyware attack six years ago. The verdict—and its $168 million damages award—sends a strong message to the cyber crime ecosystem: violating cyber security laws carries serious consequences.

KEY FACTS:

- A US federal court found that NSO Group’s Pegasus software exploited vulnerabilities to spy on the mobile devices of 1,400 individuals—including government officials, human rights activists, and journalists.
- NSO Group claimed its clients were legitimate governments using the software to combat drug trafficking and terrorism. However, the verdict confirms that the company is ultimately responsible for its illegal hacking activities—and that inferred or explicit government approval is not a legal shield.
- This case demonstrates that technology companies can successfully pursue legal action against entities that abuse their platforms to harm users, regardless of claims about government affiliations or jurisdictional complexity.

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