February 2025

F-Alert

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

F-Secure.

Meta Cuts Fact Checkers: What's the Impact on Scams?

WHERE: Menlo Park, CA

WHAT: Meta has announced plans to remove third-party 'fact checkers'—a small but influential group responsible for reviewing content accuracy—and replace them with Community Notes, a democratized system that allows users to collaboratively add context to misleading posts. The initiative will begin in the US over the next few months.

KEY FACTS:

- While its original intent was pure, the fact-checking system became highly susceptible to individual biases. It gradually shifted from removing policy-violating content to serving as a political tool, as evidenced by the White House repeatedly pressuring Meta to censor content.
- Community Notes is a collaborative effort where no one is exempt—not heads of state, billionaires, or media organizations. If implemented like on X, users from diverse groups will vote on notes for misleading posts, with the most popular one displayed alongside the post. This reduces the risk of rigged voting.
- Community Notes doesn't replace content policies or terms of service but adds another layer of defense against unwanted content. Social media platforms will still rely on software-driven measures to detect and prevent scams and cyber crime.

EXPERT INSIGHT:

"Half the world uses Meta apps regularly, yet only a fraction of content, especially in smaller markets, has been reviewed by fact checkers. Community Notes expands capacity to flag posts linked to scams, such as crypto schemes, and serves as an apolitical tool to combat misinformation. However, outright illegal content or material causing potential harm may bypass automatic measures like software or AI-based filtering, so reporting such posts immediately is crucial."

Joel Latto
Threat Advisor
Helsinki, Finland

Get-Rich-Quick Scams Will Surge Amid Crypto Boom

WHERE: All States

WHAT: Bitcoin’s price surged by over 100% in 2024, reigniting interest in cryptocurrency following its four-year decline. With crypto's popularity expected to grow throughout 2025, we can anticipate a rise in ‘get-rich-quick’ schemes promoted by internet personalities. One such scheme has already emerged from online meme star ‘Hawk Tuah Girl’.

KEY FACTS:

- Bitcoin’s four-year halving cycle—which reduces the rate of new coin creation—has driven its rebound in 2025. Yet since its inception in 2009, this cycle has followed predictable patterns, giving alternative coins (altcoins) a chance to gain ground.
- Celebrity involvement in crypto is also nothing new. From tech entrepreneurs to actors and athletes, the allure of cryptocurrency spans industries. Some back established coins like Bitcoin and Ethereum, while others create their own altcoins.
- One example is Haliey Welch, known as ‘Hawk Tuah Girl’. Her digital coin, ‘Hawk’, reached a $490m market cap—only to lose 95% of its value within hours. Critics accuse Welch of a pump-and-dump scheme, inflating its value before selling for profit, while others allege a ‘rug pull’, where trading was halted, leaving investors with worthless assets.

EXPERT INSIGHT:

“As cryptocurrencies gain popularity, they often attract endorsements from influencers. Unfortunately, some of these promotions are linked to deceptive schemes, where trusting followers end up bearing significant losses. For people considering crypto investments: research them thoroughly. Be cautious of newly created coins that rely on hype and lack substantial backing. Avoid rushing into decisions; take time to evaluate the risks of any investment opportunity.”

Sarogini Muniyandi
Senior Manager, Scam Protection Engineering
Helsinki, Finland

Trending Scam

Criminals Trick iMessage Users to Enable Phishing Links

WHERE: All States

WHAT'S HAPPENING:

- Criminals have found a way to bypass the phishing protection built into Apple's iMessage platform.
- iMessage automatically disables links in messages from unknown senders. However, criminals found that if a user replies to their message or adds them as a contact, the links are enabled. They exploit this by tricking recipients into replying.
- Recent smishing scams include a fake USPS shipping issue or an unpaid road toll asking recipients to reply 'Y' to activate a link—mimicking legitimate confirmation requests for appointments or other legitimate actions.

WHAT TO DO:

- Avoid replying to messages from unknown senders. Even without clicking the link, replying shows bad actors you're a responsive target, increasing your risk.
- Instead, verify the message by contacting the sender directly through official channels. Using online security with SMS scam protection can also help block malicious text messages.

Breach That Matters

Hackers Target Students & Teachers in School Breaches

WHERE: NC & OR

WHAT'S HAPPENING:

- Schools across the US are increasingly becoming targets for data breaches due to the vast amount of sensitive information they hold and their generally limited cyber security resources.
- In Oregon, multiple school districts were impacted by a breach at Carruth Compliance Consulting, confirmed after detecting suspicious activity. Tens of thousands of current and former school employees may have had their data compromised.
- In North Carolina, the Wake County Public School System disclosed a breach involving the PowerSchool Student Information System after credentials were compromised, exposing the data of current and former students and employees.

WHAT TO DO:

- If you suspect your personal data may have been part of a breach, regularly monitor your financial accounts for unusual activity.
- Consider using a credit monitoring and identity restoration service, which can alert you to fraud and help reclaim your identity. Companies involved in breaches often offer these services for free.

Carding Scams Are Thriving on the Clear Web

WHERE: All States

WHAT: Carding has long been a prevalent cyber crime, facilitated by dedicated online forums and marketplaces. However, these platforms are evolving—now requiring prepayments to preview stolen credit card data, complicating investigation efforts. Fortunately, protections are continually being developed to counter this threat.

KEY FACTS:

- Carding is a term used by security professionals, law enforcement, and criminals when referring to activities involving stolen credit cards, cryptocurrency, and other financial data. It encompasses more than selling card details; it includes sharing tips on keeping stolen cards active, covering tracks, and more.
- There are websites, channels, and forums dedicated to carding. Unlike other types of stolen data, stolen cards are usually sold on niche platforms. And contrary to popular belief, these sites operate on the clear web rather than the dark web, meaning that the internet we all use has become much 'safer' for criminals to use.
- In recent years, there has been a rise in cryptocurrency carding, focusing on how to leverage stolen crypto wallets, how to use stolen credit card details to buy cryptocurrency, etc.

EXPERT INSIGHT:

"Our financial details can leak in various ways, such as phishing attacks or compromised online services. Be cautious when shopping online and regularly check your bank account. Even with strong user authentication in place, it's still possible for it to be bypassed. I strongly suggest using F-Secure tools to stay safe from phishing attacks, monitor personal data for breaches, guard against online shopping scams, and more."

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

Telegram Cracks Down on Criminal User Base

EXPERT INSIGHT:

“Telegram's updated Privacy Policy states that if authorities issue an order confirming someone as a crime suspect, the platform will conduct a legal analysis of the request and may disclose their IP address and phone number. While this policy change has prompted many cyber crime groups to leave the platform, and multiple reports suggest a reduction in criminal activity on Telegram, only time will tell whether this decline is truly substantial.”

Amit Tambe
Researcher
Helsinki, Finland

WHERE: All States

WHAT: In 2024, Telegram disclosed the IP addresses or phone numbers of 2,253 users to US law enforcement, complying with 900 requests. Notably, between January and September, Telegram fulfilled only 14 requests (affecting 108 users) specifically in cases of terrorism. This demonstrates a significant shift in their level of cooperation in recent months.

KEY FACTS:

- Telegram is an online community and instant messaging platform known to be used by criminals to sell illicit goods or services and coordinate cyber attacks.
- Telegram’s 2024 Transparency Report shows a significant increase in law enforcement requests fulfilled globally in recent months, following a policy change on sharing user data announced in September. The United States has the third-highest number of requests fulfilled, after India and Germany.
- This policy shift, implemented after the arrest of CEO Pavel Durov in August, signifies that Telegram will now cooperate with authorities by sharing user data in crime investigations, such as cases of online fraud and the sale of illegal goods.

New Program Targets Smart Device Security Standards

WHERE: Washington, DC

WHAT: The White House is launching a new program to simplify the identification of secure smart products, educate consumers on device security, and encourage manufacturers to create safer devices. Set to debut later this year, the US Cyber Trust Mark will appear on Internet of Things (IoT) devices sold in the US that meet specific cyber security standards.

KEY FACTS:

- The US Cyber Trust Mark will appear on smart devices like dishwashers, TVs, baby monitors, and fitness trackers, indicating that they meet National Institute of Standards and Technology (NIST) security criteria, including regular software updates, incident detection, data protection, and strong default passwords.
- This program builds on the success of the Energy Star label, introduced in 1992 to help consumers reduce energy consumption. It has since become a vital tool for educating consumers on energy efficiency and motivating companies to create energy-saving appliances.
- In addition to efforts in the US, other initiatives are underway globally. Last year, the UK passed a law requiring smart device manufacturers to meet basic cyber security standards, including specifying the minimum duration of security updates.

EXPERT INSIGHT:

“This year, smart device manufacturers can submit products for testing to earn the US Cyber Trust Mark, which will be highlighted by retailers like Amazon and Best Buy. While voluntary, the program aims to become an emblem consumers seek when purchasing IoT devices, encouraging manufacturers to improve security. It’s hoped this will mirror the impact of Energy Star ratings; however, whether stronger legislation will be needed remains to be seen.”

Tom Gaffney
Director of Business Development
London, UK

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