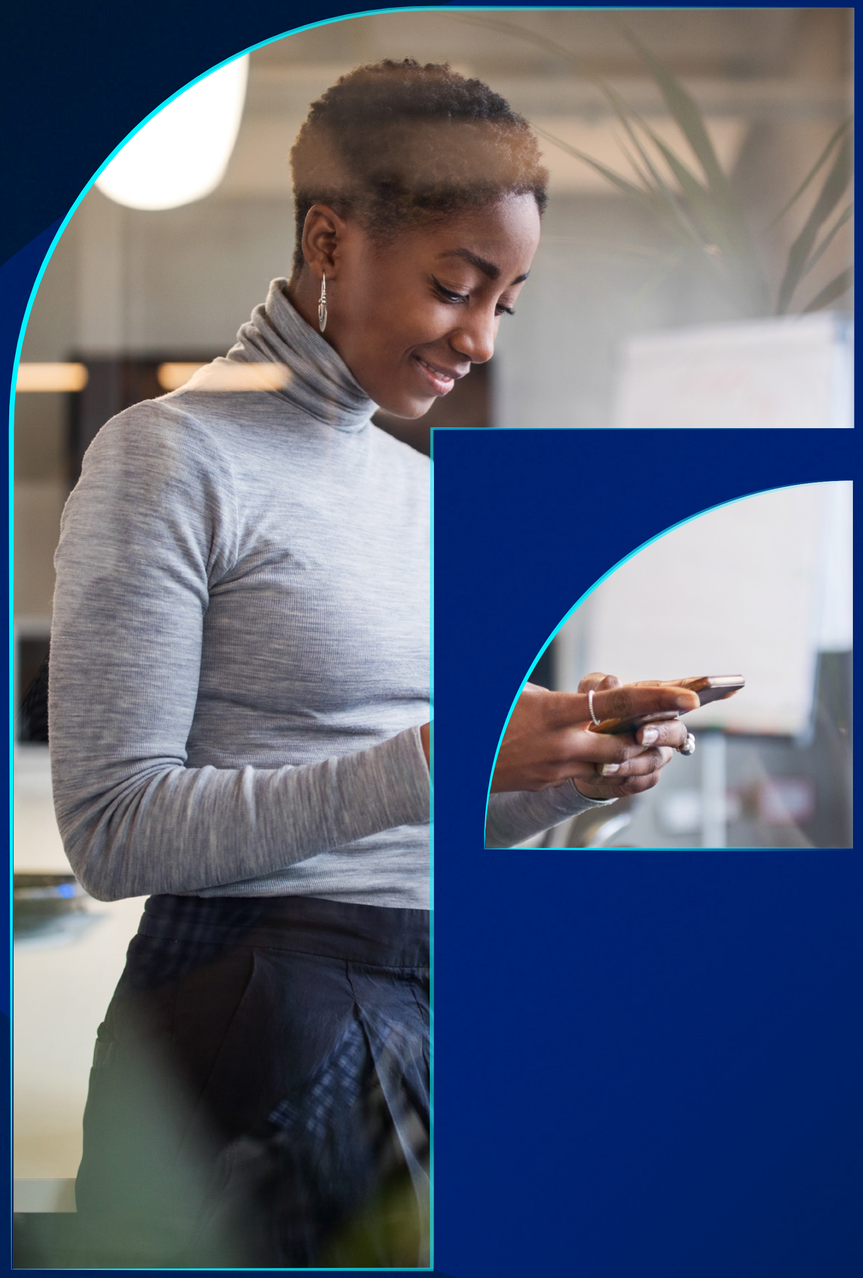
January 2025

F-Alert

Predictions for 2025 US cyber threats from
F-Secure threat intelligence experts



F-Secure

2025 PREDICTION

Everyday AI Tools Will Become Instrumental in Cyber Attacks

EXPERT INSIGHT:

“While AI companies do impose restrictions on malicious use, they’re often not very successful in enforcing them. More must be done to prevent their platforms from being used for nefarious purposes – it can’t be left solely to legislation to define the boundaries of what content can be generated. AI companies must do better.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

WHERE: All US States

WHAT: The use of AI tools for malicious purposes has become increasingly evident over the past year. In 2025, we can expect more sophisticated attacks leveraging everyday AI tools like ChatGPT, ElevenLabs, or others that are affordable and easily accessible online.

KEY FACTS:

- AI tools are becoming progressively more widespread and accessible – anyone can harness their power with just a few clicks from the homepage.
- However, the real threat isn’t public access to AI – it’s cyber criminals exploiting this readily available technology to enhance their scams.
- The bottom line is that the companies developing these tools should be held to a higher moral standard in preventing their misuse by criminals.

2025 PREDICTION

Companies Will Be Penalized for Failing to Prevent Scams

WHERE: DC & All US States

WHAT: Lawmakers worldwide are pressuring telecom operators, banks, and social media companies to take responsibility when customers fall victim to fraud. New bills are being passed in Australia and the UK, with the US expected to follow suit in 2025 and beyond.

KEY FACTS:

- In Australia, a new bill will fine companies up to $50 million for failing to protect customers from scams, while in the UK, banks must now reimburse victims in most cases.
- In July, the US Senate investigated Zelle, a money transfer app partnered with major US banks, for allegedly failing to protect account holders from fraud.
- As a result, it's expected that the US may soon take similar action to the UK and Australia.
- Passing new laws to empower businesses to strengthen scam protections is a welcome step. Fighting scams requires a collaborative effort involving governments, organizations, and individuals alike.

EXPERT INSIGHT:

"Just as GDPR in Europe pushed companies to take privacy more seriously, new legislation could add an extra layer of protection for consumers. However, there's no foolproof way to prevent scams entirely. Consumers must take daily precautions, especially on scam-prone platforms like social media and messaging apps."

Calvin Gan
Senior Manager, Scam Protection Strategy
Kuala Lumpur, Malaysia

2025 PREDICTION

Scammers Will Exploit Rising DeFi Investments

EXPERT INSIGHT:

“The manipulation of DeFi smart contracts poses risks to investor funds. Some platforms entice users with unsustainable high-yield rates, only for investors to find they can’t withdraw their Bitcoin or that the platform has vanished along with their funds. While DeFi offers financial freedom and profit potential, its unregulated, anonymous nature makes it ripe for scams – something Bitcoin investors must watch for in 2025.”

Sarogini Muniyandi
Senior Manager, Scam Protection Engineering
Helsinki, Finland

WHERE: All US States

WHAT: In 2025, Decentralized Finance (DeFi) is expected to attract even more users seeking alternatives to traditional finance. However, as it becomes more mainstream, scammers are likely to exploit individuals interested in Bitcoin and other digital assets, particularly those unfamiliar with the risks of blockchain-based finance.

KEY FACTS:

- DeFi is an emerging blockchain-based financial service that gained significant traction in 2024. It refers to financial services operated by algorithms on a blockchain, without the need for traditional financial institutions.
- The DeFi market offers loans, interest-bearing accounts, and high-yield investments with promises of substantial returns. As DeFi's popularity grows, the increasing total value locked in these projects makes them prime targets for large-scale fraud.
- DeFi platforms run on decentralized blockchain networks, allowing participation without identification or regulatory oversight. While this fosters accessibility, it also enables scammers to steal funds and vanish, exploiting the platforms’ anonymity.

Trending Scam

Winter Months Spark Rise in Bill and Invoice Scams

WHERE: MN & All US States

WHAT'S HAPPENING:

- The winter months often see a rise in scammers exploiting consumers' desire to save on their energy bills, and this year is no different.
- With energy costs increasing across most states, scammers often target vulnerable individuals by offering fake winter heating allowances through phishing messages.
- However, energy bills aren't the only avenue scammers are using to defraud people. In Minnesota, PayPal invoice scams have resurfaced. One man reported receiving a fraudulent request for $399, supposedly owed for a tech purchase, along with a threat to suspend his account if he didn't call the number to pay.

WHAT TO DO:

- Energy bill and invoice scams are becoming increasingly sophisticated. No matter how genuine an email or SMS message appears, it's important to avoid reacting to pressure and take a moment to assess the situation.
- Whenever possible, consumers should log in directly to their energy provider's or financial institution's website or app to verify invoices and account details.

Breach That Matters

Senior Dating Website Breach Exposes 765,000 Users

WHERE: All US States

WHAT'S HAPPENING:

- Senior Data, a dating site for individuals over 40, recently experienced a data breach due to an exposed Firebase database.
- The personal information of 765,517 users was compromised, including email addresses, photos, genders, Facebook account links, dates of birth, and precise geographical locations.
- After acknowledging the breach in December, the owner of Senior Data shut down the site, along with another dating platform they operated, ladies.com, which had also been affected by a breach.

WHAT TO DO:

- Affected individuals should change any passwords shared with their Senior Dating account across other platforms or services. Additionally, enabling two-factor (2FA) or multi-factor authentication (MFA) provides an extra layer of security.
- Users are advised to monitor their accounts for suspicious activity and remain vigilant against scams targeting the exposed information.

2025 PREDICTION

Scammers Will Use AI to Simulate Phone Calls at Scale

WHERE: All US States

WHAT: Sophisticated AI chatbots allow scammers to mimic real human interactions at scale, with 24/7 conversations in multiple languages. Paired with deepfake audio, these call-based scams blur the line between human and machine interactions, making them far more dangerous than robocalls. By 2025, this threat is expected to rise exponentially.

KEY FACTS:

- Criminals have long used multi-stage social engineering schemes involving direct interaction. For example, a scammer might call a victim about a loan application, then transfer them to another posing as a bank worker to steal banking details.
- These scams work because victims believe they are speaking with genuine, helpful people, making them more susceptible under pressure. Until now, their scalability was limited by scammers' capacity to handle only a finite number of interactions.
- AI is overcoming these limitations, enabling faster and more scalable simulations of human phone calls in multiple languages.

EXPERT INSIGHT:

"Defenses must adapt to counter these evolving threats. Blocking call-forwarding malware, detecting suspicious numbers, and using advanced audio analysis to identify deepfakes are essential. Educating users about scam warning signs is equally important. Defensive strategies must keep pace with attackers, leveraging AI-driven solutions and collaboration between security experts, telecom providers, and regulators."

Joel Latto
Threat Advisor
Helsinki, Finland

2025 PREDICTION

Regulator-Retailer Privacy Battles Will Impact Children

EXPERT INSIGHT:

“We need to ensure a balance between protecting children’s rights without compromising their right to privacy, and their right to explore the digital world without judgment. Therefore, it’s crucial that governments and technology companies collaborate to provide the right tools, such as VPNs, ad-blockers and privacy aware browsers, while also helping parents and children understand and navigate the risks.”

Tom Gaffney
Director of Business Development
London, UK

WHERE: CA & All US States

WHAT: In 2025, social media giants and shopping magnates will adopt new business practices to bypass the growing influence of regulators. This will be especially evident in the domain of children, as many of the fines levied this year were related to the inappropriate collection of children's data.

KEY FACTS:

- Governments are starting to crack down on companies exploiting consumer data, particularly shopping platforms like Amazon and Temu, whose business models rely on profiling online behavior for targeted ads and revenue through data brokers.
- In 2024, the California Privacy Protection Agency proposed updates to the CCPA to better protect consumers’ personal data, while the EU issued penalties to Meta, TikTok, and X. In response, Meta is offering paid subscriptions that allow users to opt out of ad collection – a dangerous move that suggests user privacy is a luxury.
- This year, regulators across the world will push for stronger protections for children’s data. For example, the Australian government has announced plans to block teens' access to social media platforms. However, this is unlikely to succeed as kids will always find a workaround.

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