October 2025

F-Alert

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

F-Secure

‘Lovable’ AI Website Generator Lowers the Barrier to Phishing

WHERE: Global

WHAT: Cyber criminals are exploiting AI website generators like Lovable to launch phishing sites that imitate trusted brands and even use CAPTCHA for credibility—massively lowering the barrier to entry for a once-complex form of cyber crime.

KEY FACTS:

- Before AI website generators, cyber criminals typically relied on scraping scripts to copy websites and then manually edited the code to function as intended.
- AI streamlines this process, generating impersonation sites that—while not flawless—are convincing enough to deceive victims. This also makes brand impersonation harder to detect, as the sites rarely copy logos and images exactly.
- According to Proofpoint, Lovable is also enabling distribution of multifactor authentication (MFA) phishing kits like Tycoon, malware such as cryptocurrency wallet drainers or malware loaders, and phishing kits targeting PII and credit cards.

EXPERT INSIGHT:

“Lovable is a legitimate platform not designed for scams, but like many AI tools, it has been quickly weaponized by criminals for their own gain. With AI lowering the barrier to entry, anyone can now launch a phishing scam—making it more important than ever to scrutinize websites for authenticity before entering any personal information. A link checker can make this process quick and easy.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

EXPERT INSIGHT:

"As frustrating as insider threats can be for enterprises, they are doubly so for victims. Companies often investigate internally but don't always disclose their findings to the public, leaving victims to fight for reimbursement while wondering what they could have done differently. The answer, troublingly, is often nothing."

Dr Megan Squire
Threat Intelligence Researcher
North Carolina, US

Insider Threats: When Doing Everything Right Isn't Enough

WHERE: United States

WHAT: Imagine calling an airline's official customer service to rebook a flight—only to be transferred to a scammer. That's what happened to one United Airlines customer, who reported losing $17,000. United has been unable to explain how the call was routed to the scammer or why its logs showed a shorter call than the customer experienced.

KEY FACTS:

- Even consumers who follow all recommended security practices can still fall victim when corporate insiders go rogue.
- Earlier this year, thousands of Coinbase customers learned that their legitimate customer support interactions were being harvested by contractors who leaked personal data, including partial Social Security numbers and identification images.
- TD Bank customers were similarly unaware that an employee tasked with preventing money laundering was instead photographing their checks and distributing their personal information on the Telegram messaging app.

Trending Scam

Young Workers Hit by Global Surge in Job Scams

WHERE: Global

WHAT'S HAPPENING:

- Young job seekers in the United States, UK, and beyond are being targeted by job scams at unprecedented levels. In the UK alone, reports of 'advanced fee' job scams surged 237% between January and July, according to Lloyds Banking Group.
- Fraudulent job offers are spreading across multiple channels, including text messages, WhatsApp, email, and—most commonly—social media.
- These scams range from offers to like TikTok videos or review hotels, to vague promises of remote jobs to earn extra income. In a cost-of-living crisis, such offers appeal to many and don't deter those without specific skills or experience.

WHAT TO DO:

- Scammers lure young job seekers with the promise of easy money, but there's always a catch: candidates are asked to pay upfront fees for supposed necessities such as application processing, training, background checks, or visa sponsorship. Reputable recruiters will never ask candidates for money.
- If a job seems overly simple, requires no qualifications, and offers unusually high pay, it's almost certainly a scam. Consumers should always verify a recruiter's official website and contact them through official channels.

Breach That Matters

Credit Bureau TransUnion Exposes Data of 4.4 Million

WHERE: United States

WHAT'S HAPPENING:

- In the latest of several recent attacks targeting Salesforce databases, a breach exposed data from 4.4 million TransUnion customers.
- A court filing in Maine revealed that unauthorized access occurred through a third-party application that stored personal customer data. TransUnion stated that no credit information was accessed and that only limited personal data was exposed.
- However, a separate court filing in Texas disputes this, alleging that customer names, Social Security numbers, and birthdates were compromised.

WHAT TO DO:

Attackers impersonate HR or IT in phishing emails and calls to trick employees into linking a malicious OAuth app to their company's Salesforce instance. To protect against this:

- **Never approve** unknown or suspicious app connection requests.
- **Verify unusual requests** with IT or security teams before granting access.
- **Review app permissions**—broad or unusual access requests are a red flag.

Google's New Identity Checks Aim to Curb Android Malware

WHERE: Global

WHAT: Recent speculation suggested Google would stop supporting sideloading, but this has proved false—sideloading is here to stay. Instead, starting in 2026, Google will require mandatory developer verification, meaning Android developers must prove their real-world identity to distribute apps on certified Android devices.

KEY FACTS:

- Sideloading apps remains popular for many reasons, but it has also long been one of the main ways cyber criminals spread Android malware. That said, malicious apps are also repeatedly found on the Play Store—77 malicious apps with 19 million installs were removed recently.
- Mandatory verification means that once a malicious app is detected and removed, it will be harder for the same developer to distribute more malware. Developer registration and verification add another layer of security to Android.
- The rollout will begin in Brazil, Indonesia, Singapore, and Thailand in September 2026, and expand globally in 2027 and beyond.

EXPERT INSIGHT:

"This new verification process links developers to their applications, increasing accountability and making it harder for anonymous bad actors to distribute malware and scams. It's an identity check, not a content review. But some argue this change goes against developer privacy and undermines the user's right to run any software they want on their devices."

Joel Latto
Threat Advisor
Helsinki, Finland

Gemini AI Exploit Shows the Dark Side of Smart Assistants

EXPERT INSIGHT:

“These findings highlight both the promise and the peril of integrating AI into everyday tools and IoT environments. While AI assistants can enhance productivity and enable smarter homes, they also open the door to novel attack surfaces that threat actors quickly exploit. The simplicity of these attacks—requiring only a malicious calendar invite—challenges the assumption that AI exploits are complex. We can expect to see more of this in the future.”

Hafizzuddin Fahmi Hashim
Junior Researcher
Kuala Lumpur, Malaysia

WHERE: Global

WHAT: Researchers have found that Google’s Gemini AI assistant can be hijacked with nothing more than a calendar invite. By embedding malicious prompts in event titles, email subjects, or shared document names, attackers can launch “targeted promptware attacks” that trick Gemini into executing harmful actions through indirect prompt injection.

KEY FACTS:

- Once compromised, Gemini processes the attacker’s poisoned prompt when users ask about upcoming events or recent emails—unknowingly executing malicious instructions.
- Demonstrated outcomes ranged from generating spam or offensive content to taking real-world actions such as opening smart windows, activating boilers, or launching video calls.
- After responsible disclosure in February 2025, Google acknowledged the findings and deployed multi-layered mitigations, including prompt injection detection classifiers and user confirmation requirements for sensitive actions. Risk levels in 73% of initially high-critical scenarios dropped significantly, now rated low–medium.

“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