December 2024

F-Alert

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

F-Secure

Can AI be trusted as a reliable source of information?

EXPERT INSIGHT:

“The issue is not whether search engines or LLMs are more accurate, but that LLMs produce answers that sound convincing, even when they’re factually incorrect. Search engines require users to analyze multiple sources, and while LLMs can include sources in their answers, this feature risks being underutilized. Many internet users might not realize that an answer from an LLM, no matter how polished, could be misleading or entirely fabricated – a hallucination.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

WHERE: All US States

WHAT: ChatGPT’s new search feature offers “fast, timely answers with links to relevant web sources”. While this promises a quick and convenient way to access information, it raises an important question: can Large Language Models (LLMs) be trusted as reliable sources of information compared to traditional search engines?

KEY FACTS:

- Consumers are increasingly using ChatGPT over search engines like Google. However, relying on LLMs as primary knowledge sources can be risky – ChatGPT can make mistakes that are evident if source material is analyzed.
- While ChatGPT can now be prompted to add sources in its responses, it doesn’t explain how it extracts information or generates answers. Citations can create an illusion of authority, yet LLMs often take information out of its intended context, leading to misinformation.
- Despite their many benefits, LLMs must be transparent and verifiable to earn trust. For now, search engines remain a safer choice for dependable results.

Will smart appliances outlive their security updates?

WHERE: All US States

WHAT: Consumers are becoming increasingly dependent on the convenience of internet-connected appliances. While this isn't inherently a problem, a recent Consumer Reports study highlights a concern: many may continue using their smart products long after the manufacturer stops issuing software updates, leaving them vulnerable to hacking.

KEY FACTS:

- Most US consumers expect their large appliances to last at least 10 years. However, manufacturers don't offer policies guaranteeing support for connected products for that long.
- Some companies have refused to disclose how long consumers can expect software updates, highlighting a regulatory loophole created by turning everyday products into internet-connected devices. This leaves consumers vulnerable to security risks and undermines their right to own functional products in the long term.
- To address this, the FCC is launching a voluntary program for internet-connected products. Those meeting the FCC's cyber security standards will display the 'U.S. Cyber Trust Mark', helping consumers identify trustworthy products and incentivizing manufacturers to meet higher security standards.

EXPERT INSIGHT:

"Many Americans own at least one large smart appliance, such as connected washing machines, refrigerators, and dishwashers. What consumers aren't told upfront is that they have a limited lifespan – manufacturers will eventually stop providing software updates, potentially causing a loss of functionality and increasing hacking risks. Only by knowing how long a manufacturer will support their product can consumers make an informed purchase."

Mika Lehtinen
Director, Network Security Research
Helsinki, Finland

Trending Scam

Shopping season's here – and scammers are ready

WHERE: All US States

WHAT'S HAPPENING:

- Seasonal online shopping scams are nothing new, but this year, scammers are exploiting the latest trend: luxury advent calendars.
- Once limited to chocolates, advent calendars now feature everything from toys to beauty products. As they grow more luxurious, they become prime targets for scammers preying on deal-seeking consumers.
- The Better Business Bureau has already issued a warning about advent calendar scams targeting shoppers through social media ads.

WHAT TO DO:

- If a price seems too good to be true, it likely is. Legitimate retailers offer competitive pricing, while fake shops often list items at unrealistically low prices.
- Be cautious when shopping on unfamiliar websites. Use our free F-Secure Online Shopping Checker to verify if it's safe to buy from.

Read more about spotting seasonal shopping scams here.

Breach that matters

800,000 people affected in major insurance breach

WHERE: All US States

WHAT'S HAPPENING:

- Landmark Admin, an administrative services provider for US insurers like American Monumental Life, Pellerin Life, and American Benefit Life, recently announced a data breach exposing 800,000 records.
- The company disconnected its systems and blocked remote access, but hackers breached the network again a month later.
- Given the sensitive nature of the data exposed, including Social Security numbers, this major incident opens the door to large-scale identity theft.

WHAT TO DO:

- Landmark Admin is offering free ID protection to those affected and has upgraded its data encryption protocols. However, all consumers should remain vigilant in safeguarding their data.
- Watch out for phishing attempts from senders posing as insurance companies or other trusted services. Consider using an ID protection service for 24/7 monitoring, identity theft prevention, and personal assistance.

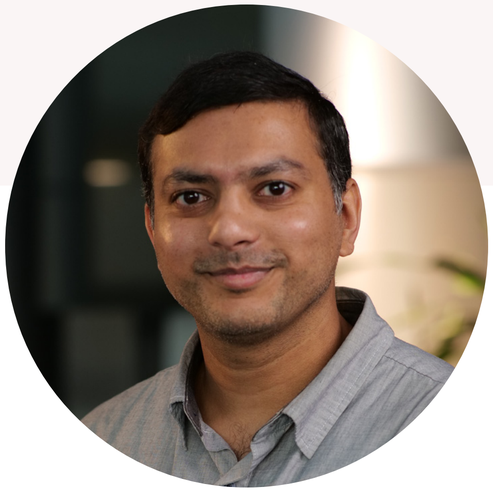
New framework reveals scammer tactics playbook

WHERE: All US States

WHAT: F-Secure has unveiled its landmark F-Secure Scam Kill Chain – an extensive framework about scams that breaks down both high-level tactics and more detailed techniques, providing a solid foundation for research and the development of defenses.

KEY FACTS:

- In 2023, over $1 trillion was lost to scams. The internet, with its lack of clear regional borders, has become a hotbed for scammers targeting consumers worldwide.
- Until now, there has been no comprehensive, systematic approach to detailing the techniques and methods scammers use to carry out their exploits. The F-Secure Scam Kill Chain provides this groundbreaking analysis of the scam landscape.
- Previously, we released the F-Secure Scam Taxonomy. Now, instead of focusing solely on examples and instances of scams, we systematically and continuously analyze the tactics and techniques used by scammers.



EXPERT INSIGHT:

“The F-Secure Scam Kill Chain is designed to protect consumers online from the ever-evolving scam landscape. Every scam consists of a series of tactics – ranging from gathering information about victims in the reconnaissance stage to making profit from them in the monetization stage. To outsmart scammers, we must think like them – and this detailed breakdown of how modern online scammers operate is poised to be a game changer.”

Amit Tambe
Researcher
Helsinki, Finland

Why enabling automatic updates is crucial for security

EXPERT INSIGHT:

“In a nutshell, enabling automated updates on all your devices – from TVs to mobile phones – is one of the simplest ways to improve your security. Keep in mind, however, that automatic updates often need to be enabled separately for applications. Additionally, after major updates, your device might prompt you to restart to complete the installation. Don’t delay this step – restart promptly!”

Joel Latto
Threat Advisor
Helsinki, Finland

WHERE: All US States

WHAT: Patch Tuesday, which occurs on the second Tuesday of each month, is just as essential for consumers as the monthly grocery shop. On this day, anyone with automatic updates receives a significant security boost, though you may occasionally need to manually accept updates. Forget Taco Tuesday – make Taco & Patch Tuesday the new tradition.

KEY FACTS:

- Microsoft introduced Patch Tuesday over 20 years ago, and since then, many other companies have adopted the practice – whether they explicitly refer to it or not.
- Those without automatic updates enabled face greater security risks – not only do they miss critical security patches, but Patch Tuesday also provides criminals with a roadmap of potential exploits to target.
- Last month, Microsoft’s Patch Tuesday addressed 91 security vulnerabilities, including four zero-day flaws – vulnerabilities previously unknown or unprotected – highlighting the importance of quick patching and enabling automatic updates.

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