November 2024

F-Alert

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

F-Secure

Funeral scams target bereaved Facebook users

EXPERT INSIGHT:

“Since the Covid-19 pandemic, more people are live streaming events like funerals to allow distant friends and family to attend. Typically, live streaming is included in events packages, with the organizer covering the cost – not the viewers. Always use the official link provided by the event organizer and be cautious of links from individuals claiming to represent a streaming service; look for signs of fake accounts.”

Laura Kankaala
Head of Threat Intelligence
Helsinki, Finland

WHERE: All US States

WHAT: Fake Facebook groups have recently targeted grieving users, offering video streaming services for funerals of the recently deceased. Those who click the links are asked to provide credit card information to pay a fee for access to the fake live stream.

KEY FACTS:

- Facebook users often create groups or fake profiles to share funeral arrangements in memory of loved ones. Scammers exploit this by setting up fake groups with images of the deceased and accurate funeral details, inviting their Facebook friends to join.
- The pages lead Facebook users to video streaming sites that require a credit card payment for access. They may also solicit donations under the guise of honoring the deceased or raising money for charity and funeral costs. At first glance, these sites appear legitimate, but they are actually phishing sites imitating real services.
- Scammers have also targeted events like graduations, concerts, award ceremonies, weddings, and even rodeos. In Plympton, MA, scammers duplicated a Facebook group run by Plympton Police, misleading users into thinking they could stream the popular Plympton Night Out event.

Meta fined $101.56m for poor user password storage

WHERE: All US States

WHAT: A statutory inquiry into Meta by the Irish Data Protection Commission (DPC) has concluded with a $101.56 million fine for storing user passwords in plaintext. Meta claims this was a mistake and asserts that it took "immediate action" to rectify the error.

KEY FACTS:

- The investigation revealed that Meta violated four articles of the EU's General Data Protection Regulation (GDPR) by failing to record incidents of plaintext password storage, not implementing proper security measures, and not promptly notifying the DPC about the breach. The investigation affects Meta's global user base, including those in the US.
- User passwords must never be stored in plaintext due to the risks of unauthorized access. Instead, systems should store hashed passwords, transforming them into unique codes that are nearly impossible to reverse. If a hacker accesses a database, they will only find the hashed values instead of the actual passwords.
- This incident not only jeopardizes Meta accounts but also puts other online accounts at risk. For example, logging into other sites using Facebook exposes those accounts as well.

EXPERT INSIGHT:

“While we must trust companies to store our passwords safely, there are steps we can take to keep our accounts secure. Never reuse passwords across multiple services, and ensure each one is strong and unique. Better yet, use a password manager to generate and store strong passwords. F-Secure's password manager also alerts consumers if existing ones are weak or reused.”

Timo Salmi
Senior Solution Marketing Manager
Oulu, Finland

Trending Scam

Extortion scams use photos of victims' homes

WHERE: All US States

WHAT'S HAPPENING:

- Police in NY, DC, FL, AL, and WA have warned of a new extortion scam trend involving PDFs with photos of victims' homes.
- Scammers claim to have evidence of visits to porn sites or spying through spyware, then demand payment to destroy the supposed proof.
- It's suspected that scammers are using Google Maps to find photos of homes.

WHAT TO DO:

- It's best to ignore these emails. Scammers rely on panic tactics, such as including addresses in email subject lines and attaching home photos. They send mass emails using collected data, so it's unlikely to be personal.
- It's relatively easy to find personal information online, so while it may feel like a targeted attack, it's likely the unfortunate result of your data being sold.

Breach that matters

Temu denies breach of 87m customer records

WHERE: All US States

WHAT'S HAPPENING:

- A hacker posted alleged Temu customer data for sale on the BreachForums hacking forum, claiming to have 87 million records and offering small samples as 'proof'.
- The company found no matches in its database after cross-checking the data, thus denying a breach. The threat actor has since been banned from the forum for making false claims and trying to sell publicly accessible data.
- Temu, a rapidly expanding Chinese e-commerce platform, has over 100 million active users in the United States, which accounts for 26.39% of its website traffic. This growing popularity has made Temu a tempting target for criminal activity.

WHAT TO DO:

- Regardless of the validity of the breach claims, Temu users should stay vigilant in protecting their data. Change your password to a strong, unique one, and enable two-factor authentication for added security. Additionally, be cautious of phishing attempts.

Hurricanes Helene & Milton will incite recovery scams

WHERE: FL, GA, SC, NC, TN, VA

WHAT: The flooding and destruction caused by Hurricanes Helene and Milton has been devastating. To make matters worse, scammers will prey on both those trying to rebuild their lives and the kindness of unsuspecting individuals looking to help.

KEY FACTS:

- Historically, scammers have exploited the desperation people feel during and after disasters. We saw this with Hurricanes Irma and Harvey, the Covid-19 pandemic, the Hawaii wildfires, and we are likely to see it again following Hurricanes Helene and Milton.
- Whether it's wars, elections, concerts, or natural disasters, scammers ignore ethical guidelines and prey on the vulnerable to capitalize on whatever is making headlines.
- That's because people in urgent need of assistance are often more susceptible to social engineering, where scammers exploit emotions to bypass the skepticism we would typically apply to their messages.

EXPERT INSIGHT:

"I expect scammers to pose as government officials, NGOs, or insurance companies. They'll use the 'appeal to authority' tactic to gain trust and steal money or information. My advice is to trust, but verify – always ask for proper identification and, if possible, independently confirm their claims. For example, call the government agency or insurer directly and ask to be transferred to the person claiming to assist you."

Joel Latto
Threat Advisor
Helsinki, Finland

Website bug exposes connected Kia cars to hackers

EXPERT INSIGHT:

“While car theft is less common than phishing emails or fake shopping websites, a vulnerability like this makes it possible to unlock cars to steal their contents and access personal data, cameras, and more – posing serious privacy and safety risks. My advice is the same for all car owners: don’t leave valuables in your vehicle. Additionally, keep your system updated with the latest security patches and use a strong, unique password.”

Mika Lehtinen
Director, Network Security Research
Helsinki, Finland

WHERE: All US States

WHAT: A group of independent security researchers have uncovered a vulnerability in Kia's web portal, enabling them to track millions of vehicles, unlock doors, and even start engines remotely. The hack was as simple as exploiting a bug in the website.

KEY FACTS:

- The flaw let researchers transfer control of Kia’s connected features from the owner’s smartphone to their own devices. By scanning a license plate, they could access the car’s functions within seconds.
- Kia has since fixed the web portal vulnerability and is investigating the group's findings. However, this was not a unique occurrence; a similar hack allowing control of Kia's digital systems was found last year.
- Vehicle web security remains weak overall, with issues repeatedly emerging in connected cars. This goes beyond Kia, with vulnerabilities affecting multiple brands like Honda, Infiniti, Nissan, BMW, Mercedes-Benz, Hyundai, and Ferrari.

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