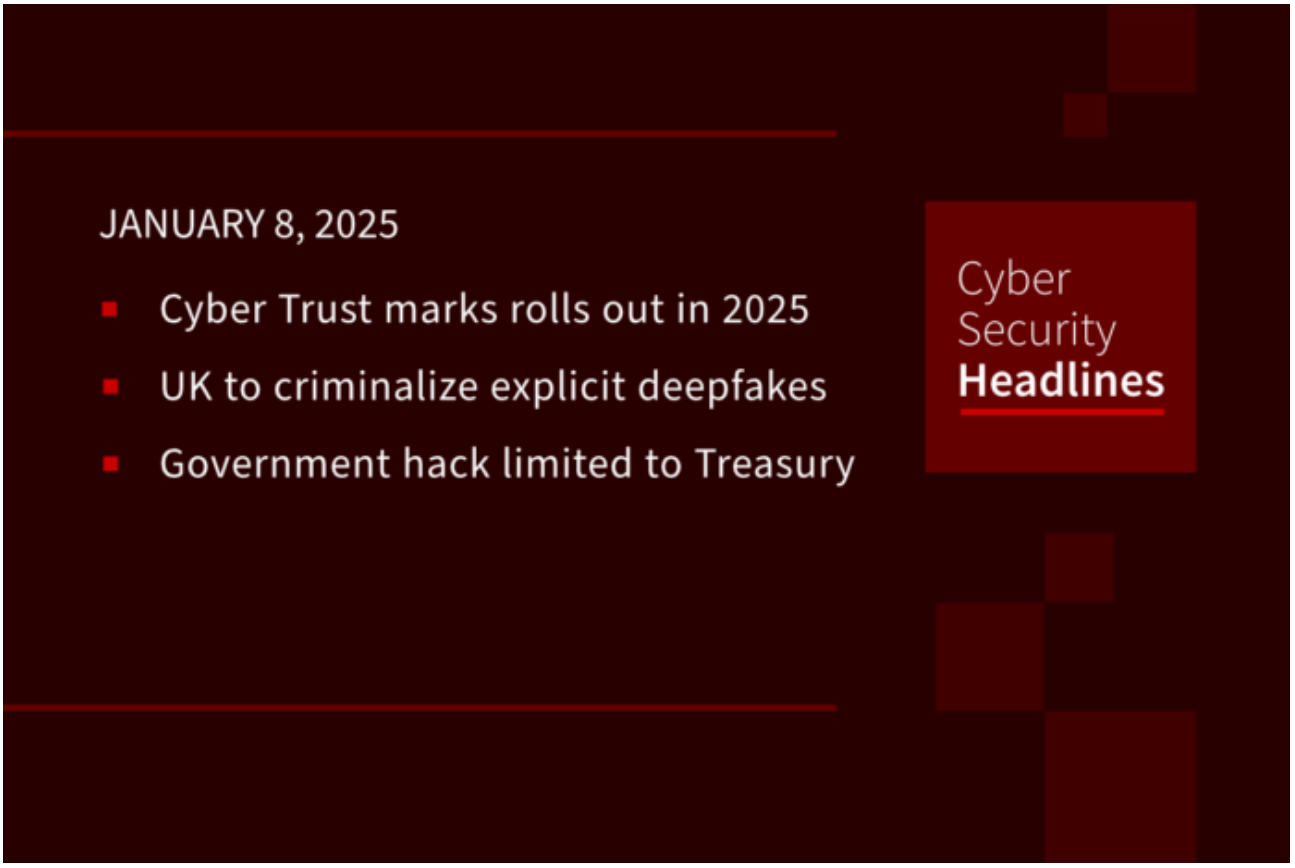
Cyber Security News: Cyber Trust label, UK deepfake laws, Treasury attack details

By Rich Stroffolino

Published: 2025-01-08 · Archived: 2026-05-01 02:06:31 UTC



Cyber Trust marks to roll out in 2025

In 2023, the White House launched an initiative to add Cyber Trust labels to retail packaging for connected devices. This was compared to the equivalent of Energy Star certification to indicate a consumer baseline of cybersecurity best practices. The FCC unanimously approved the label in March. Now, White House officials say the label will start appearing on consumer devices this year. Deputy National Security Adviser for Cyber Anne Neuberger said an upcoming executive order will mandate that the federal government only purchase devices with the Cyber Trust label as of 2027. The program will go off NIST cybersecurity criteria and inform users how long companies plan to provide software updates at the point of purchase. CISA, the FCC, and the Department of Justice will collaborate to oversee and enforce the program.

(The Record)

UK to criminalize sexually explicit deepfakes

The UK already criminalized the publishing of intimate media meant to cause distress without consent, aka revenge porn, back in 2015. But that only accounted for actual images, not machine-generated ones. The British government announced it will make creating and sharing explicit deepfake media that represents a real likeness a crime, punishable with up to two years in prison. The government also said it will increase scrutiny on tech platforms hosting these images. The Revenge Porn Helpline found that digitally altered revenge porn images have increased by over 400% since 2017.

(Reuters)

CISA says government hack limited to Treasury

Last week, the US Treasury Department informed lawmakers that state-sponsored Chinese threat actors breached its systems in a “major cybersecurity incident” through its remote support provider BeyondTrust.” After an investigation, CISA announced it found no signs of the breach impacting any other federal agencies. CISA said it will continue to monitor the response to the attack and coordinate with “relevant federal authorities” as needed. Investigators are still looking into the full scope of the Treasury attack but said there was no evidence the threat actors maintained access after the Treasury terminated its BeyondTrust instance.

(Bleeping Computer)

Philippines targeted by Chinese threat actors

Bloomberg’s sources say Chinese state-sponsored actors orchestrated a yearlong campaign to penetrate systems of the Philippines’ executive branch, stealing “sensitive” data. However, Department of Information and Communications Technology Secretary Ivan Uy said the attacks did not compromise current data but did obtain “old data from many years ago.” Uy said his department deals with thousands of breach attempts against the government daily and challenges the threat actors to publish details if they obtained relevant data.

(Bloomberg, PhilStar)

Huge thanks to our sponsor, Nudge Security

2,000 attacks launched against critical infrastructure

Temple University's Department of Criminal Justice maintains the Critical Infrastructure Ransomware Attacks database, or CIRA. Operating since 2013, the database now holds details on over 2,000 different attacks, with 45% added since February 2022. Government facilities, healthcare, public health, and education facilities were the most commonly targeted in the last two years. While attacks on water infrastructure got a lot of attention, they were among the least targeted. The database also shows ransom amounts increasing, with attacks requisitioning a $5 million or more ransom up 42% over the last two years. The entire dataset is available upon request from CIRA.

(Security Week)

Defense Department ties Tencent to the Chinese military

The US Defense Department formally added Tencent, the parent company of the massively popular Chinese messaging app WeChat, to a list of companies with ties to aiding and supplying the Chinese military, which could pose a security risk to the US. While this designation doesn't impose direct bans or sanctions, it does add considerable risk to Western companies doing business with it. Any sanctions would come from the Treasury. The Defense Department also added the firm CATL, the world's largest EV battery maker, to the list.

(Reuters)

Washington sues T-Mobile over data breach

Back in 2021, T-Mobile disclosed that a brute force attack on its corporate network resulted in a data leak impacting 79 million people across the US. It took T-Mobile six months to discover the malicious activity when data began appearing on hacking forums. Washington Attorney General Bob Ferguson filed a lawsuit against the telco, claiming it misrepresented its cybersecurity capabilities. The lawsuit also criticized T-Mobile for not telling customers that specifically had Social Security numbers stolen and for sending brief and incomplete text message alerts about the breach. The lawsuit seeks a court order for T-Mobile to strengthen its cybersecurity practices and financial penalties under the Consumer Protection Act.

(Bleeping Computer)

Aviation agency investigating breach claims

In a post of BreachForums 2, the account "Natohub" claimed it compromised 42,000 documents from the UN's International Civil Aviation Organization (ICAO), supposedly containing personal records of staff and others working with the agency. ICAO did not confirm it suffered a breach but said it was "actively investigating reports of a potential information security incident." The Natohub account doesn't have an extensive track record of leaks, but also made the unsubstantiated claim that it accessed personal data on thousands of UN delegates last month.

(The Record)

Green Bay Packers' online store sacked by threat actors

The American football team notified customers that a threat actor injected a card-skimming script into its official online store sometime between late September and early October 2024. The team learned of the skimmer on October 23rd from the Dutch e-commerce security company Sansec. It immediately disabled checkouts and payment systems while investigating the issue. The skimmer could only steal information of customers paying directly with a payment card. Customers using gift cards, PayPal, and Amazon Pay were not impacted. No word on how many customers the attack impacted, but the team will offer all victims three years of credit monitoring services.

(Bleeping Computer)
