Week of March 9, 2026

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

Cybercriminals impersonating city officials to steal permit payments, FBI says

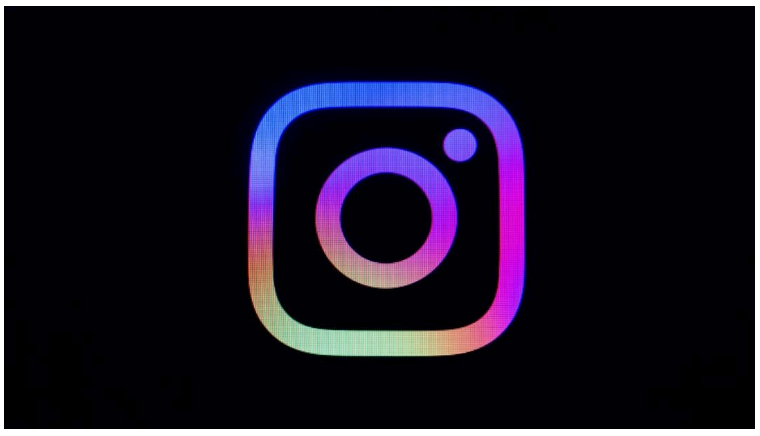
therecord.media

In a notice on Monday, the agency said people and businesses with active applications for the permits are being targeted with phishing emails that often include detailed, accurate information "including property addresses, case numbers, and the true ...

Meta says it culled millions of scam ads amid accusations that it profits from them

therecord.media

Meta said it removed 159 million scam ads last year amid calls from U.S. lawmakers for an investigation into the company's "facilitation of and profiting from" fraudulent advertising.



Iranian influence operation using fake personas to deceive US Instagram users disrupted, Meta says

therecord.media

Meta said it disrupted an influence operation linked to Iran that used "sophisticated fake personas" on Instagram to build relationships with U.S. users before introducing political messaging.

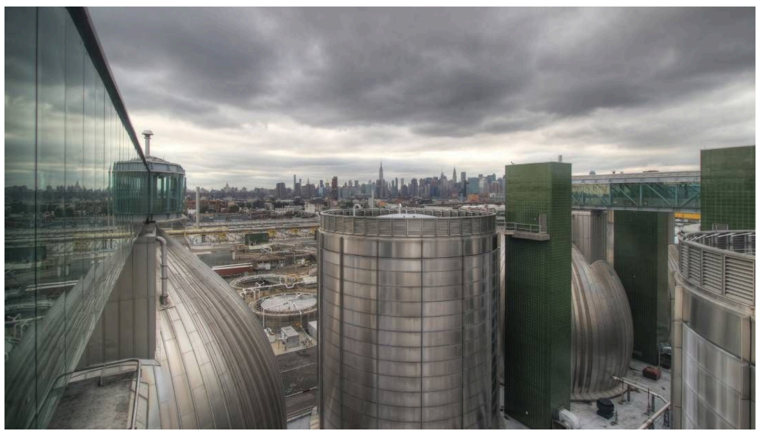
Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Exclusive: New data shows increase in FBI searches of Americans' data last year

therecord.media

The number of FBI searches of data collected through the surveillance program known as Section 702 of the Foreign Intelligence Surveillance Act (FISA) between December 2024 to November 2025 rose to 7,413 from 5,518 the previous year.



New York cyber regulations for water organizations to take effect in 2027

therecord.media

The new rules for water and wastewater entities in New York include mandatory cybersecurity training for certified operators, incident response plans and reporting requirements.

Federal Cyber Strategy Holds Few Details for State, Local Govt.

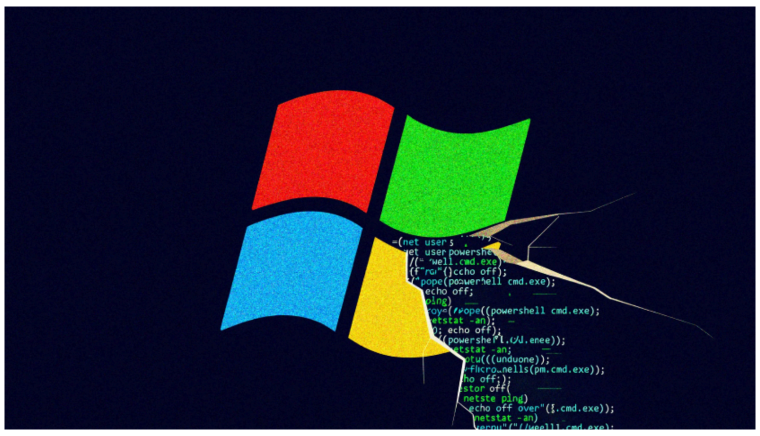
www.govtech.com

A new federal cyber strategy outlines six pillars for deterrence, infrastructure protection and regulatory reform, but offers few specifics about what support for state and local governments will ...

235,000 affected by cyberattack on largest ambulance provider in Wisconsin

therecord.media

The company said Social Security numbers, driver's license numbers, financial accounts, medical information and health insurance information was stolen during the cyberattack.



Microsoft Patches 84 Flaws in March Patch Tuesday, Including Two Public Zero-Days - The Hacker News

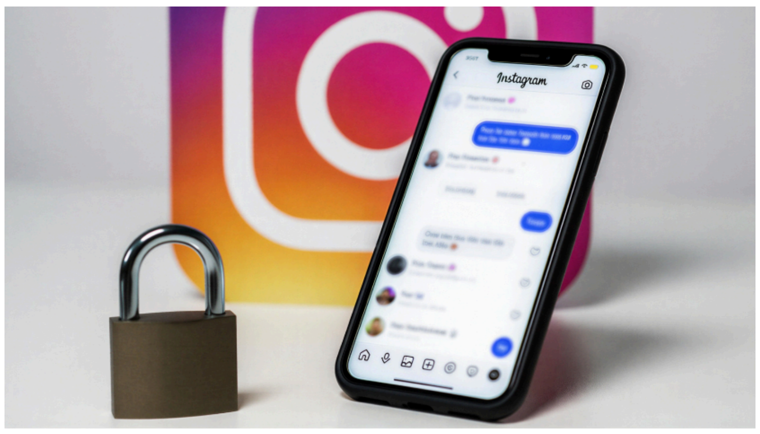
thehackernews.com

Microsoft patches 84 vulnerabilities, including two public zero-days, strengthening defenses against privilege escalation and cloud token theft.

Medical device giant Stryker confirms cyberattack as employees say devices were wiped

therecord.media

The medical device manufacturer Stryker confirmed reports Wednesday that a cyberattack has disrupted operations after a hacker group claimed to have targeted the company in retaliation for U.S. and Israeli strikes on Iran.



Meta to Shut Down Instagram End-to-End Encrypted Chat Support Starting May 2026 - The Hacker News

thehackernews.com

Meta will end Instagram E2EE chats May 8, 2026, reversing a 2021 privacy test and reigniting debate over encrypted messaging oversight.

Stryker tells SEC that timeline for recovery from cyberattack unknown

therecord.media

In an 8-K filing with the SEC, Stryker confirmed that the cyberattack caused a global disruption to the company's Microsoft environment and said external cybersecurity experts were brought in to "assess and to contain the threat."

How AI Assistants are Moving the Security Goalposts

krebsonsecurity.com

AI-based assistants or "agents" -- autonomous programs that have access to the user's computer, files, online services and can automate virtually any task -- are growing in popularity with ...

Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker

krebsonsecurity.com

A manifesto posted by the Iran-backed hacktivist group Handala, claiming a mass data-wiping attack against medical technology maker Stryker.

***Please be advised that** the following resources and materials are for informational purposes only. **The opinions and views expressed in these materials** are the opinions of the designated authors and do not reflect the opinions or views of **the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth).** The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.*

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record