



Week of May 5, 2025

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

Botnet Dismantled in International Operation, Russian and Kazakhstani Administrators Indicted

www.justice.gov

The Indictment alleges that a botnet was created by infecting older-model wireless internet routers worldwide, including in the United States, using malware without their owners’ knowledge. The installed malware allowed the routers to be reconfigured, granting unauthorized access to third parties and making the routers available for sale as proxy servers on the Anyproxy.net and 5socks.net websites

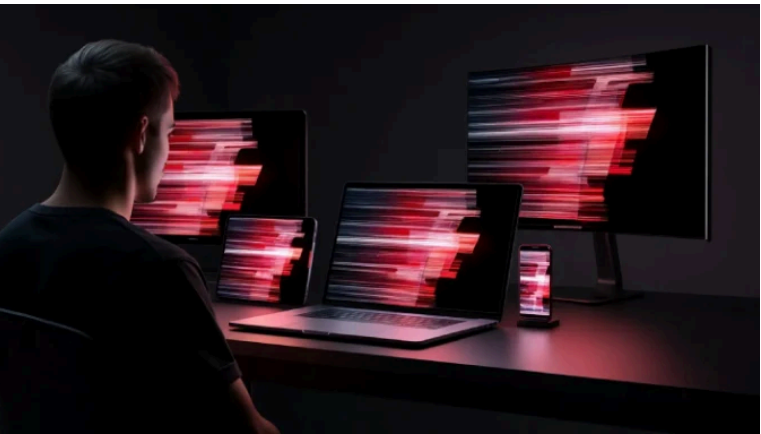
Cybercrimes, Scams & Incidents

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks

Pakistani Firm Shipped Fentanyl Analogs, Scams to US

krebsonsecurity.com

However, an investigation into the company’s founders reveals they are connected to a sprawling network of websites that have a history of extortionate scams involving trademark registration ...



Wormable AirPlay Flaws Enable Zero-Click RCE on Apple Devices via Public Wi-Fi - The Hacker News

thehackernews.com

Some of the other notable flaws are listed below - CVE-2025-24271 - An ACL vulnerability that can enable an attacker on the same network as a signed-in Mac to send AirPlay commands to it without pairing; CVE-2025-24137 - A vulnerability that could ca...



Education giant Pearson hit by cyberattack exposing customer data - BleepingComputer

www.bleepingcomputer.com

Education giant Pearson suffered a cyberattack, allowing threat actors to steal corporate data and customer information, BleepingComputer has learned.

Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech



Harrods latest retailer to be hit by cyber attack - BBC

www.bbc.com

The firm told the BBC it had restricted internet access in its stores following an attempted cyber attack.



Microsoft: April updates cause Windows Server auth issues

www.bleepingcomputer.com

Microsoft says the April 2025 security updates are causing authentication issues on some Windows Server 2025 domain controllers.





Kickidler employee monitoring software abused in ransomware attacks - BleepingComputer

www.bleepingcomputer.com

Ransomware operations are using legitimate Kickidler employee monitoring software for reconnaissance, tracking their victims' activity, and harvesting credentials after breaching their networks.



New Microsoft 365 outage impacts Teams and other services

www.bleepingcomputer.com

Microsoft is investigating a new Microsoft 365 outage affecting multiple services across North America, including the company's Teams collaboration platform.



CISA warns of hackers targeting critical oil infrastructure - BleepingComputer

www.bleepingcomputer.com

CISA warned critical infrastructure organizations of "unsophisticated" threat actors actively targeting the U.S. oil and natural gas sectors.



Doubling down: How Universal 2nd Factor (U2F) boosts online security - BleepingComputer

www.bleepingcomputer.com

Passwords alone aren't cutting it—31% of breaches involve stolen credentials. Learn from Specops Software about how Universal 2nd Factor (U2F) and strong password policies can work together to ...


Unexpected behavior in Snowflake's Cortex AI


www.cyera.com


In this post, we'll examine how Snowflake's CORTEX Search Service, a cutting-edge AI-driven search and retrieval tool, could end up exposing sensitive data within your Snowflake user base, even in a secure environment with tightly configured access and masking policies.


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.


Official Quick Links


-  CISA


 FBI


 CIS/MS-ISAC


 NIST


 CyberCom


 NSA


 DHS


 DOJ
- External Quick links


 AIScoop


 Cybersecurity Dive


 FedScoop


 Krebs on Security


 Schneier on Security


 BleepingComputer


 Cyware


 Government Executive


 MITRE ATT&CK®


 SC Media


 Cisco Talos Intelligence Group


 CyberWire


 Government Technology


 NASCIO


 StateScoop


 CSO Online

 ISACA

 The Hacker News

 CyberScoop

 ISSA International

 The Record