



Week of June 30, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents



Cyberattack on Russian independent media had links to US-sanctioned institute, researchers find
therecord.media

A Russian hosting provider allegedly involved in a recent cyberattack against independent media organizations in the country is reportedly connected to a state-affiliated research center sanctioned by the U.S.

Microsoft shuts down 3,000 email accounts created by North Korean IT workers

therecord.media

Microsoft said it suspended 3,000 Outlook and Hotmail email accounts it believed were created by North Korean IT workers as part of a larger effort to help companies address the costly scheme.



FBI: Cybercriminals steal health data posing as fraud investigators - BleepingComputer

www.bleepingcomputer.com

The Federal Bureau of Investigation (FBI) has warned Americans of cybercriminals impersonating health fraud investigators to steal their sensitive information.

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies



US defense firms must 'remain vigilant' against Iranian cyber activity, agencies warn
therecord.media

"At this time, we have not seen indications of a coordinated campaign of malicious cyber activity in the U.S. that can be attributed to Iran," an advisory from the Cybersecurity and Infrastructure Security Agency (CISA), FBI, National Security Agency and the Department of Defense Cyber Crime Center said.

California jury orders Google to pay \$314 million over data transfers from Android phones

therecord.media

A California jury has ordered Google to pay \$314 million for collecting data from Android phones while they were connected to cellular networks, a practice that plaintiffs said equated to stealing a resource that they had paid for.



Over 1,200 Citrix servers unpatched against critical auth bypass flaw

www.bleepingcomputer.com

Over 1,200 Citrix NetScaler ADC and NetScaler Gateway appliances exposed online are unpatched against a critical vulnerability believed to be actively exploited, allowing threat actors to bypass ...

Senator Chides FBI for Weak Advice on Mobile Security

krebsonsecurity.com

Agents with the Federal Bureau of Investigation (FBI) briefed Capitol Hill staff recently on hardening the security of their mobile devices, after a contacts list stolen from the personal phone of the White House Chief of Staff Susie Wiles was reportedly used to fuel a series of text messages and phone calls impersonating her to U.S. lawmakers...



AT&T rolls out "Wireless Lock" feature to block SIM swap attacks

www.bleepingcomputer.com

AT&T has launched a new security feature called "Wireless Lock" that protects customers from SIM swapping attacks by preventing changes to their account information and the porting of phone ...



















Big Tech’s Mixed Response to U.S. Treasury Sanctions

krebsonsecurity.com

In May 2025, the U.S. government sanctioned a Chinese national for operating a cloud provider linked to the majority of virtual currency investment scam websites reported to the FBI. But a new report finds the accused continues to operate a slew of established accounts at American tech companies — including Facebook, Github, PayPal and Twitter/X.

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 | | | |