



Week of February 24, 2025

## Cybersecurity Headlines

### Official Security Bulletins

Headlines from List of Official Government Sources

#### Vulnerability Summary for the Week of February 24, 2025

[www.cisa.gov](https://www.cisa.gov)

The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded in the past week. In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores.



#### District of New Jersey | Thirteen Individuals Charged As Part Of International Ring Targeting Cell Phone Shipments For Theft - United States Department of Justice

[www.justice.gov](https://www.justice.gov)

NEWARK, N.J. – Thirteen members of an international network that stole thousands of shipments of iPhones and other electronic devices around the United States were charged today, Acting U.S. Attorney Vikas Khanna, District of New Jersey, announced.

### Cybercrimes, Scams & Incidents

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

#### U.S. Soldier Charged in AT&T Hack Searched “Can Hacking Be Treason”

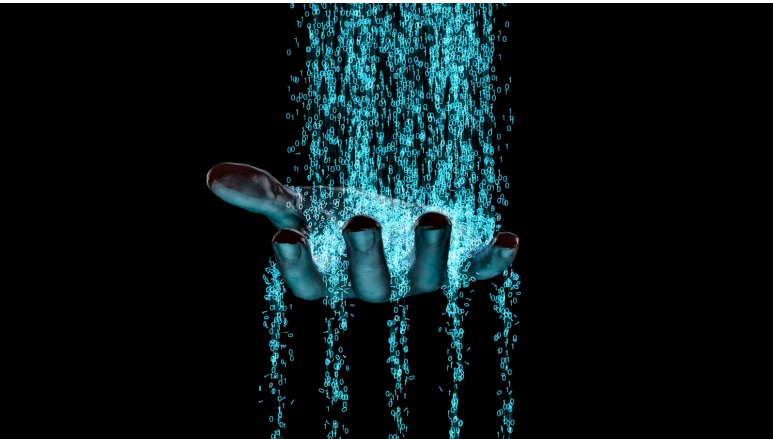
[krebsonsecurity.com](https://krebsonsecurity.com)

A U.S. Army soldier who pleaded guilty last week to leaking phone records for high-ranking U.S. government officials searched online for non-extradition countries and for an answer to the question “can hacking be treason?” prosecutors in the case said Wednesday. The government disclosed the details in a court motion to keep the defendant in custody until he is discharged from the military.

#### Notorious Malware, Spam Host “Prospero” Moves to Kaspersky Lab

[krebsonsecurity.com](https://krebsonsecurity.com)

One of the most notorious providers of abuse-friendly “bulletproof” web hosting for cybercriminals has started routing its operations through networks run by the Russian antivirus and security firm Kaspersky Lab, KrebsOnSecurity has learned...



#### US drug testing firm DISA says data breach impacts 3.3 million people - BleepingComputer

[www.bleepingcomputer.com](https://www.bleepingcomputer.com)

DISA Global Solutions, a leading US background screening and drug and alcohol testing firm, has suffered a data breach impacting 3.3 million people.

### Industry News

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



#### Australia bans all Kaspersky products on government systems

[www.bleepingcomputer.com](https://www.bleepingcomputer.com)

The Australian government has banned all Kaspersky Lab products and web services from its systems and devices following an analysis that claims the company poses a significant security risk to the ...



#### Microsoft fixes Entra ID authentication issue caused by DNS change - BleepingComputer

[www.bleepingcomputer.com](https://www.bleepingcomputer.com)

Microsoft has fixed an issue that caused Entra ID DNS authentication failures when using the company's Seamless SSO and Microsoft Entra Connect Sync.



## Cybersecurity Tips

Helpful information for you to become more secure in your day to day



### Three Password Cracking Techniques and How to Defend Against Them - The Hacker News

thehackernews.com

Passwords are rarely appreciated until a security breach occurs; suffice to say, the importance of a strong password becomes clear only when faced with the consequences of a weak one. However, most end users are unaware of just how vulnerable their p...



### CISA Adds Microsoft and Zimbra Flaws to KEV Catalog Amid Active Exploitation - The Hacker News

thehackernews.com

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday placed two security flaws impacting Microsoft Partner Center and Synacor Zimbra Collaboration Suite (ZCS) to its Known Exploited Vulnerabilities catalog, based on evidence of...

*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

- |  |   |  |   |   |
|--|---|--|---|---|
|  <a href="#">CISA</a> |  <a href="#">CIS/MS-ISAC</a> |  <a href="#">CyberCom</a> |  <a href="#">DHS</a> |  <a href="#">DOJ</a> |
|  <a href="#">FBI</a>  |  <a href="#">NIST</a>        |  <a href="#">NSA</a>      |   |   |

#### External Quick links

- |  |  |  |   |  |
|--|--|--|---|--|
|  <a href="#">AIScoop</a>              |  <a href="#">BleepingComputer</a>     |  <a href="#">Cisco Talos Intelligence Group</a> |  <a href="#">CSO Online</a>      |  <a href="#">CyberScoop</a>         |
|  <a href="#">Cybersecurity Dive</a>   |  <a href="#">Cyware</a>               |  <a href="#">CyberWire</a>                      |   |  |
|  <a href="#">FedScoop</a>             |  <a href="#">Government Executive</a> |  <a href="#">Government Technology</a>          |  <a href="#">ISACA</a>           |  <a href="#">ISSA International</a> |
|  <a href="#">Krebs on Security</a>    |  <a href="#">MITRE ATT&amp;CK®</a>    |  <a href="#">NASCIO</a>                         |   |  |
|  <a href="#">Schneier on Security</a> |  <a href="#">SC Media</a>             |  <a href="#">StateScoop</a>                     |  <a href="#">The Hacker News</a> |  <a href="#">The Record</a>         |