



Week of November, 11, 2024

## Cybersecurity Headlines

### Official Security Bulletins

Headlines from List of Official Government Sources

#### NASCIO Report Explores the Risks and Rewards of Generative AI in State Government - NASCIO

www.nascio.org

Meredith Ward Deputy Executive Director National Association of State Chief Information Officers 859.514.9209 mward@NASCIO.org



#### CISA, NSA, and Partners Issue Annual Report on Top Exploited Vulnerabilities

www.nsa.gov

FORT MEADE, Md. - Malicious cyber actors are increasingly exploiting zero day vulnerabilities to compromise enterprise networks, according to an annual Cybersecurity Advisory (CSA) about the top



#### NSA Issues Guidance for using Trusted Platform Modules (TPMs)

www.nsa.gov

FORT MEADE, Md. – The National Security Agency (NSA) is issuing guidance for using Trusted Platform Modules (TPMs) to secure computing devices and harden the Department of Defense (DoD)



#### USCYBERCOM Unveils AI Roadmap for Cyber Operations

www.cybercom.mil

Mr. Michael Clark, deputy director of plans and policy at U.S. Cyber Command, presented a plan to integrate artificial intelligence into military cyber operations at AI Defense Forum, the annual

### Cybercrimes, Scams & Incidents

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

#### FBI: Spike in Hacked Police Emails, Fake Subpoenas

krebsonsecurity.com

The Federal Bureau of Investigation (FBI) is urging police departments and governments worldwide to beef up security around their email systems, citing a recent increase in cybercriminal services that use hacked police email accounts to send unauthorized subpoenas and customer data requests to U.S.-based technology companies.



#### New Phishing Tool Golssue Targets GitHub Developers in Bulk Email Campaigns

thehackernews.com

Cybersecurity researchers are calling attention to a new sophisticated tool called Golssue that can be used to send phishing messages at scale targeting GitHub users.



#### Palo Alto Networks warns of potential PAN-OS RCE vulnerability

www.bleepingcomputer.com

Palo Alto Networks warned customers to restrict access to their next-generation firewalls because of a potential remote code execution vulnerability in the PAN-OS management interface.

### Industry News

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



#### Report card: State, local geospatial leaders need better governance, infrastructure to collaborate across agencies | StateScoop

statescoop.com

A new report says geospatial leaders across states and localities need more organized governance, which could power better data collaboration.



#### Veterans' military skills can help them fill cyber vacancies, State official says

www.govexec.com

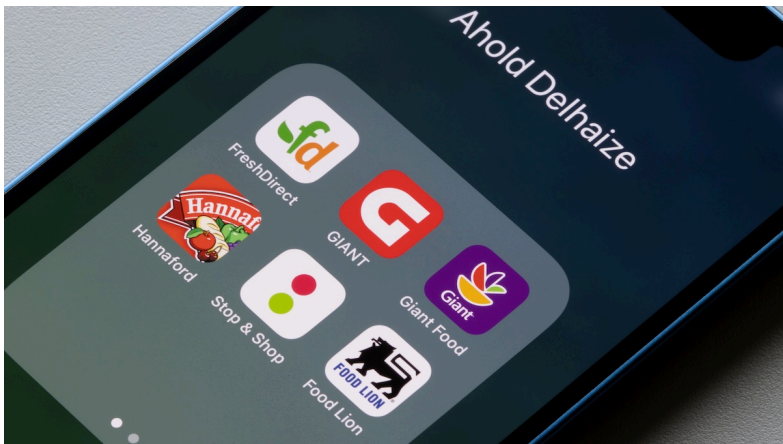
The White House's national cybersecurity strategy said that greater veteran participation in the U.S. cyber workforce can help enhance critical digital defenses.



#### Windows 11 is adding a 'Share' button to the Start menu and Taskbar

www.bleepingcomputer.com



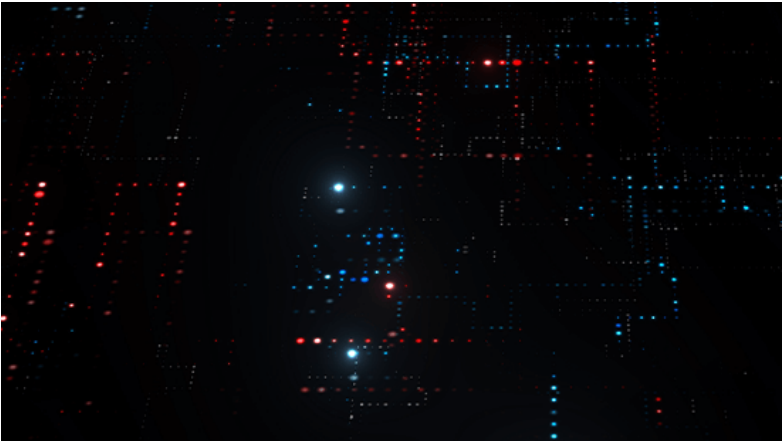


### Ahold Delhaize Cybersecurity Incident Impacts Giant Food, Hannaford

www.securityweek.com

Cybersecurity incident impacts Giant Food, Hannaford, and other Ahold Delhaize USA brands, including pharmacies and e-commerce services.

Microsoft wants you to share content/items more frequently, so it's now adding the "Share" button everywhere, including the Start menu and even the taskbar.



### CrowdStrike Panel Explores Lessons Learned from Massive Outage

www.isaca.org

An ISACA conference panel dissected the massive CrowdStrike incident, dissecting what went wrong and lessons learned to help avoid similar incidents in the future.



### US indicts Snowflake hackers who extorted \$2.5 million from 3 victims

www.bleepingcomputer.com

The Department of Justice has unsealed the indictment against two suspected Snowflake hackers, who breached more than 165 organizations using the services of the Snowflake cloud storage company.



### A Look at Government Cyber Insurance Prospects in 2024

www.govtech.com

To reduce risks, cybersecurity insurers have often raised premiums, asked for more information about applicants and tightened the sublimits on the kinds of cyber incident coverage they offer.

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

- [!\[\]\(49cafc1b4ac9c36b24a666d112dd1bdd\_img.jpg\) CISA](#)
- [!\[\]\(0ff44b1c51a0cf0a3e3adb3d5834a98e\_img.jpg\) CIS/MS-ISAC](#)
- [!\[\]\(119910d55c53d7c363d7a7af7cc110f5\_img.jpg\) CyberCom](#)
- [!\[\]\(92c0229b1b18d695c62b7ee87076b02f\_img.jpg\) DHS](#)
- [!\[\]\(ee9978c30678ad4e518b00a570930ae0\_img.jpg\) DOJ](#)
- [!\[\]\(15415784d6113627cebc2500aa30a821\_img.jpg\) FBI](#)
- [!\[\]\(fb282af4f3638ce1edee6c4cafd232cb\_img.jpg\) NIST](#)
- [!\[\]\(7ac9012a07f53747de02f75d70e72d65\_img.jpg\) NSA](#)
- [!\[\]\(e590d324942287093ca58a1a216a24e9\_img.jpg\) White house | ONCD](#)

#### External Quick links

- [!\[\]\(fbea698cdd18bad28d8e6b87acf959be\_img.jpg\) AIScoop](#)
- [!\[\]\(a65c8b450e4c61cdf4380ee7012e3c10\_img.jpg\) BleepingComputer](#)
- [!\[\]\(12c7868114a2b92d1648bff4877d5974\_img.jpg\) Cisco Talos Intelligence Group](#)
- [!\[\]\(c21ed9650a70a5701c14a0cc3bd4040a\_img.jpg\) CSO Online](#)
- [!\[\]\(0018649fcdf3fe29c5fea4d9cf2f217d\_img.jpg\) CyberScoop](#)
- [!\[\]\(b096dfb61a8b8d998559699405fb2f46\_img.jpg\) Cybersecurity Dive](#)
- [!\[\]\(e2aacf3ab40ad9c8a08f5753f495cbb0\_img.jpg\) Cyware](#)
- [!\[\]\(2dc0f22ec95dd606abbfcb05fe3e8022\_img.jpg\) CyberWire](#)
- [!\[\]\(bb0858398ee5c34d35231992d4161507\_img.jpg\) Government Executive](#)
- [!\[\]\(cf69df0255b47a71c26a823e160b03c1\_img.jpg\) Government Technology](#)
- [!\[\]\(574f5097387761db356ef47f371edd49\_img.jpg\) ISACA](#)
- [!\[\]\(07d810486a29ea5700e5425e76f70ca1\_img.jpg\) Krebs on Security](#)
- [!\[\]\(908c7e4ac9441ff2d4bc8dbfc7582c4d\_img.jpg\) MITRE ATT&CK®](#)
- [!\[\]\(569a42878f8eb14cbc24ad6aac850365\_img.jpg\) NASCIO](#)
- [!\[\]\(cdd3ed2251fe7706e0bd5a2de3cabadd\_img.jpg\) FedScoop](#)
- [!\[\]\(aa085dd983ee675ac97d135c628f56d8\_img.jpg\) StateScoop](#)
- [!\[\]\(767cc288d2fcabf992a0f0c59efb3ea3\_img.jpg\) The Hacker News](#)
- [!\[\]\(af8d7cfd89cf5b85649760ed7dd699a7\_img.jpg\) The Record](#)
- [!\[\]\(2a5810d4cccbb9f7e03fad7031ac6714\_img.jpg\) Schneier on Security](#)
- [!\[\]\(53aaabcddda191267bb93c73d09855f5\_img.jpg\) SC Media](#)