

Cybersecurity Headlines

Cybercrimes, Scams & Incidents

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

Operation Endgame Hits Malware Delivery Platforms - Krebs on Security

krebsonsecurity.com

Law enforcement agencies in the United States and Europe today announced Operation Endgame, a coordinated action against some of the most popular cybercrime platforms for delivering ransomware and data-stealing malware. Dubbed “the largest ever operation against botnets,” the international effort is being billed as the opening salvo in an ongoing campaign targeting advanced malware “droppers” or “



Snowflake account hacks linked to Santander, Ticketmaster breaches

www.bleepingcomputer.com

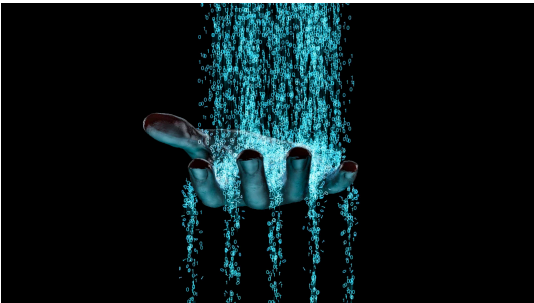
A threat actor claiming recent Santander and Ticketmaster breaches says they stole data after hacking into an employee's account at cloud storage company Snowflake. However, Snowflake disputes these claims, saying recent breaches were caused by poorl...



Everbridge warns of corporate systems breach exposing business data

www.bleepingcomputer.com

Everbridge, an American software company focused on crisis management and public warning solutions, notified customers that unknown attackers had accessed files containing business and user data in a recent corporate systems breach.



Official Security Bulletins

Headlines from CISA, MS-ISAC, and other official sources

CISA Hosts First Annual Information and Communications Technology Supply Chain Risk Management Task Force Conf

www.cisa.gov

WASHINGTON – Today, the Cybersecurity and Infrastructure Security Agency (CISA) announced it will host the first annual Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force Conference, Innovations in ICT Supply Chain Risk Management. The Conference will be a one-day event, taking place on June 12, 2024, from 9:00 a.m. to 5:15 p.m. ET at the MITRE Corporati

A Plan to Protect Critical Infrastructure from 21st Century Threats

www.cisa.gov

On April 30th, the White House released National Security Memorandum-22 (NSM) on Critical Infrastructure Security and Resilience, which updates national policy on how the U.S. government protects and secures critical infrastructure from cyber and all-hazard threats. NSM-22 recognizes the changed risk landscape over the past decade and leverages the enhanced authorities of federal departments and a



CISA warns of actively exploited Linux privilege elevation flaw

www.bleepingcomputer.com

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has added two vulnerabilities in its Known Exploited Vulnerabilities (KEV) catalog, including a Linux kernel privilege elevation flaw.



NIST's Apostol Vassilev on using AI to strengthen cyber resilience

fedscoop.com

Apostol Vassilev, Ph.D., Research Supervisor, Computer Security Division at NIST, talks about where he is seeing signs that AI will help accelerate agency efforts to establish zero trust practices. In addition, he discusses the role AI and automation play in strengthening cyber resilience

Industry News

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



CISA advisors urge changes to JCDC's goals, operations, membership criteria

therecord.media

The Joint Cyber Defense Collaborative — a public-private cyberthreat information hub created by CISA — should focus more on incidents and less on policy, while refining other aspects of its operations, an advisory committee said.



What CISOs need to know about Microsoft's Copilot+

www.csoonline.com

The Recall feature of Microsoft's AI-powered Copilot+ introduces some potential security risks by capturing and storing user activity.



Third-Party Cyber Attacks: The Threat No One Sees Coming – Here's How to Stop Them

thehackernews.com

Learn about critical threats that can impact your organization and the bad actors behind them from Cybersixgill's threat experts.

More Responsible Data Usage Through Privacy Enhancing Technologies

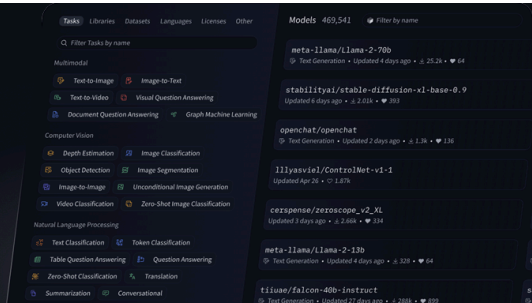
www.isaca.org

Privacy-enhancing technology (PET) is the privacy control consisting of information and communication technology (ICT) measures, products or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or

AI platform Hugging Face says hackers stole auth tokens from Spaces

www.bleepingcomputer.com

AI platform Hugging Face says that its Spaces platform was breached, allowing hackers to access authentication secrets for its members.



AI Company Hugging Face Detects Unauthorized Access to Its Spaces Platform

thehackernews.com

Hugging Face detected unauthorized access to its Spaces platform. A subset of secrets might have been accessed without authorization.



Researcher Uncovers Flaws in Cox Modems, Potentially Impacting Millions

thehackernews.com

Researchers discovered authorization bypass vulnerabilities in Cox modems that could have allowed hackers to access and control millions of devices.



FBI recovers 7,000 LockBit keys, urges ransomware victims to reach out

www.bleepingcomputer.com

The FBI urges past victims of LockBit ransomware attacks to come forward after revealing that it has obtained over 7,000 LockBit decryption keys that they can use to recover encrypted data for free.



Major service tag security problems reported in Microsoft Azure

www.csoonline.com

Microsoft has opted not to fix the issue reported by Tenable Research, but many defend that decision, arguing that this should be decided by CISOs based on their environment.

A Vulnerability in Check Point Security Gateways Could Allow for Credential Access

www.cisecurity.org

A vulnerability has been discovered in Check Point Security Gateway Products that could allow for credential access. A Check Point Security Gateway sits between an organization's environment and the Internet to enforce policy and block threats and...

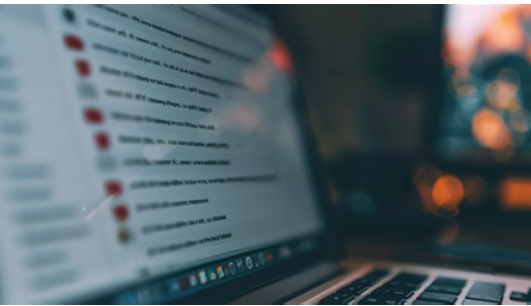
undesired processing of PII, all without losing the functionality of the ICT system.



States urge Congress not to claw back cybersecurity grant funding | StateScoop

statescoop.com

A cohort of state and local government associations wrote congressional leaders a letter asking them not to redirect funding already approved for cybersecurity enhancements.



Navigating Email: From Spam Wars to Trusted Relationships

www.govtech.com



SASE Threat Report: 8 Key Findings for Enterprise Security

thehackernews.com

Discover how AI is transforming enterprise security and the associated risks in Cato's latest SASE Threat Report.



What are non-human identities and why do they matter?

www.csoonline.com

When digital systems need access and permissions they require credentials just like human beings. These non-human identities allow many components of complex systems to work together but present significant security issues.





Atlassian’s Confluence hit with critical remote code execution bugs

www.csoonline.com

The input validation bug enables an authenticated attacker to exploit the privileges to inject malicious codes.

Microsoft: The brand attackers love to imitate

www.csoonline.com

Cybercriminals often hide attack attempts behind well-known brand names with the intent to trick targeted users into making the fatal click. Microsoft is their favorite — by far.



New ISACA Research: Many Organizations Believe Digital Trust Will Become More Important, Yet Budget, Strategy, Skills...

www.isaca.org

82 percent of respondents say in five years digital trust will be more important, yet only 20 percent are increasing budgets for digital trust.




HHS reverses course, allows Change Healthcare to file breach notifications for others

therecord.media


The department had received pushback against a previously released FAQ page that said every organization affected by the hack of Change Healthcare would have to file their own breach notices with federal and state regulators.

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.

 [BleepingComputer](#)

 [CIS](#)


 [CISA](#)


 [Cisco Talos Intelligence Group](#)


 [CSO Online](#)


 [Cyware](#)


 [ISACA](#)


 [Government Executive](#)

 [Government Technology](#)

 [Krebs on Security](#)

 [The Hacker News](#)

 [The Record](#)

 [NASCIO](#)

 [StateScoop](#)