# AI-generated voices in robocalls now illegal

Link: https://www.helpnetsecurity.com/2024/02/09/ai-generated-voices-robocalls-illegal/

Summary: The ruling, which takes effect immediately, makes voice cloning technology used in common robocall scams targeting consumers illegal.  
This would give State Attorneys General across the country new tools to go after bad actors behind these nefarious robocalls.  
“Bad actors are using AI-generated voices in unsolicited robocalls to extort vulnerable family members, imitate celebrities, and misinform voters.  
The Commission can also take steps to block calls from telephone carriers facilitating illegal robocalls.  
The FCC currently has a Memorandum of Understanding with 48 State Attorneys General to work together to combat robocalls.

# February 2024 Patch Tuesday forecast: Zero days are back and a new server too

Link: https://www.helpnetsecurity.com/2024/02/09/february-2024-patch-tuesday-forecast/

Summary: Microsoft Server 2025Microsoft announced Server 2025 is now available on the Windows Server Insider Channel.  
Apple released updates for all the operating systems on January 22 and Safari 17.3 for Monterey and Ventura macOS.  
Microsoft released their monthly non-security preview patch for Windows 10 22H2, Windows 11 22H2, and Windows 11 23H2 on January 23.  
Expect all the OS, Office, SharePoint and Exchange server updates.  
Be on the lookout for zero-day updates and give them the priority they deserve.

# Why we fall for fake news and how can we change that?

Link: https://www.helpnetsecurity.com/2024/02/09/fight-disinformation/

Summary: Defining disinformationDisinformation refers to false or misleading information that is spread with the intent to create confusion, undermine trust, or advance a particular agenda.  
Disinformation can take many forms, such as fake news articles, manipulated images or videos, misleading social media posts, and more.  
(Misinformation, on the other hand, is the unintentional creation and spreading of false or misleading information.)  
Psychologist Gordon Robert Pennycook and David G. Rand, a professor of Management Science and Brain and Cognitive Sciences at Massachusetts Institute of Technology, have outlined a number of reasons why people believe fake news.  
They also found that those who turned to social media for news (younger adults), were more likely to fall for fake news.

# New infosec products of the week: February 9, 2024

Link: https://www.helpnetsecurity.com/2024/02/09/new-infosec-products-of-the-week-february-9-2024/

Summary: Here’s a look at the most interesting products from the past week, featuring releases from Cisco, Metomic, OPSWAT, Qualys, and Varonis.  
OPSWAT enhances its MetaDefender Kiosk product lineOPSWAT announced new advancements to its MetaDefender Kiosk product line.  
Building on the success of last year’s Mobile Kiosk, OPSWAT introduces the Kiosk Min.  
The new form factor of the MetaDefender Kiosk addresses specific customer needs, designed to be more accessible, portable and versatile.  
Also unveiled is the new OPSWAT MetaDefender Kiosk Stand, a new hardware that supports VESA-mountable Kiosks and other VESA-mountable devices.

# Key strategies for ISO 27001 compliance adoption

Link: https://www.helpnetsecurity.com/2024/02/09/robin-long-kiowa-security-iso-27001-implementation/

Summary: You might call this the ‘ISMS Team’ (where ISMS means Information Security Management System, another way to describe ISO 27001).  
What advice do you have for organizations, particularly SMEs, in effectively allocating resources and budget for ISO 27001 implementation?  
What strategies can be employed to convince top management of the necessity and benefits of ISO 27001 compliance?  
Many businesses like the concept of ISO 27001 but aren’t quite ready to commit fully.  
After a few months of this, you may feel that ISO 27001 isn’t quite so formidable, and that you are ready to tackle it.

# Cybersecurity teams recognized as key enablers of business goals

Link: https://www.helpnetsecurity.com/2024/02/09/cybersecurity-teams-trust-levels/

Summary: 97% of office workers across the UK and US trust their cybersecurity team’s ability to prevent or minimize damage from cyberattacks, according to CybSafe.  
It indicates how cybersecurity teams and professionals are increasingly viewed as a vital strategic function enabling both individuals and business success.  
When receiving communications from cybersecurity teams, 52% of respondents said they read emails immediately.  
Positive impact of security teams on business goalsWhen it comes to the impact of security teams on business success, 74% believe security teams enable business goals as well as personal work objectives (77%), with just 7% of respondents stating their cybersecurity team has had an overall negative impact on their working experience.  
“We hear a lot of negativity regarding the uphill battle faced by many cybersecurity teams, especially those protecting sensitive data.

# How AI is revolutionizing identity fraud

Link: https://www.helpnetsecurity.com/2024/02/09/identity-fraud-growth/

Summary: Nearly half of businesses reported a growth in synthetic identity fraud, while biometric spoofs and counterfeit ID fraud attempts also increased, according to AuthenticID.  
In the meantime, the explosion of AI has also pushed identity fraud into a new frontier that will become a potential global shift in the coming year.  
68% of people said the threat of identity fraud and scams impacts how they make purchases, open accounts, and do business.  
“These attacks and identity fraud crimes can lead to high economic losses and a loss of customer trust.  
Awareness of these trends and staying agile enough to minimize the damage is crucial for a business’ identity proofing strategy.

# LassPass is not LastPass: Fraudulent app on Apple App Store

Link: https://www.helpnetsecurity.com/2024/02/08/lasspass-lastpass-apple-app-store/

Summary: A fraudulent app named “LassPass Password Manager” that mimics the legitimate LastPass mobile app can currently be found on Apple’s App Store, the password manager maker is warning.  
The fraudulent app on Apple’s App Store“The app in question is called ‘LassPass Password Manager’ and lists Parvati Patel as the developer.  
The app attempts to copy our branding and user interface, though close examination of the posted screenshots reveal misspellings and other indicators the app is fraudulent,” says Mike Kosak, Senior Principal Intelligence Analyst at LastPass.  
As the company is working to get this application taken down, it’s heartening to see that several users have left reviews warning users about the likely scammy nature of the app:Before downloading mobile apps, users should always check that the stated developer of the app is the right one (in LastPass’ case, it’s LogMeIn) and check user reviews for possible red flags.

# Akira, LockBit actively searching for vulnerable Cisco ASA devices

Link: https://www.helpnetsecurity.com/2024/02/08/ransomware-cisco-asa-vulnerabilities/

Summary: Akira and Lockbit ransomware groups are trying to breach Cisco ASA SSL VPN devices by exploiting several older vulnerabilities, security researcher Kevin Beaumont is warning.  
“But the problem is nobody has complete visibility of what exploits actually exist,” he added, and advised admins to upgrade to the latest ASA release on all devices that have the AnyConnect SSL VPN feature enabled on the device’s (internet-exposed) interface.  
Old vulnerabilities haunt many organizationsCisco ASA devices are widely deployed in organizations of all sizes, and are regularly targeted by attackers (including ransomware groups) via unpatched vulnerabilities, credential stuffing and targeted brute-force attacks.  
And though an exploit for CVE-2020-3580, a cross-site scripting (XSS) vulnerability affecting Cisco ASA and FTD devices, was leveraged by attackers in 2021, ransomware groups are obviously hoping that many organizations are VERY slow to patch.  
There has been a significant uptick in scanning for Cisco AnyConnect VPN devices,” Beaumont also noted on Wednesday.

# 10 tips for creating your security hackathon playbook

Link: https://www.helpnetsecurity.com/2024/02/08/security-hackathon-tips/

Summary: In this article, I’d like to share some of my key insights and tips that could help your organization create or refine a security hackathon playbook.  
Hackathon events bring together product and security experts for the sole purpose of finding security vulnerabilities within a product.  
A security lead responsible for analyzing the security architecture and identifying the priority security areas.  
Rate the vulnerabilities – Confirmed security vulnerabilities need to be reviewed and rated for severity using CVSS scoring.  
This can be used to drive systemic improvements in product security architecture, design, and the evaluation process.

# Choosing the right partner when outsourcing cybersecurity

Link: https://www.helpnetsecurity.com/2024/02/08/anya-shpilman-wdigital-outsourcing-cybersecurity/

Summary: Additionally, she predicts a future trend toward increased automation in cybersecurity outsourcing.  
Can you elaborate on the benefits and potential risks of outsourcing cybersecurity services?  
Potential risksThere are few real risks, however, outsourcing cybersecurity will mean handing over a certain amount of control.  
Is outsourcing cybersecurity more cost-effective than maintaining an in-house team?  
I’ve experienced both perspectives: creating an effective in-house cybersecurity team and offering outsourced cybersecurity solutions.

# SOAPHound: Open-source tool to collect Active Directory data via ADWS

Link: https://www.helpnetsecurity.com/2024/02/08/soaphound-open-source-collect-active-directory-data-adws/

Summary: SOAPHound is an open-source data collection tool capable of enumerating Active Directory environments through the Active Directory Web Services (ADWS) protocol.  
How SOAPHound worksSOAPHound is a substitute for various open-source security tools typically employed for extracting data from Active Directory via the LDAP protocol.  
The ADWS server decodes these LDAP queries and relays them to the LDAP server located on the same domain controller.  
Finally, SOAPHound supports additional collection methods for specific internal services of interest, such as Active Directory Certificate Services (ADCS) and Active Directory integrated DNS records.  
Must read: 15 open-source cybersecurity tools you’ll wish you’d known earlierMore open-source tools to consider: