ISSUE 29

31 March 2025

IDENTITY AND UTS

HIGHLIGHTS

In This Issue

Welcome to this week's edition of Identity & UTS Highlights, where we delve into the crucial topics of identity protection. From emerging technologies and privacy risks to surveillance concerns and protection strategies, we cover the essential developments that impact your digital security. Stay informed with our weekly updates on the most pressing issues affecting our community.

The opinions expressed within the articles are not representative of our office's views and are selected solely for their relevance to identity protection and threat mitigation.

Special Point of Interest:

This week we have also attached an informational insert on Incogni, a data privacy service that helps remove personal information from data brokers.

China

China Strengthening Face Biometrics Regulation to Mandate Choice, Consent

Key Insights: China is introducing new regulations for facial recognition technology, requiring businesses to obtain explicit consent and provide alternatives for those who refuse biometric data collection. The rules, which take effect in June, also mandate that companies handling over 100,000 biometric records register with cybersecurity authorities and conduct data protection assessments.

#China #FacialRecognition #Biometrics #Technology #Cybersecurity
DOI: March 24, 2025
Full Article

China Releases New Rules Regarding the Use of Facial Recognition Technology

Key Insights: On March 21, 2025, China introduced new "Security Management Measures for the Application of Facial Recognition Technology," effective June 1, 2025, which regulate the processing of facial information for individual identification purposes. Key requirements include restricted storage and transmission of facial data, conducting privacy impact assessments, ensuring necessity for public place installations, restricting exclusive use of facial recognition, and mandatory filing with authorities when processing data of over 100,000 individuals.

#China #FacialRecognition #Privacy #Biometrics #Cybersecurity #PrivacyLaw #IdentityProtection
DOI: March 27, 2025
Full Article

Global Surveillance Activities

China

Chinese FamousSparrow Hackers Deploy Upgraded Malware in Attacks

Key Insights: The China-linked cyberespionage group FamousSparrow has been using a new modular version of its SparrowDoor backdoor in targeted attacks, including on a US-based trade organization, exploiting outdated Microsoft Exchange and Windows Server vulnerabilities. The new version of SparrowDoor features improved code, parallel command execution, and a plugin-based architecture, with added capabilities such as file manipulation, keylogging, and screenshot capturing, while also leveraging the ShadowPad RAT for enhanced stealth.

#China #CyberAttack #Hacking #Malware #Microsoft #Windows
DOI: March 27, 2025
Full Article

US Expands Export Blacklist to Keep Computing Tech Out of China

Key Insights: The US has added 80 organizations to its export blacklist, including Chinese entities, to prevent China from acquiring advanced American technology for military purposes, particularly in computing, AI, and hypersonic weapons. The move, which includes companies like Inspur Group and the Beijing Academy of Artificial Intelligence, aims to safeguard national security but has faced criticism from affected entities and China, which condemns the restrictions as violations of international law.

#USA #China #Technology #ArtificialIntelligence
DOI: March 26, 2025
Full Article

Russia

Russia’s Information Security Industry Expands International Footprint

Key Insights: The 2025 Information Security Forum in Russia highlighted growing ties with authoritarian states, as companies like Positive Technologies expand despite U.S. sanctions, capturing markets in Russia, Belarus, and beyond. Russia's push for a sovereign internet and collaboration with countries like Iran and China reflects its challenge to Western digital dominance and promotion of authoritarian information control models.

#Technology #Russia #Belarus #Iran #China #Cybersecurity
DOI: March 27, 2025
Full Article

Researchers Uncover 200 Unique C2 Domains Linked to Raspberry Robin Access Broker

Key Insights: Raspberry Robin, a sophisticated malware used by various criminal groups, has been linked to nearly 200 unique command-and-control domains and is associated with Russian state-sponsored actors like Cadet Blizzard. This malware has evolved with multiple attack methods, including USB-based propagation, fast-flux domain rotation, and pay-per-install botnet services, making it a versatile tool for distributing malicious payloads such as Dridex, LockBit, and IcedID.

#Malware #Russia #CyberAttack #Botnet
DOI: March 25, 2025
Full Article

When Getting Phished Puts You in Mortal Danger

Key Insights: Russian intelligence is mimicking recruitment websites for Ukrainian paramilitary units specifically targeting those websites focused on recruiting anti-Putin Russian nationals. The fake websites are intended to gather personal information on Russian nationals visiting the websites or entering their personal information in the websites’ recruitment pages. Participation in anti-war actions is illegal in Russia and convictions come with 10 and 20 years in prison.

#Russia #Ukraine #Phishing #PII
DOI: March 28, 2025
Full Article

The Rest of the World

Google's Parent To Buy Cybersecurity Group Wiz In Its Biggest Ever Deal

Key Insights: Google's $32 billion acquisition of Israeli cybersecurity firm Wiz has raised concerns about the company's deepening ties with the Israeli government, particularly amid criticism of its involvement in the Project Nimbus cloud contract. Human rights organizations worry that this acquisition will strengthen Google's role in AI-driven military technologies and contribute to human rights abuses, especially with leadership from former members of Israel's military cyber-espionage unit.

#Technology #Google #Israel #Cybersecurity #ArtificialIntelligence
DOI: March 20, 2025
Full Article

Teledyne FLIR to Supply Long-Range Surveillance Systems to Saudi Arabia

Key Insights: Teledyne FLIR has secured a $7.8-million contract to supply Saudi Arabia with next-generation Lightweight Vehicle Surveillance Systems, which integrate long-range thermal imaging and radar for enhanced surveillance. The LVSS, designed for mobility and rapid deployment, will support border security, infrastructure monitoring, and other critical applications, though the exact number of units to be delivered remains undisclosed.

#Technology #Surveiallnce #USA #SaudiArabia
DOI: March 25, 2025
Full Article

Data Breaches, Hacks, and Scams

T-Mobile Reaches $350M Settlement for 2021 Data Breach Affecting 76M Customers

Key Insights: T-Mobile has agreed to a $350 million settlement for a 2021 data breach affecting 76 million customers, offering compensation for financial losses, time spent addressing the breach, and alternative payments, along with two years of identity protection services. The settlement also includes investments in improved cybersecurity measures, such as enhanced SIM swap protection and identity verification systems, to prevent future incidents.

#DataBreach #Financial #IdentityProtection #Cybersecurity
DOI: March 24, 2025
Full Article

Brazilian ID App FacePass Leaks 1.6M Files in Major Biometric Data Breach

Key Insights: A major data breach at FacePass, a Brazilian ID app, exposed over 1.6 million files containing sensitive personal information, including national IDs, selfies, and AWS credentials, due to an exposed AWS S3 bucket. The breach poses significant risks for identity theft, financial fraud, and phishing attacks, highlighting the challenges of securing biometric data in digital identification systems.

#Biometrics #MobileApplication #DataBreach #PII #IdentityTheft #Financial #Phishing #CyberAttack
DOI: March 26, 2025
Full Article

Major Cyber Attacks Targeting Transportation & Logistics Industry

Key Insights: The transportation and logistics industry is facing a surge in cyberattacks, including ransomware and data breaches, disrupting critical operations and stealing sensitive information. High-profile incidents, such as attacks on Nagoya Port and Seattle-Tacoma Airport, highlight the growing threat and the urgent need for enhanced cybersecurity measures.

#CyberAttack #Ransomware #DataBreach #PII #Cybersecurity
DOI: March 28, 2025
Full Article

Identity & Privacy Issues

Anti-DOGE Activists Dox Tesla Owners' Personal Information, Addresses on Dark Web Page

Key Insights: Dogequest, a website that previously doxed Tesla owners and Department of Government Efficiency members, has reemerged on the dark web as "DOGEQUEST Unleashed," making it harder for authorities to track and shut down. The site promotes anonymity for users and administrators, escalating tensions surrounding Tesla and the government's involvement with the company, likely leading to intensified law enforcement actions.

#DarkWeb #PII
DOI: March 24, 2025
Full Article

Ransomware Gang Fog Publishes Victim IPs on Dark Web

Key Insights: Kaspersky experts have uncovered a new tactic used by the Fog Ransomware group, which now publishes victims' IP addresses on the Dark Web, making them more vulnerable to further attacks. This strategy, aimed at increasing psychological pressure and the likelihood of ransom payments, heightens the risk of additional criminal activities targeting compromised networks and puts affected organizations at greater risk of regulatory penalties.

#DarkWeb #Ransomware #CyberAttack
DOI: March 25, 2025
Full Article

B1ack's Stash Marketplace Actors Set to Release 4 Million Stolen Credit Card Records for Free

Key Insights: B1ack's Stash, a dark web carding marketplace, plans to release 4 million stolen credit card records for free as part of its strategy to attract cybercriminals and gain credibility. The release of sensitive data, including card details and personal information, significantly increases the risk of financial fraud and identity theft, highlighting the need for stronger cybersecurity and collaborative efforts to combat such threats.

#DarkWeb #PII #Financial #IdentityTheft
#CyberAttack #Cybersecurity
DOI: March 26, 2025
Full Article

Ransomware Gang Blackmails Victims After Publicly Revealing Data

Key Insights: The Fog Ransomware group has introduced a new tactic by linking victims' IP addresses to their stolen data and publishing them on the Dark Web, increasing psychological pressure and regulatory risks for affected organizations. This shift from traditional double extortion tactics aims to intimidate victims into paying quickly and may also facilitate follow-up cyberattacks by exposing entry points to other criminals.

#Ransomware #DarkWeb #CyberAttack
DOI: March 27, 2025
Full Article

Hacking Incidents

Major Hacks of The Week: Are You At Risk?

- UAE Public and Private Sector
- ReversingLabs
- M.A.D Mobile Apps Developers Limited

New npm Malware Attack Infects Popular Ethereum Library with Backdoor

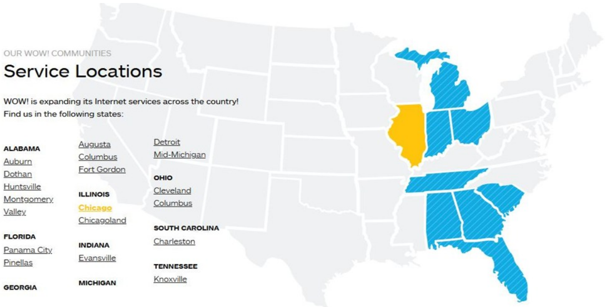
Key Insights: Researchers at ReversingLabs found a new malware attack on the npm repository. Hackers hid harmful code inside fake download tools to secretly install a backdoor in the popular Ethereum blockchain tool, ethers. The malware used tricks to avoid detection, like deleting temporary files, showing the ongoing risk of malicious software in package repositories.

#Malware #CyberAttack #Blockchain
DOI: March 26, 2025
Full Article

Arkana Ransomware Attack on WideOpenWest: What You Need to Know

Key Insights: The newly emerged ransomware group Arkana has launched its first attack, compromising over 403,000 customer accounts of WideOpenWest, a major US broadband provider, and gaining control of critical backend systems. Arkana's attack exposed sensitive customer data, including passwords, security questions, and financial information, and included doxing of WOW!'s executives, highlighting the growing threat posed by this group's extortion-based, multi-phase ransomware tactics.

#Ransomware #CyberAttack #PII #Financial
DOI: March 25, 2025
Full Article



OUR WOW! COMMUNITIES

Service Locations

WOW! is expanding its Internet services across the country!
Find us in the following states:

ALABAMA
Auburn
Dothan
Huntsville
Montgomery
Valley

FLORIDA
Panama City
Pinellas

GEORGIA
Augusta
Columbus
Fort Gordon

ILLINOIS
Chicago
Chicagoland

INDIANA
Evansville

MICHIGAN
Detroit
Mid-Michigan

OHIO
Cleveland
Columbus

SOUTH CAROLINA
Charleston

TENNESSEE
Knoxville

Data Breaches, Hacks, and Scams

Hacking Incidents

LGBTQ and BDSM Dating Apps Leak Private Photos

Key Insights: Cybernews research has discovered that the applications BDSM People, CHICA, TRANSLOVE, PINK, and BRISH developed by M.A.D. Mobile Apps Developers Limited leak "secrets" (i.e. API keys, passwords, encryption keys, etc.) that can allow anyone to gain access to confidential photos, videos, and other personal information. Nearly 1.5 million user-uploaded images including profile photos, public posts, profile verification images, photos removed for rule violations, and private photos sent through direct messages, were left publicly accessible to anyone.

#Apple #Cybersecurity #MobileApplication #PII #SocialMedia
DOI: March 27, 2025
Full Article

Fake DeepSeek Ads Spread Malware to Google Users

Key Insights: Malicious links to fake DeepSeek sites are popping up in ads located in Google-sponsored research results. Clicking on the malicious links results in the deployment of the Heracles information stealer malware designed to go after crypto wallets. Google has been unable to prevent fake malicious ads from appearing in sponsored search results. Google users are advised to not click on sponsored search results.

#Google #Malware #AdTech #Crypto #DeepSeek
DOI: March 27, 2025
Full Article

Massive Auto-Hack Threat Emerges- Why Passwords Are Now Obsolete

Key Insights: Microsoft and Google are leading the shift towards passwordless authentication, with Microsoft phasing out passwords for over a billion users and Google expanding its hardware-based passkeys. As traditional passwords become increasingly vulnerable to cyberattacks, security experts urge users to adopt more secure alternatives like passkeys, biometrics, and multi-factor authentication to better protect their accounts.

#Microsoft #Google #CyberAttack #Cybersecurity #Biometrics
DOI: March 30, 2025
Full Article

GorillaBot Attacks Windows Devices with 300,000+ Attack Commands Across 100+ Countries

Key Insights: The new GorillaBot botnet, built on the Mirai framework, has executed over 300,000 attacks across more than 100 countries in just three weeks, targeting industries like telecommunications, finance, and education. Using advanced encryption, anti-debugging techniques, and custom authentication methods, GorillaBot evades detection and hijacks vulnerable devices for DDoS attacks and other malicious activities.

#Botnet #CyberAttack #Financial #Hacking #Windows #MobileDevice
DOI: March 27, 2025
Full Article

Hacking Incidents

GitHub-Hosted Malware Infects 1M Windows Users

Key Insights: Cybercriminals are creating undetectable Android malware that hides malicious code in mobile applications, bypassing traditional detection methods. Users should only download applications from official app stores and be wary of applications requesting unnecessary permissions.

#Android #Google #Malware #MobileApplication
DOI: March 25, 2025
Full Article

PlayBoy Locker Ransomware

Key Insights: PlayBoy Locker is a type of ransomware that locks files, making them unusable. It also removes backup copies stored on the system, making recovery harder. It was originally distributed as a Ransomware-as-a-Service, but now security tools like VMware Carbon Black and Symantec can detect and block it.

#Ransomware
DOI: March 26, 2025
Full Article

CISA Warns of RESURGE Malware Exploiting Ivanti RCE Vulnerability

Key Insights: CISA has issued a report on a critical vulnerability in Ivanti Connect Secure devices, allowing attackers to deploy sophisticated malware, which enable unauthorized access, backdoor creation, and system manipulation. CISA recommends applying security patches, monitoring activity, and enforcing strong security to mitigate risk.

#CyberAttack #Malware #Cybersecurity
DOI: March 29, 2025
Full Article

Google Confirms Cyber ‘Espionage’ Attacks on Chrome Users from ‘Highly Sophisticated Malware’

Key Insights: Cybersecurity researchers discovered a sophisticated zero-day exploit in Google Chrome, triggered by clicking a phishing link in emails, which allowed attackers to bypass Chrome's sandbox protection and infect devices with spyware. Google has since confirmed the vulnerability and released a patch, emphasizing the importance of avoiding suspicious links and maintaining cautious email practices.

#Google #Phishing #Spyware #Malware #CyberAttack
DOI: March 26, 2025

RedCurl Cyberspies Create Ransomware to Encrypt Hyper-V Servers

Key Insights: The threat actor RedCurl, known for corporate espionage, has started deploying ransomware which specifically targets Hyper-V virtual machines in addition to their typical data exfiltration tactics. The shift to ransomware operations raises questions about whether RedCurl is using it as a distraction for espionage or as a private form of extortion for financial gain.

#Ransomware #Financial #CyberAttack
DOI: March 26, 2025
Full Article

Hacking Incidents

Google Suspends Account of Advertisers That Distributed Malware

Key Insights: Google suspended an advertiser for running sponsored ads that impersonated the legitimate DeepSeek website, delivering malware instead of the advertised service. The fake ads linked to a fraudulent site that resembled DeepSeek's, tricking users into downloading a Trojan, and Google acted swiftly to suspend the account after detecting the campaign.

#Google #AdTech #Malware
DOI: March 28, 2025
Full Article

New Sophisticated Malware CoffeeLoader Bypasses Endpoint Security to Deploy Rhadamanthys Shellcode

Key Insights: Researchers discovered a new macOS malware called **CoffeeLoader**, which bypasses security protections to install harmful code through phishing emails and compromised downloads. It evades detection by modifying system files, creating hidden directories, and disabling macOS security features while tricking trusted programs into running its malicious code. Once infected, the computer can be used by hackers to steal data, spy on users, spread malware, or even add it to a botnet that mines cryptocurrency, slowing down performance and draining system resources.

#Malware #Apple #macOS #Phishing #Botnet #Crypto
DOI: March 27, 2025
Full Article

New ReaderUpdate macOS Malware Loader Variants Emerge

Key Insights: Since mid-2024, a new Go-based variant of the ReaderUpdate macOS malware loader has emerged, continuing the distribution of Genieo adware through trojanized apps. This variant also collects system hardware details for unique identification and has the potential to deliver more malicious payloads, possibly enabling Pay-Per-Install or Malware-as-a-Service.

#Malware #Apple #MobileApplication #AdTech
DOI: March 27, 2025
Full Article

Hacking Incidents

New Phishing Attack Uses Real-Time Interception to Bypass 2FA

Key Insights: The Astaroth phishing kit bypasses two-factor authentication by intercepting and manipulating real-time credentials, including session cookies, to gain unauthorized access to accounts. It works as a middleman between the victim's device and legitimate authentication services, making it a highly advanced and stealthy threat that cybercriminals can exploit to steal sensitive data.

#Phishing #CyberAttack #PII
DOI: March 30, 2025
Full Article

CISA Warns of RESURGE Malware Exploiting Ivanti RCE Vulnerability

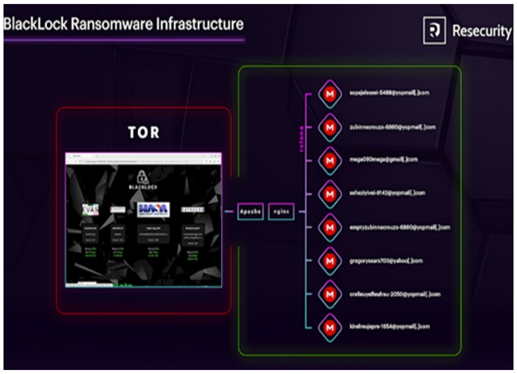
Key Insights: CISA has issued a report on the exploitation of a critical vulnerability in Ivanti Connect Secure devices, allowing attackers to deploy sophisticated malware like RESURGE and SPAWNSLOTH, which enable unauthorized access, backdoor creation, and system manipulation. CISA recommends applying security patches, monitoring network activity, and enforcing strong security practices to mitigate the risk of these advanced threats.

#CyberAttack #Malware #Cybersecurity
DOI: March 29, 2025
Full Article

BlackLock Ransomware Exposed After Researchers Exploit Leak Site Vulnerability

Key Insights: Threat hunters infiltrated the BlackLock ransomware group's infrastructure, uncovering a significant vulnerability in their data leak site that exposed sensitive information, including configuration files, credentials, and command histories. BlackLock, a rebranded version of the Eldorado group, has been heavily targeting various sectors in 2025, and the vulnerability was exploited to leak critical data, with hints of potential ties between BlackLock and another ransomware group, DragonForce.

#Ransomware #PII #CyberAttack
DOI: March 29, 2025
Full Article


BlackLock Ransomware Infrastructure
Resecurity
TOR
BLACKLOCK
Apache
nginx
rclone
sopajelessei-5488@yopmail[.]com
zubinnecrouzo-6860@yopmail[.]com
mega080mega@gmail[.]com
sehezlyivei-9142@yopmail[.]com
emptyzubinnecrouzo-6860@yopmail[.]com
gregorysears703@yahoo[.]com
crelleuyeffeufrau-2050@yopmail[.]com
kirefreujepre-1654@yopmail[.]com

Hacking Incidents

Automatic Password Hacking Machine Confirmed- Stop Using Passwords Now

Key Insights: Infostealer malware and credential stuffing attacks are on the rise, with tools like Atlantis AIO automating the use of millions of stolen passwords to target a wide range of services, including email, VPNs, and streaming platforms. Despite two-factor authentication, hackers can bypass protections using session cookies. Technology leaders are recommending and prioritizing passkeys over passwords.

#Malware #CyberAttack #Hacking
DOI: March 27, 2025
Full Article

95% of organizations reported deepfake incidents during 2024.

49% of companies experienced breaches over the past year, with 87% linked to identity vulnerabilities.

47% of the breaches mentioned above were driven by credential misuse, 41% by privileged access abuse, 36% by social engineering attacks and 35% by 2FA bypass attacks

T3 Financial Crimes Unit Freezes $9 Million Linked to Bybit Hack

Key Insights: The T3 Financial Crimes Unit, including Tether, Tron, and TRM Labs, froze nearly $9 million linked to the Bybit hack, one of the largest cryptocurrency thefts. Since its launch in September 2024, the unit has recovered over $150 million, demonstrating stablecoin technology's potential for security and transparency in combating illicit activity.

#Hacking #Crypto #Technology #CyberAttack
DOI: March 28, 2025
Full Article

“Crocodilus”, A New Malware Targeting Android Devices for Full Takeover

Key Insights: Researchers have discovered the Crocodilus mobile banking Trojan, which uses advanced techniques like remote device control, social engineering, and stealthy overlays to steal sensitive data from financial institutions and cryptocurrency platforms. Initially targeting banks in Spain and Turkey, the malware's capabilities are evolving, with experts warning of its potential global expansion and advising users to be cautious of sideloading apps and urgent security warnings.

#Spain #Turkey #CyberAttack #Malware
#SocialEngineering #Financial #Crypto #Android
#MobileApplication
DOI: March 29, 2025
Full Article

Data Breaches, Hacks, and Scams

5,000 CAPTCHA Tests Used as Infostealer Gateways – Do Not Complete Them

Key Insights: The "Morphing Meerkat" phishing campaign uses DNS-over-HTTPS to bypass traditional security filters and create convincing fake login pages tailored to over 110 email providers. Attackers steal credentials by prompting users to enter them on counterfeit sites, then redirect them to the legitimate login page, leaving victims unaware of the theft.

8 Smart Ways Users Can Avoid Getting Phished

1. **Do Not Rush—Pause Before You Click**
Be suspicious of emails that pressure you to act quickly.
If you are unsure, visit the website directly instead of clicking a link in an email.
2. **Use Multi-Factor Authentication**
Always enable MFA on your email, social media, and banking accounts. Even if your password is stolen, MFA can stop attackers from logging in.
3. **Install A Password Manager**
Password managers prevent you from entering your login credentials on fake websites. They will only autofill your credentials on legitimate domains.
4. **Keep Software and Devices Updated**
Regular updates patch security vulnerabilities that attackers exploit. Enable automatic updates for your operating system, browser, and antivirus software.
5. **Use A Trusted DNS Provider with Filtering**
Services like Cloudflare (1.1.1.1 for Families), OpenDNS, or NextDNS provide DNS-level protection and may block known phishing sites.
6. **Block DoH on Your Router (If Possible)**
Some advanced home routers allow you to block encrypted DNS traffic (DoH), which prevents attackers from hiding their phishing domains from your network.
7. **Check URLs Carefully**
Phishing sites often use lookalike URLs. Make sure you are visiting the correct domain (e.g., https://accounts.google.com for Gmail).
8. **Use Anti-Phishing Browser Extensions**
Extensions like uBlock Origin or DuckDuckGo Privacy Essentials can block suspicious scripts and trackers often used in phishing campaigns.

#Phishing #CyberAttack #Scam
DOI: March 28, 2025
Full Article

Scams

Smishing Texts Can Trick You Into Turning Off Your iPhone's Security Protections. Here's Why Replying to Scammers is a Bad Idea

Key Insights: Hackers are targeting iPhone users with a smishing campaign that tricks them into disabling built-in phishing protections by encouraging responses like "STOP" or "Y," which marks the number as trusted. Engaging with these messages can expose users to future attacks, as scammers use responses to identify active numbers and refine their targeting for more sophisticated fraud.

#Hacking #Smishing #Phishing #CyberAttack #Scam #iPhone #Apple
DOI: March 25, 2025
Full Article

New Phishing Attack Uses Real-Time Interception to Bypass 2FA

Key Insights: The Astaroth phishing kit bypasses two-factor authentication by intercepting and manipulating real-time credentials, including session cookies, to gain unauthorized access to accounts. It works as a middleman between the victim's device and legitimate authentication services, making it a highly advanced and stealthy threat that cybercriminals can exploit to steal sensitive data.

#Phishing #CyberAttack #PII
DOI: March 30, 2025
Full Article

U.S. Seizes $8.2 Million in Crypto Linked to 'Romance Baiting'

Key Insights: The U.S. Department of Justice has seized over $8.2 million in stolen USDT cryptocurrency from 'romance baiting' scams, where victims were manipulated into investing in fraudulent platforms with false promises of large returns. The FBI traced the laundered funds, leading to the seizure, which will allow restitution to victims, some of whom lost millions, while also revealing ties to human trafficking syndicates in Cambodia and Myanmar.

#Crypto #Scam
DOI: March 29, 2025
Full Article

Identity & Privacy Issues

Online Privacy

AI Fuels 137% Increase in Sextortion Scams: New Tactics to Watch Out For

Key Insights: Scammers are using artificial intelligence to create personalized scams and AI-generated imagery to extort victims. Sextortion scams targeting Americans increased by 137% in the first few months of 2025 over 2024 figures. Due to their susceptibility to emotional pressure and embarrassment, teenagers are a prime target of sextortion scams utilizing social media and messaging apps.

#ArtificialIntelligence #Scam #SocialMedia #MobileApplication #ChildSafety
DOI: March 26, 2025
Full Article

NSA Warned of Vulnerabilities in Signal App a Month Before Houthi Strike Chat

Key Insights: In February 2025, the NSA issued a bulletin warning its employees about vulnerabilities in the Signal app, highlighting phishing scams that could bypass its encryption and target sensitive information. The bulletin followed a controversy involving Defense Secretary Pete Hegseth, who accidentally shared war plans in a Signal chat, raising concerns about the security of unclassified communication tools despite their approval for senior officials' use.

#Signal #MobileApplication #Phishing #Scam #PII #Cybersecurity
DOI: March 25, 2025
Full Article

Meta Considers Charging for Ad-Free Facebook and Instagram in the UK

Key Insights: Meta is considering launching a paid subscription option in the UK that would remove ads from Facebook and Instagram, allowing users to avoid data tracking. This follows the company's practice in the EU, where users can opt for an ad-free experience for €5.99 (£5) a month. The move comes after Meta's legal settlement with a UK woman and ongoing discussions with the UK data watchdog. Critics argue that this "consent or pay" model could raise data protection concerns, while social media experts believe limited uptake in the UK is likely, as many users would prefer to exchange their data for free access.

#Meta #Facebook #Instagram #UnitedKingdom #AdTech #Privacy #SocialMedia #Cybersecurity #IdentityProtection
DOI: March 24, 2025
Full Article

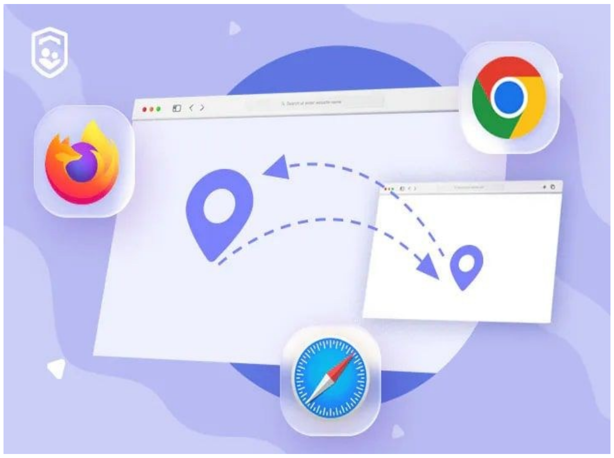
Google Defeats Part of US Shareholder Class Action Over Digital Ads

Key Insights: A federal judge dismissed part of a lawsuit accusing Google of misleading investors about its digital advertising practices and user privacy but allowed the case to proceed regarding a false statement made by CEO Sundar Pichai to Congress in 2020. The shareholders, who sued in 2023, claim Google rigged its ad auctions to favor its platforms, but the judge ruled that the plaintiffs failed to prove Google had the necessary intent to commit securities fraud in certain statements.

#Google #AdTech #Privacy #PrivacyLaw
DOI: March 25, 2025
Full Article

Identity & Privacy Issues

Online Privacy



Prevent Cross-Site Tracking: What It Is and How to Block It

Key Insights: Cross-site tracking allows advertisers to monitor your online activities across websites, creating detailed profiles for targeted ads or sale to data brokers, raising privacy concerns. To protect privacy, users can block third-party cookies, use VPNs, and other privacy tools to control trackers and reduce the risks of sensitive data collection and intrusive ads.

#Technology #AdTech #Privacy #Cybersecurity
DOI: March 27, 2025
Full Article

Security Expert Troy Hunt Lured in by Mailchimp Phish

Key Insights: The creator of the *HaveIBeenPwned* website, which allows users to check whether their email has been part of a data breach, announced that he had fallen victim to a phishing scam resulting in the compromise of his newsletter mailing list. Hunt fell victim to a tailored phishing email that duped him into revealing his Mailchimp username and password.

#Phishing #DataBreach #Scam
DOI: March 26, 2025
Full Article

Dolphin Partner Loti AI Expands Digital Identity Protection to Everyone

Key Insights: Loti AI, in partnership with Dolphin, is now offering its advanced digital identity protection tools to the public, previously available only to celebrities and brands, with both free and premium membership options. The AI-driven technology safeguards digital reputations by quickly removing unauthorized content, such as deepfakes and impersonations, positioning Loti AI as a leader in the growing digital security market.

#Privacy #ArtificialIntelligence #IdentityProtection #Technology #DeepFake
DOI: March 27, 2025
Full Article

Identity & Privacy Issues

Privacy Law

Trump Administration Takes Action to Fight Identity Fraud, Address Concerns Raised by Ways and Means Committee

Key Insights: The Trump Administration announced new steps to improve the Electronic Consent Based Social Security Number Verification system, making it more accessible and effective in combating identity fraud. These changes, which include lowering implementation costs and fees, aim to protect Social Security beneficiaries and improve the integrity of the program, following concerns raised by the Ways and Means Committee.

#IdentityTheft #IdentityProtection #SSN
DOI: March 24, 2025
Full Article

Google and Apple Will Have to Verify Kids' Ages When Downloading Apps Under Newly Signed Utah Law- and Meta is Celebrating

Key Insights: Utah has passed a law requiring app stores like Apple's App Store and Google Play Store to verify children's ages when downloading apps, effective in May. This shift places the responsibility on app stores rather than app publishers to ensure users are 13 or older, particularly for social media apps. While some tech companies, including Meta, have supported the move, industry groups like the Chamber of Progress argue that it could compromise privacy and lead to legal challenges.

#Apple #Google #Meta #MobileApplication #SocialMedia #IdentityProtection #Privacy #ChildSafety
DOI: March 27, 2025
Full Article

Trump Executive Order Seeks to Reform Voting Process; Privacy Issues Are Problematic

Key Insights: President Trump's executive order aims to restore public confidence in U.S. elections by strengthening voter verification, enforcing federal election laws, and ensuring only eligible citizens participate, with a focus on paper ballots, voter ID, and citizenship verification. The order has sparked legal challenges from advocacy groups and concerns over voter privacy, as it mandates stricter voter list maintenance, data sharing, and compliance with federal election standards, including prohibiting foreign contributions and adjusting voter registration processes.

#IdentityProtection #Privacy #PrivacyLaw
DOI: March 26, 2025
Full Article

Judge Says Treasury, Education, OPM Can't Share Personal Information with DOGE

Key Insights: A federal judge ruled that the Office of Personnel Management, Treasury, and Education must stop sharing personal data with the DOGE initiative, citing violations of the Privacy Act. The decision follows a lawsuit over the unauthorized exposure of sensitive information, causing distress to affected individuals.

#Privacy #PrivacyLaw #PII
DOI: March 24, 2025
Full Article

Identity & Privacy Issues

Biometrics

23andMe Files for Bankruptcy as Concerns Erupt Over DNA Biometric Data

Key Insights: 23andMe has filed for bankruptcy following poor sales of its ancestry testing kits, sparking concerns over the security of user data, especially after a 2023 breach exposed millions of personal records. Despite these financial struggles, the company assures that its bankruptcy will not affect how it manages or protects customer data, though experts urge users to delete their accounts to mitigate potential risks.

#Privacy #DataBreach #PII #Cybersecurity #Biometrics
DOI: March 25, 2025
Full Article

23andMe
Welcome to you
saliva collection
23andMe
DNA Testing Firm 23andMe Files for Bankruptcy— 15 Million Customers' Genetic Data Could Be Sold in Auction

Apple Launches Stolen Device Protection Feature for Enhanced iPhone Security

Key Insights: Apple has introduced Stolen Device Protection, a security feature that requires Face ID or Touch ID authentication for sensitive actions when an iPhone is used in unfamiliar locations. This feature also enforces a one-hour security delay for added protection, even if the device is offline, to prevent unauthorized access after theft.

#Apple #Biometrics #IdentityProtection #Technology
DOI: March 29, 2025
Full Article

House Committee Passes "Freedom to Read Act" and Facial Recognition Protections

Key Insights: The House Education Committee passed a bill aimed at protecting biometric data collected by schools, restricting the use of facial recognition technology to specific safety scenarios.
#Biometrics #FacialRecognition #ChildSafety
DOI: March 26, 2025
Full Article

Trust Stamp Patents New Anti-Deepfake Biometric Authentication System for Smartphones

Key Insights: A new technology patented, using an interactive challenge-response mechanism for real-time verification of live users to enhance biometric security against deepfake attacks. The solution does not require specialized hardware, offering a cost-effective way to strengthen biometric authentication against increasing risks of deepfake technology.

#Biometrics #DeepFake #MobileDevice
DOI: March 25, 2025
Full Article

Emerging Technology

Using Defensive AI as a Countermeasure to AI Threats

Key Insights: As cyber risks grow, defensive AI, which uses artificial intelligence and machine learning to enhance security, is emerging as a dynamic solution to combat sophisticated threats. While offering benefits like improved detection and real-time responses, defensive AI also presents challenges, including false positives and integration issues, requiring organizations to carefully choose the right solution for their needs.

#Technology #ArtificialIntelligence #Cybersecurity
DOI: March 24, 2025
Full Article

Microsoft Unveils Microsoft Security Copilot Agents and New Protections for AI

Key Insights: Microsoft is expanding its AI-first security platform with the launch of new AI agents within Microsoft Security Copilot, designed to autonomously handle tasks like phishing triage, vulnerability remediation, and data security, improving efficiency in responding to cyber threats. The company is also enhancing its solutions to secure and govern AI, addressing emerging risks in generative AI, and offering tools for organizations to prevent data leaks, secure AI applications, and strengthen cybersecurity across multicloud environments.

#Microsoft #ArtificialIntelligence #Phishing #Cybersecurity
DOI: March 24, 2025
Full Article

Apple Files a Patent That Advances Optic ID for Vision Pro with Machine Learning, Multiple Illumination Conditions & More

Key Insights: Apple has filed a patent application advancing its Optic ID system for the Vision Pro, integrating machine learning and multiple illumination channels to enhance biometric authentication security. The system uses varying illumination conditions to capture more detailed biometric data, improving accuracy and robustness while reducing computational resources, and may also incorporate additional biometric factors like facial or hand recognition for added security.

#Apple #Biometrics #Cybersecurity #FacialRecognition #Technology
DOI: March 28, 2025
Full Article

Emerging Technology

Cybersecurity & Computing

Scientists Built a Memory Device That Doesn’t Lose Power- and the Implications Are Mind-Blowing

Key Insights: Magnetoresistive RAM offers the potential to replace volatile DRAM by providing non-volatile memory that retains data without power, potentially reducing energy consumption. A recent breakthrough in Japan could enable higher MRAM densities and lower power usage, with the technology likely to first appear in specialized applications before reaching consumer products.

#Technology #Japan
DOI: March 25, 2025
Full Article

Defense Agency Deploys BIO-Key Biometric Security System in Four Days

Key Insights: BIO-key completed a rapid four-day deployment of its biometric-based identity and access management system for a major defense agency, showcasing its expertise in high-security government solutions. This deployment provides the agency with a secure, scalable, passwordless authentication system, highlighting BIO-key's ability to meet urgent operational needs in government security.

#Biometrics #IdentityProtection #Cybersecurity
DOI: March 26, 2025
Full Article

Novel Technique Can Unmask up to 70% of Crooks Hiding Behind VPNs, Proxies, Tor

Key Insights: Researchers from Denmark and India have developed a technique that unmasked cybercriminals hiding behind VPNs, proxies, and Tor browsers with up to 70% reliability. By leveraging honeypots and Canary tokens embedded in files or URLs, the method captures attackers' real IP addresses and metadata when they interact with bait. This technique outperforms traditional methods like traffic analysis and protocol fingerprinting, offering higher success rates and aiding cybersecurity efforts in identifying and mitigating threats.

#Denmark #India #Technology #Cybersecurity
DOI: March 27, 2025
Full Article

Wearable Computing Goes Woven, Wireless, and Washable

Key Insights: A new research project has introduced "fiber computers" embedded into textiles, creating washable, flexible, and wireless wearable computing systems that can monitor health and activity with minimal power usage. These fiber computers, each containing standard components like microcontrollers, sensors, and batteries, communicate wirelessly to form a distributed network, offering a novel solution for unobtrusive, durable, and washable wearable technology.

#Technology #Computer
DOI: March 24, 2025
Full Article