San Diego Regional Cyber Lab

Protecting AI: Federal Agencies Release Cybersecurity Best Practices

During the Cyber Lab's upcoming executive stakeholder call on June 12, attendees will be discussing a variety of critical cybersecurity issues, including the growing risks associated with artificial intelligence (AI). As AI systems become more deeply embedded in organizational infrastructure, the importance of securing the data that powers these technologies cannot be overstated. Recognizing this urgency, the FBI, NSA, CISA, and several international partners have released a joint Cybersecurity Information Sheet titled "Securing the Data for Artificial Intelligence Systems." The guidance outlines comprehensive recommendations to help organizations protect the confidentiality, integrity, and reliability of AI systems throughout their lifecycle.

The publication highlights that AI is only as trustworthy as the data it consumes. Without strong safeguards, that data becomes vulnerable to threats such as data poisoning, insider manipulation, and compromised third-party sources. To mitigate these risks, the information sheet recommends encrypting data in transit and at rest, verifying integrity using cryptographic hashes and digital signatures, and applying Zero Trust principles across AI environments. It also encourages classifying data by sensitivity, adopting secure storage practices, and using privacy-preserving techniques like federated learning and differential privacy. These measures aim to ensure that AI systems are both resilient and ethical in the face of rapidly evolving cyber threats.

A particularly concerning issue is data drift, which occurs when input data changes over time, potentially weakening model accuracy. The guidance stresses the importance of routine performance monitoring, regular model updates, and adaptive learning strategies to maintain reliability. As cyber threats become more sophisticated, the report serves as a timely reminder that safeguarding AI isn't just about protecting algorithms—it requires robust data governance and proactive cybersecurity hygiene. By following these best practices, organizations can strengthen trust in their AI systems and reduce the risks that come with deploying emerging technologies in critical environments.

To view the full document, click here.

Upcoming Events:

- *Quarterly Executive Stakeholder Committee Meeting (6/12)*
- *Quarterly Technical Stakeholder Committee Meeting (6/26)*

In This Issue

Upcoming Events:

San Diego Cyber Group

When: Tuesday, June 10, 2025 | 5:00 PM - 7:00 PM PDT

Where: Eppig Brewing North County Vista Tasting Room | 1347 Keystone Way Ste C Vista, CA

Click here for details

DEF CON San Diego - Monthly Meeting

When: Wednesday, June 11, 2025 | 6:00 - 8:00pm

Where: Round Table Pizza 16761 Bernardo Center Dr, San Diego, CA 92128 (Upstairs Dining Area)

Click here for details

ISACA SD June Meeting

When: Thursday, June 19, 2025 | 12:00 PM - 1:15 PM

Where: 12225 El Camino RealSan Diego, CA, 92130

Click here for details

San Diego Cyber Group

When: Wednesday, July 25, 2025 | 6:00 PM - 8:00 PM

Where: Novo Brazil Brewing Mission Valley | 1640 Camino Del Rio N suite 341 · San Diego, CA

Click here for details

Google Rolls Out Passkeys as Default Sign-In Option

Google is automatically enrolling users into its Passkey system to reduce reliance on traditional passwords. This affects platforms like Gmail, Google Drive, and YouTube.

What Are Passkeys?
Passkeys are digital credentials that let users sign in using biometrics (like Face ID or fingerprint) or a device PIN instead of a password. Stored locally and unique to each account, passkeys are more secure than traditional methods.

Why It Matters

- **Stronger Security** – Passkeys use public key cryptography, preventing phishing and credential stuffing.
- **Simplified Sign-In** – Users authenticate using their device's unlock method.
- **Local Storage** – No plaintext passwords in the cloud, lowering breach risk.

Testing the Feature

Users who are interested in experiencing the new system can visit Google's official passkey demo here.

The site allows users to test passkey functionality and determine whether their devices are compatible.

ISACA San Diego Empowers Cybersecurity

ISACA San Diego Chapter is proud to serve over 900 members from across America's Finest City's cybersecurity, audit, risk, and IT governance communities. ISACA's global mission is to advance the professional practice of information systems governance and ensure trust in an ever-evolving digital world.

ISACA San Diego offers professional workshops and monthly speaking engagements on emerging topics such as AI in cybersecurity/audit and career advancement, all of which are free to the public. Our organizational mission is to build a diverse and informed cybersecurity workforce in the region and support both seasoned professionals and those new to the field.

Collaboration across sectors will be required to meet today's cybersecurity challenges such as the rise of AI-enabled threats, the evolving risk landscape, and a rapidly shifting use of technology. ISACA San Diego invites all who are passionate about cybersecurity and technology audit: attend events, provide or receive mentorship, and continuously learn. ISACA San Diego also sponsors professional membership for students, reach out for more information!

Upcoming events include sessions on AI Risk Management, Cybersecurity Resilience and Security Awareness and extended workshops on API Security and CMMC Compliance within the Cloud.

Together, we are creating a stronger, safer digital future and looking forward to your participation! Learn more at https://isaca-sd.org.

Trust But Verify: Code on TikTok

In a disturbing new trend, threat actors have turned to TikTok to spread information-stealing malware such as Vidar and StealC. According to Trend Research, these cybercriminals are leveraging the platform's viral reach and AI-generated content to post videos that instruct users—especially teens and young adults—on how to run seemingly harmless PowerShell commands. Posing as activation guides for pirated software like Spotify, Microsoft Office, or CapCut, the videos have garnered hundreds of thousands of views, making the attack both scalable and alarmingly effective.

This method bypasses traditional detection by relying solely on audio-visual instruction rather than embedding malicious code within TikTok itself. As a result, many viewers may not realize they're being manipulated into infecting their own devices. Parents of teens and educators should be particularly vigilant, as young users are more likely to trust and engage with platform content. For aspiring cybersecurity professionals and students transitioning into the field, this campaign is a critical reminder that cyber hygiene must extend beyond email and website filters—it now includes the content we casually scroll through on social media.

Preventive measures include actively discussing the risks of downloading pirated software or following unsolicited tech advice from social media. Encourage teens and new cybersecurity learners to verify all software sources, avoid executing unknown commands, and stay informed through trusted threat intelligence channels. For institutions and employers, consider expanding awareness training to include emerging threats from visual social engineering, reinforcing skepticism, and teaching users how to recognize manipulative cues in online videos. The rise of AI-generated deception makes it more urgent than ever to think before you click—or in this case, type.

For more click here.

Scam Alert: QR Codes in Unsolicited Packages

A new wave of phishing scams is emerging, where victims receive unexpected packages labeled as gifts. Inside, a note urges the recipient to scan a QR code—often claiming it will reveal the sender's identity or provide return instructions. In reality, these codes may lead to phishing sites that steal personal information or install malware.

If you didn't expect the package, don't scan the code. These scams are part of a tactic known as "brushing," where fake deliveries are used to manipulate online reviews or lure people into disclosing private data.

If you already scanned a suspicious code or entered information on a linked site, change your passwords immediately and enable two-factor authentication. It's also wise to check your credit report at AnnualCreditReport.com and monitor bank statements for unfamiliar activity.

According to U.S. law, unsolicited packages can be kept, but treat unknown QR codes as red flags. For more information or to report identity theft, visit IdentityTheft.gov.

For more click here.

Unsecured Database Leaks 184M Records

Data breaches are no longer isolated events—they are a persistent threat across industries. A recent discovery by cybersecurity researcher Jeremiah Fowler highlights how vulnerable systems still are. During a routine scan, Fowler uncovered an unprotected database with over 184 million account credentials in plain text. These included emails, usernames, and passwords tied to platforms like Google, Microsoft, Apple, as well as financial and government services.

The database required no authentication or encryption. Anyone with the link could access the data instantly. Fowler believes the information was collected using an "infostealer," a tool used by cybercriminals to extract login details from infected devices.

While the file was removed after Fowler's report, the database owner remains unknown. The breach reveals how some organizations still fail to apply basic cybersecurity protections. Several individuals confirmed their information was accurate, making the breach more than just a statistic.

Experts urge users to take proactive steps: use strong, unique passwords, enable two-factor authentication, watch for unusual activity, and update software regularly. Tools like password managers and data removal services can also help reduce risk.

This incident reminds us that cybersecurity is a shared responsibility—both organizations and users must act to protect sensitive data.

For more click here.

San Diego Regional Cyber Lab
1200 Third Avenue, Suite 1800
San Diego, CA 92101
http://www.sandiego.gov/cyber-lab

SAN DIEGO REGIONAL CYBER LAB

New Offerings at the San Diego Regional Cyber Lab

We're expanding hands-on cybersecurity training and tools at the San Diego Regional Cyber Lab. Here's what's available:

- **Pluralsight** – On-demand technical courses covering cybersecurity, IT, software development, and more.
- **Burp Suite Pro** – Professional-grade web application testing tools to practice real-world security testing.
- **Haiku Cyber Range** *(Coming Soon)* – Custom-built cyber ranges launching in about two months to simulate various attack/defense scenarios.
- **Digital Forensics Playbooks** – Hands-on training with forensic tools like the UltraDock and TX1 Imager, guided by easy-to-follow playbooks.

LinkedIn

Contact Us

SDRCL Program Lead
Ian Brazill
IBrazill@sandiego.gov

SDRCL Cyber Lead
Brendan Daly
BMDaly@sandiego.gov

Cyber Center of Excellence (CCOE), Community Partner
Lisa Easterly
Lisa.easterly@sdccoe.org