San Diego Regional Cyber Lab

Hacking & Smacking: SDRCL Pioneers Free Forensic Training for the Next Generation of Cybersecurity Professionals

We proudly support Hacking & Smacking, an all-female capstone team from National University, led by our intern Bianca Arce, and secondary-lead Callie Gardunio. This team of Navy veterans is developing user-friendly playbooks for forensic tools like the USB 3.1 Writeblocker, Forensic Ultra Dock, Forensic Duplicator, and TX1 Forensic Imager at the San Diego Regional Cyber Lab (SDRCL). Their goal is to provide students with hands-on experience to prepare them for cybersecurity careers.

Recognizing the significant skills gap in the cybersecurity field, especially in digital forensics, SDRCL took the initiative to bridge this gap by offering free training sessions. The goal is to give students practical, real-world experience with the tools they'll use in the workforce.

Thanks to Hacking & Smacking, SDRCL will be the first in the nation to offer free, hands-on training with forensic tools, empowering the next generation of cybersecurity professionals!

This initiative benefits current students and sets the foundation for future collaborations, creating a sustainable model for hands-on forensic training in the cybersecurity field.

Upcoming Events:

- *Quarterly Executive Stakeholder Committee Meeting (3/13)*
- *Quarterly Technical Stakeholder Committee Meeting (3/20)*

In This Issue

Level Up Your Cybersecurity Game: Must-Attend Events in March!

March is full of must-attend cybersecurity events in San Diego! Network, learn, and connect with industry pros and fellow enthusiasts—don't miss out!

ISACA San Diego

When: Thursday, March 20, 12:00pm - 1:15pm

Where: 12225 El Camino Real San Diego, CA, 92130 or Online

Why: Join experts to learn how to strengthen security and mitigate risks, including using AI.

Cost: Non-Member Returning; $15

To register click here.

WiCyS 2025 Cyber Speakers

When: Saturday, March 22, 10am - 12pm. Doors at 9:30am

Where: 4820 Eastgate Mall San Diego, CA 92121

Why: Learn to hack IoT devices safely in this hands-on session.

Cost: Free

To register click here.

San Diego Cyber Group Meetup

When: Wednesday, March 26, 6:00pm

Where: Novo Brazil Brewing, Mission Valley

Why: Casual networking event for cybersecurity professionals & enthusiasts.

Cost: Free

To register click here.

Unlock Your Cybersecurity Potential at BSides San Diego 2025!

BSides San Diego is a must-attend event for cybersecurity professionals looking to learn, network, and stay ahead of industry trends. This annual conference features insightful talks, hands-on workshops, and opportunities to connect with experts.

The event takes place on Saturday, March 29, 2025, from 8:30 AM to 10:00 PM at San Diego State University. Attendees can enjoy engaging talks, interactive training, and exciting giveaways. Tickets range from $15.00 to $290.00 and are available now.

Join BSides San Diego to hear from top speakers, gain practical skills, and explore the latest cybersecurity solutions—all while growing your network and career. Whether you're a seasoned professional or just starting out, this event offers something for everyone. Don't miss the chance to engage with cutting-edge security topics and innovative ideas. Secure your spot today and be part of the thriving cybersecurity community!

This is a unique opportunity to meet like-minded professionals and exchange ideas in a collaborative environment. With hands-on learning and real-world case studies, you'll leave with valuable insights to enhance your skills. Experience the excitement of BSides San Diego and take your cybersecurity expertise to the next level!

For more information click here.

San Diego Parking Scam Alert

The City of San Diego is warning residents about a new scam impersonating a City webpage and requesting payment for fake parking citations. Scammers are sending text messages with phony ticket notifications and a fraudulent payment link. Please do not use that link to make any citation payment.

The City's cybersecurity team and the San Diego Police Department are working to shut down the fraudulent page and find those responsible. If you receive one of these scam texts, you are asked to report it.

This latest fraud attempt follows a similar scam from last January. Residents are urged to remain vigilant, as scammers may attempt to create new fraudulent sites. The City reminds the public that official parking citations will never be issued via text message, nor will the City request payment through an unsolicited text.

Stay Safe. Do not click links or enter personal/payment info.

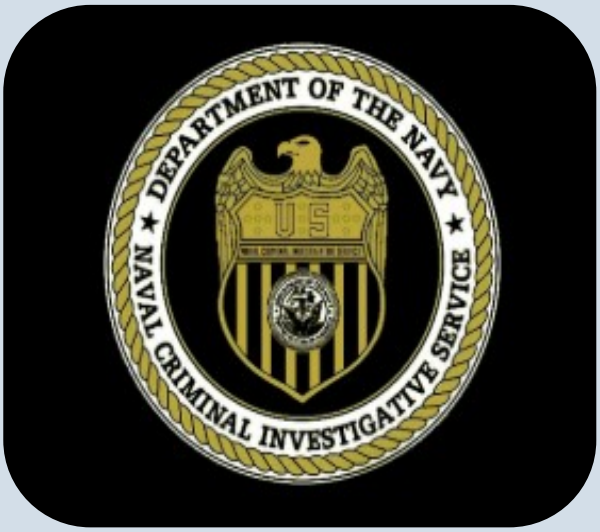
Verify citations at sandiego.gov/parking/citations or call 866-470-1308 (Mon-Fri, 9 AM-4 PM).

Report scams to reportfraud.ftc.gov and cybersecurity@sandiego.gov.

The City is committed to protecting residents—report suspicious messages and stay informed on cybersecurity best practices.

NCIS: Hiring Skilled Professionals for Critical Investigations

Join the Naval Criminal Investigative Service (NCIS), the civilian Federal law enforcement agency within the Department of the Navy, responsible for investigating felony crimes, preventing terrorism, and safeguarding secrets for the Navy and Marine Corps. NCIS combats threats to national security across intelligence, terrorism, and criminal spectrums by conducting operations and investigations ashore, afloat, and in cyberspace.



At NCIS, you'll have the opportunity to enjoy a rewarding career with competitive salary, retirement benefits, health coverage, and global opportunities. Work in a supportive environment with continuous training and a comprehensive benefits package.

Become a Special Agent or Intelligence Specialist to confront global criminal, counterterrorism, and counterintelligence threats. Special Agents undergo extensive training at the Federal Law Enforcement Training Center (FLETC), with opportunities for further specialized development. Intelligence Specialists analyze critical data to protect the Department of the Navy's personnel and assets worldwide.

NCIS also offers a variety of competitive Federal positions in fields such as Computer Science, Forensics, HR, IT, and Financial Administration.

To qualify, you must be a U.S. citizen (born or naturalized) with a valid driver's license, pass a background check, and obtain the necessary security clearance (Secret or Top Secret with SCI eligibility). Strong communication skills are essential, and additional qualifications may vary by position. Make a difference in national security with NCIS!

NCIS posts vacancy announcements on USAJOBS every April and October. At the bottom of the announcement, you'll be redirected to SalesForce, their commercial platform for tracking applicants. The portal allows you to create a profile and upload necessary documents, but it will only be accessible during the announcement window.

To find out more about how your skills best fit at NCIS, contact us at NCIScareers@NCIS.NAVY.MIL or visit our website at WWW. NCIS.NAVY.MIL .Most NCIS job announcements are posted to www.usajobs.gov

Protecting Against Fraudulent Tap-to-Pay Transactions: Prevention Tips for Consumers

Fraudulent tap-to-pay transactions in New York State (NYS) involve criminals using a mobile app to temporarily force payment terminals into offline mode. This bypasses regular approval procedures, allowing fraudsters to use stolen, fake, or cloned credit card information to make purchases. Fraud teams often target multiple vendors in one day, moving along highways and exploiting vulnerabilities in payment systems.

The technology behind this fraud relies on NFC (Near Field Communication), which allows contactless payments through credit/debit cards or mobile apps linked to digital wallets. Payment terminals typically depend on an internet connection to approve transactions, and when this connection is disrupted, it opens a window for fraudsters to act. Malicious Android APK files enabling this fraud are often bought on the dark web or through encrypted messaging services.

To prevent fraudulent tap-to-pay transactions, individuals should monitor their bank and credit card statements for unauthorized activity. Enabling transaction alerts can help detect suspicious activity early. Using strong, unique passwords for mobile payment apps, enabling multi-factor authentication, keeping devices updated with security patches, and avoiding untrusted app downloads can reduce the risk of fraud.

Law enforcement investigating these cases should gather details on payment terminals, payment service providers, transaction patterns, and mobile apps used. Retail vendors suspecting fraud should report incidents to local law enforcement or the FBI's Internet Crime Complaint Center (IC3). For further assistance, the NYSIC Intelligence & Analysis Unit and Cyber Analysis Unit are available.

Join WiCyS – Your Gateway to a Thriving Cybersecurity Career!

Are you ready to break into cybersecurity and connect with a powerful network of women leading the industry? Women in CyberSecurity (WiCyS) is the go-to organization for aspiring and experienced professionals looking to grow, learn, and succeed in this dynamic field. Whether you're a student, a career changer, or a seasoned expert, WiCyS provides the resources, mentorship, and community you need to advance in cybersecurity.

As a WiCyS member, you'll gain access to exclusive scholarships, training programs, career fairs, and an annual conference where top companies are actively recruiting talent. Plus, you'll be surrounded by a supportive community of like-minded women and allies who are committed to helping you thrive. Don't wait—join WiCyS today and take the next step toward an exciting and rewarding cybersecurity career!

For more info 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

Cybersecurity Assistance Service Program (CASP)

The NCSR is now closed for end-user submissions. However, the Cybersecurity Assistance Service Program (CASP) has a new security assessment service that you can complete at any time. It offers a series of meetings between an advisor and a member to complete an assessment such as the NCSR.

This service provides expertise and context to complete a security assessment, guiding members on identifying the areas with the most need for improvement. You can schedule a gap analysis meeting to discuss NCSR results and recommended next steps after completion.

Please email CASP@cisecurity.org to request the Security Assessment Service or click here for more info.

LinkedIn

Contact Us

SDRCL Program Lead
Ian Brazill
IBrazill@sandiego.gov

SDRCL Cyber Lead
Brendan Daly
BMDaly@sandiego.gov

SDRCL Cyber Intern
Bianca Arce
BArce@sandiego.gov

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