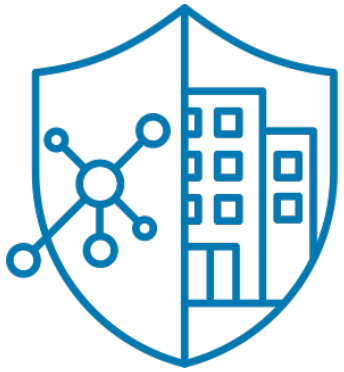
SECURITY LEADERSHIP WEBINAR SERIES #2

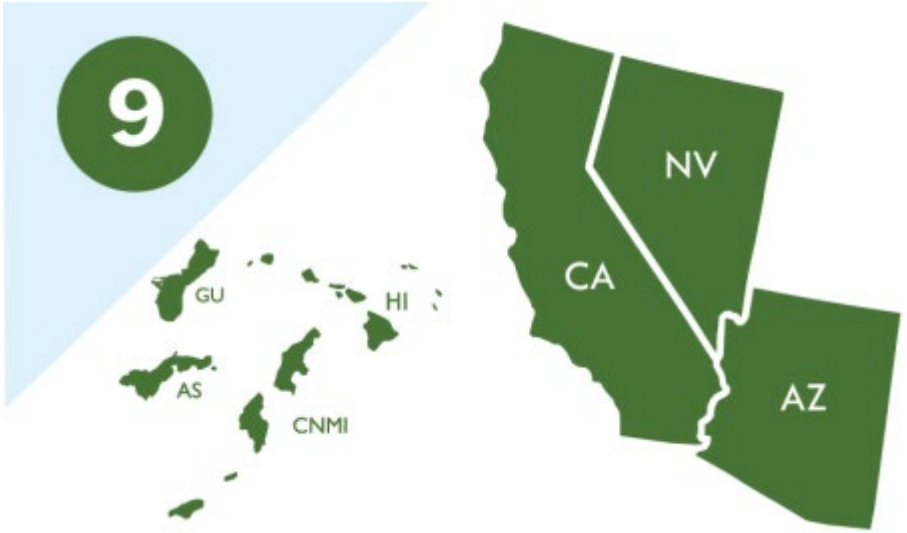
Jennilyn Labrunda
Cybersecurity Advisor, Region 9
March 05, 2024

CISA Mission and Vision

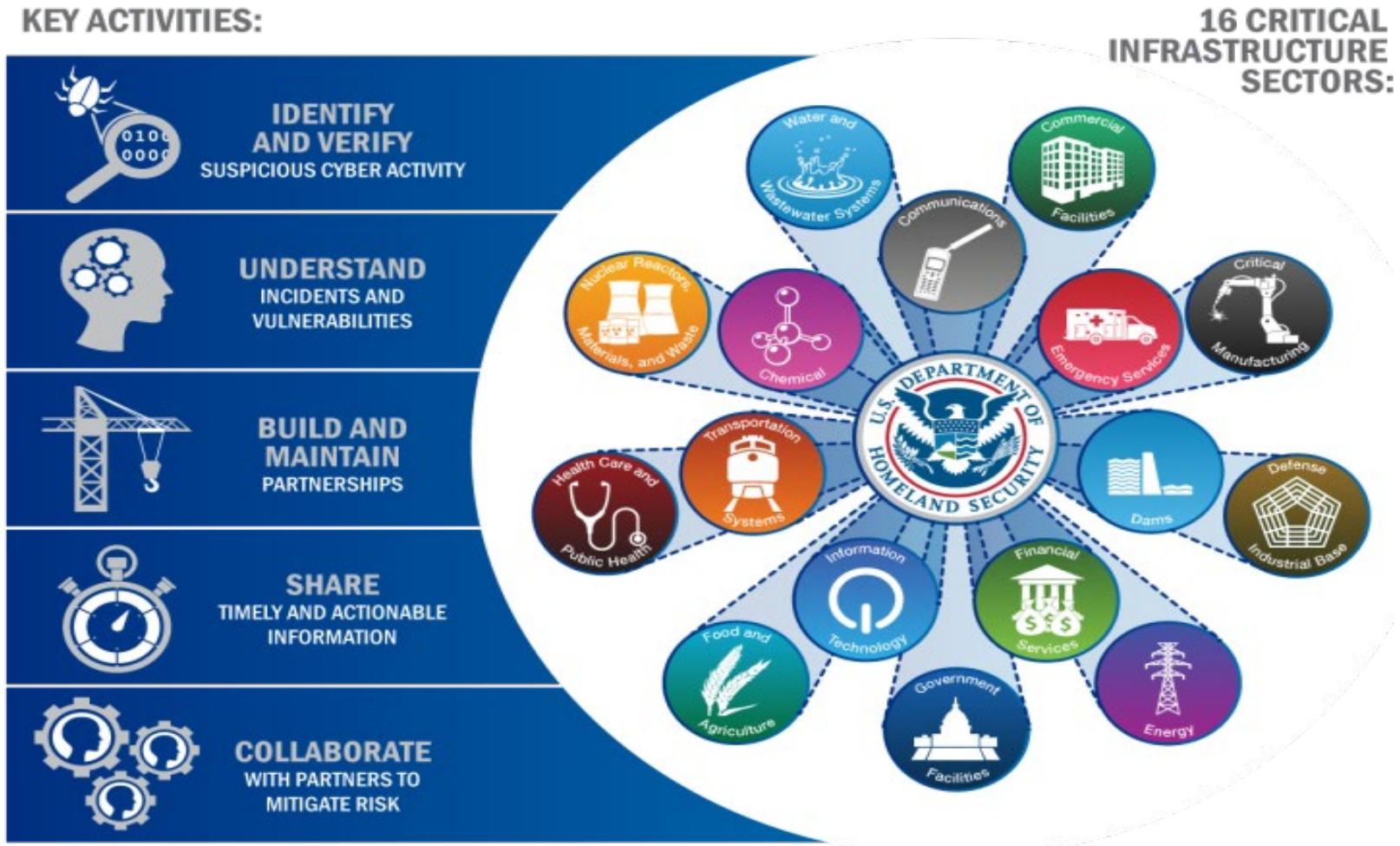
Our **mission** is to lead the national effort to understand, manage, and reduce risk to our nation's cyber and physical infrastructure.

Our **vision** is a secure and resilient critical infrastructure for the American people.





Serving 16 Critical Infrastructure



Topics

- What is Security Leadership
  - Qualities and responsibilities
  - Why is it important?
- Risk Management
  - Prioritizing Risks and Threats
  - CISA resources
- Cybersecurity Culture
  - Best practices for building a strong cybersecurity culture
  - Phishing statistics
  - Training resources

WHAT IS SECURITY LEADERSHIP?

Qualities

- Interpersonal skills
- Responsive
- Risk management
- Governance
- Honesty and integrity
- Common titles:
  - **CISO** (Chief Information Security Officer),

CSO (Chief Security Officer), **ISSM/O** (Information Systems Security Manager/Officer), Cybersecurity Director/Manager, and Information Security Director/Manager

Responsibilities

- Developing and implementing a Cybersecurity strategy
  - Risk assessment: identifying and analyzing potential cybersecurity threats & vulnerabilities
  - Deployed effectively throughout the organization; regular monitoring and adjustment
- Building a cybersecurity culture
  - Awareness and training
  - Security is everyone's responsibility
- Managing threats and Incident Response
  - Detection & prevention
  - Incident response planning & execution
- Aligning Cybersecurity with Business goals

Why is Security leadership important?

- Escalating cyber threats
- Compliance and legal requirements
- Business continuity
- Innovation and growth
- Collaboration and communication

RISK MANAGEMENT

Prioritizing Risks and Threats

- Assess your risks (CISA Cybersecurity Performance Goals – CPG)
- Assess your vendors and 3rd party risks
- Stay informed with emergent risks
- Stay compliant with regulations and legal obligations
- Increase your resilience to Cyberattacks

Cybersecurity Performance Goals (CPG)

- Prioritized subset of IT and OT cybersecurity practices; 38 questions
- Reduce likelihood and impact of known risks and adversaries
- Identify areas for potential future investment
- Aligns with the NIST Cybersecurity Framework functions: identify, protect, detect, respond, and recover.
- CSET (**C**yber**S**ecurity **E**valuation **T**ool)
  - https://github.com/cisagov/cset/releases

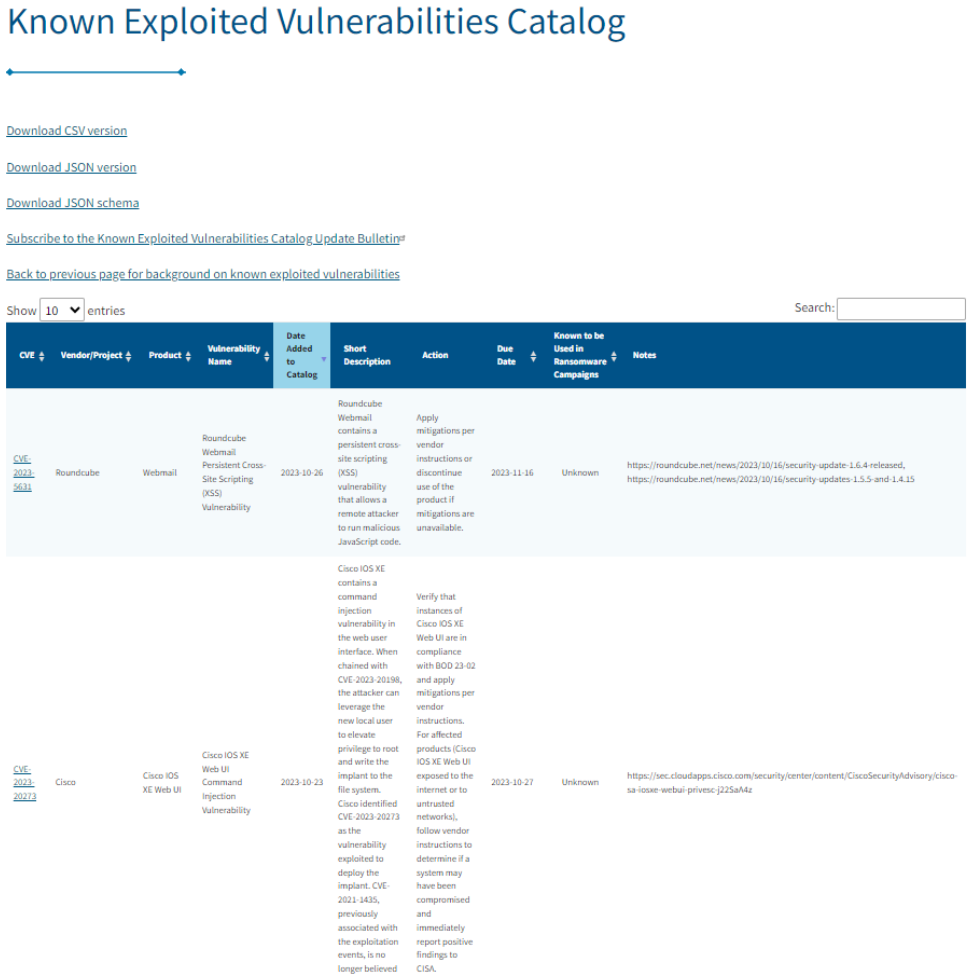
https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

CISA's KEV Catalog

CISA Known Exploited Vulnerabilities (KEV) Catalog

List of Vulnerabilities exploited by cybercriminals in recent attacks

https://www.cisa.gov/known-exploited-vulnerabilities-catalog



Known Exploited Vulnerabilities Catalog

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

Show 10 entries Search:

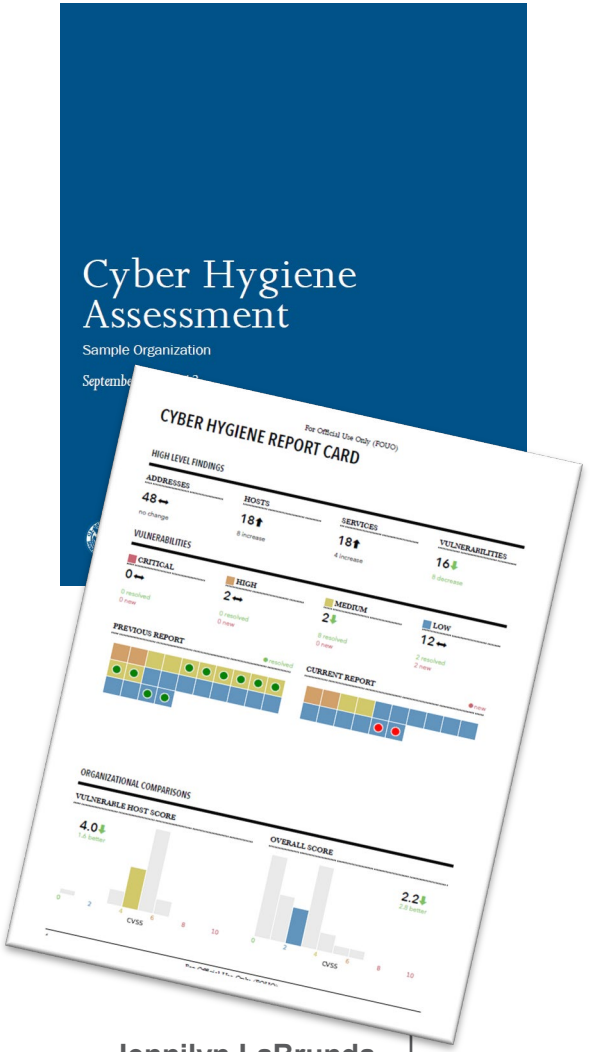
CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Known to be Used in Ransomware Campaigns	Notes
CVE-2023-5631	Roundcube	Webmail	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	2023-10-26	Roundcube Webmail contains a persistent cross-site scripting (XSS) vulnerability that allows a remote attacker to run malicious JavaScript code.	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.	2023-11-16	Unknown	https://roundcube.net/news/2023/10/16/security-update-1.6.4-released, https://roundcube.net/news/2023/10/16/security-updates-1.5.5-and-1.4.15
CVE-2023-20273	Cisco	Cisco IOS XE Web UI	Cisco IOS XE Web UI Command Injection Vulnerability	2023-10-23	Cisco IOS XE contains a command injection vulnerability in the web user interface. When chained with CVE-2023-20198, the attacker can leverage the new local user to elevate privilege to root and write the implant to the file system. Cisco identified CVE-2023-20273 as the vulnerability exploited to deploy the implant. CVE-2021-1435, previously associated with the exploitation events, is no longer believed	Verify that instances of Cisco IOS XE Web UI are in compliance with BOD 23-02 and apply mitigations per vendor instructions. For affected products (Cisco IOS XE Web UI exposed to the internet or to untrusted networks), follow vendor instructions to determine if a system may have been compromised and immediately report positive findings to CISA.	2023-10-27	Unknown	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Cyber Hygiene Vulnerability scanning

- Evaluates external network presence through continuous scans of public, static IPv4s

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities
- Email vulnerability@cisa.dhs.gov with subject line "Requesting Cyber Hygiene Services"



https://www.cisa.gov/cyber-hygiene-services

Information Sharing & Analysis Center

- Information Sharing and Analysis Center (ISAC)
- National Council of ISACs
  - FS-ISAC (Financial Services)
  - H-ISAC (Healthcare)
  - IT-ISAC (Information Technology)
  - MS-ISAC (Multi-state; State, Local, Tribal and Territorial governments)

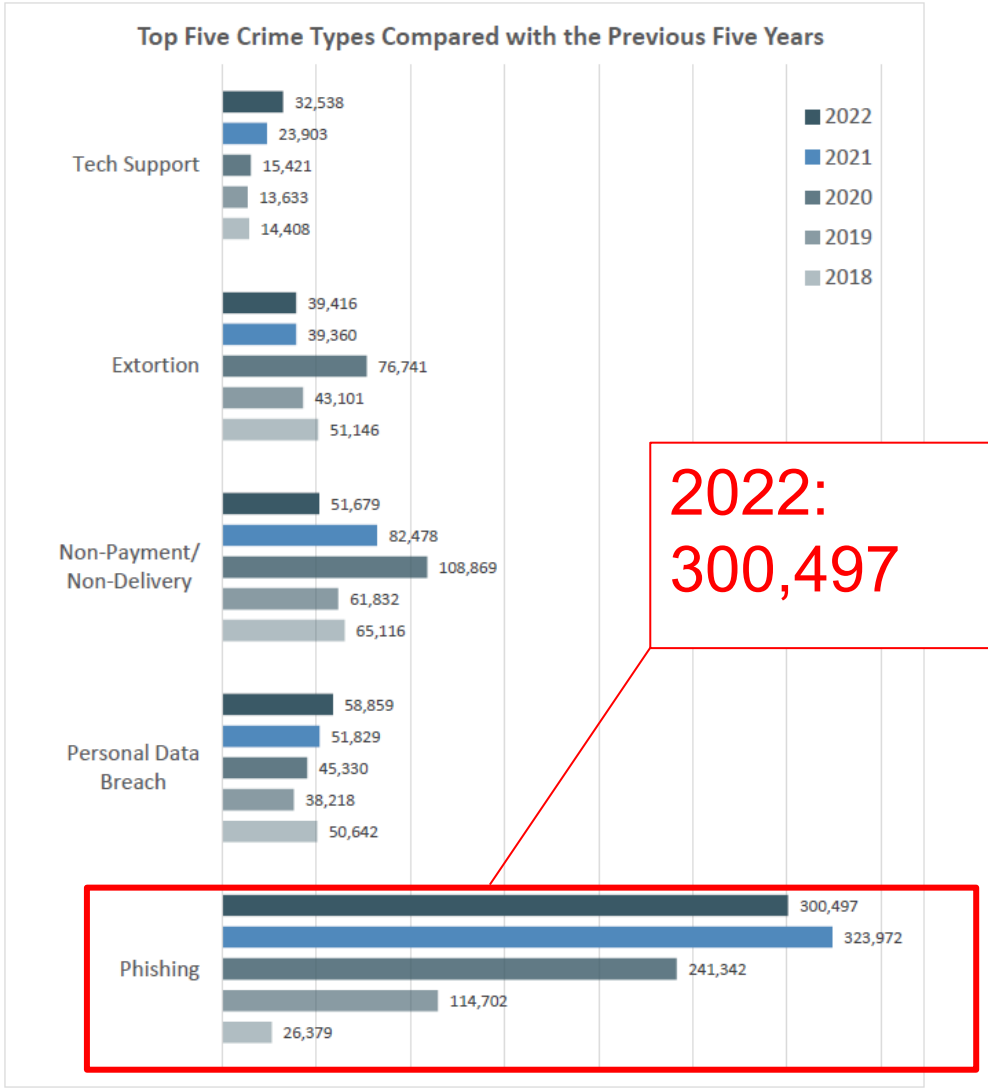
https://www.nationalisacs.org/

CYBERSECURITY CULTURE

Building a Strong Cybersecurity Culture

- Use basic cybersecurity training
- Identify available cybersecurity training resources
- Stay current on cybersecurity events and incidents
- Align cybersecurity practices with organization's values and goals
- Encourage employees to make good choices online and learn about risks like phishing and business email compromise
- Consider appointing a **Cybersecurity leader** who will champion a strong Cybersecurity culture and lead the way to a mature cybersecurity posture

Phishing statistics



2022:
300,497

OVERALL STATE STATISTICS continued

Total Victim Losses by State*

Rank	State	Loss	Rank	State	Loss
1	California	$2,012,806,866	30	Kansas	$58,149,297
2	Florida	$844,972,494	31	Kentucky	$57,045,801
3	New York	$777,099,358	32	Louisiana	$55,696,565
4	Texas	$763,140,903	33	South Dakota	$48,072,730
5	Georgia	$322,638,566	34	Puerto Rico	$47,424,485
6	New Jersey	$284,590,029	35	Arkansas	$46,230,114
7	Illinois	$266,742,489	36	Iowa	$42,806,846
8	Pennsylvania	$250,903,241	37	Delaware	$40,980,800
9	Alabama	$247,930,058	38	Idaho	$40,323,594
10	Arizona	$241,191,959	39	Hawaii	$35,776,983
11	Washington	$240,923,860	40	District of Columbia	$33,668,057
12	Massachusetts	$226,202,504	41	New Mexico	$32,941,959
13	Maryland	$217,880,447	42	New Hampshire	$29,322,824
14	Virginia	$205,462,224	43	Nebraska	$28,659,814
15	Ohio	$180,091,279	44	Mississippi	$28,213,583
16	Colorado	$178,389,862	45	Montana	$22,252,737
17	Michigan	$177,865,280	46	Rhode Island	$21,827,037
18	North Carolina	$175,454,536	47	Maine	$21,403,477
19	Nevada	$127,315,394	48	West Virginia	$18,200,401
20	Missouri	$118,365,728	49	Wyoming	$17,980,141
21	Tennessee	$113,713,897	50	Alaska	$16,826,999
22	Oregon	$109,917,253	51	Vermont	$15,664,834
23	Wisconsin	$108,909,445	52	North Dakota	$14,279,199
24	Minnesota	$103,771,677	53	Guam	$2,712,088
25	South Carolina	$100,256,530	54	Northern Mariana Islands	$1,950,513
26	Connecticut	$99,937,935	55	U.S. Minor Outlying Islands	$960,281
27	Utah	$98,840,388	56	Virgin Islands, U.S.	$826,913
28	Indiana	$73,678,120	57	American Samoa	$127,716
29	Oklahoma	$66,517,159			

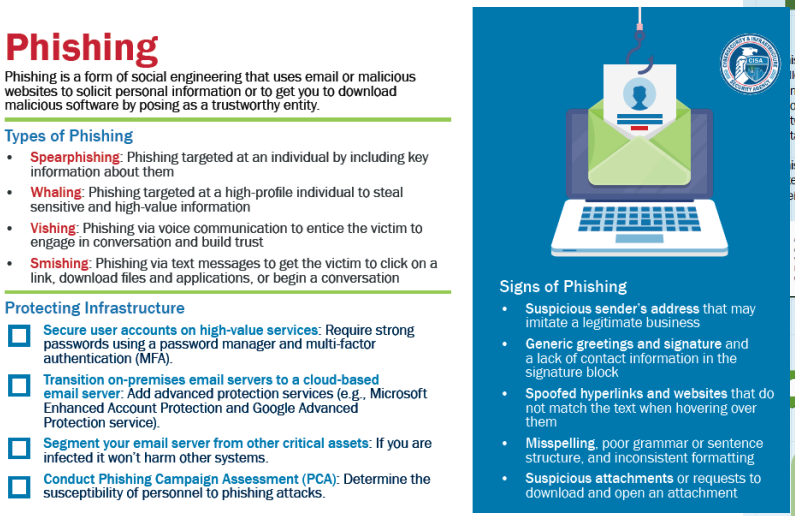
*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

#39 Hawaii:
$35,776,983

#53 Guam:
$2,712,088

Phishing - resources

- Identify available training resources and train employees how to spot phishing
- Alert employees to the risks
- Develop a culture of awareness



Phishing

Phishing is a form of social engineering that uses email or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity.

Types of Phishing

- **Spearphishing**: Phishing targeted at an individual by including key information about them
- **Whaling**: Phishing targeted at a high-profile individual to steal sensitive and high-value information
- **Vishing**: Phishing via voice communication to entice the victim to engage in conversation and build trust
- **Smishing**: Phishing via text messages to get the victim to click on a link, download files and applications, or begin a conversation

Protecting Infrastructure

- **Secure user accounts on high-value services**: Require strong passwords using a password manager and multi-factor authentication (MFA).
- **Transition on-premises email servers to a cloud-based email server**: Add advanced protection services (e.g., Microsoft Enhanced Account Protection and Google Advanced Protection service).
- **Segment your email server from other critical assets**: If you are infected it won't harm other systems.
- **Conduct Phishing Campaign Assessment (PCA)**: Determine the susceptibility of personnel to phishing attacks.

Signs of Phishing

- **Suspicious sender's address** that may imitate a legitimate business
- **Generic greetings and signature** and a lack of contact information in the signature block
- **Spoofed hyperlinks and websites** that do not match the text when hovering over them
- **Misspelling**, poor grammar or sentence structure, and inconsistent formatting
- **Suspicious attachments** or requests to download and open an attachment

4 ACTIONS TO HELP PREVENT BEING HOOKED IN A PHISHING ATTACK

ishing is a form of social engineering in which a cyber threat actor poses as a trustworthy
league, acquaintance, or organization to lure a victim into providing sensitive information
network access. The lures can come in the form of an email, text message, or even a
one call. If successful, this technique could enable threat actors to gain initial access to a
twork and affect the targeted organization and related third parties. The result can be a
ta breach, data or service loss, identity fraud, malware infection, or ransomware.

ishing susceptibility is the likelihood of an individual becoming a victim of a phishing
empt. High susceptibility increases the likelihood that cyber threat actors can exploit
ir target.

Analysis and findings presented in this infographic are derived from phishing-related data collected during CISA Assessments. CISA conducts cybersecurity assessments for federal and critical infrastructure partners to reduce their vulnerability exposure and risk of compromise. To learn more about CISA services, contact central@cisa.dhs.gov. For additional information on steps to reduce your phishing susceptibility and cybersecurity risk, see CISA's Cross-Sector Cybersecurity Performance Goals (CPG).

BLOCK THE BAIT

Implement strong network border protections—as an initial barrier to reduce the opportunity for a successful phishing attempt to further its damage.

Configure email servers to utilize protocols designed to verify the legitimacy of email communications, like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) [CPG 8.3].

https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-education-career-development

https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

https://www.cisa.gov/audiences/small-and-medium-businesses

https://www.stopthinkconnect.org/

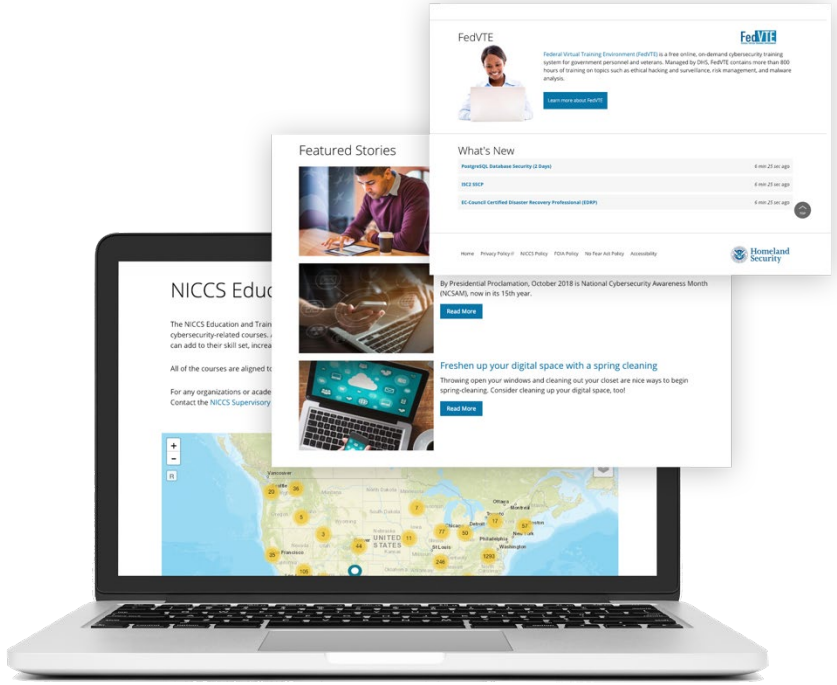
Jennilyn LaBrunda
March 6, 2024

Cybersecurity Training

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Cybersecurity education and training resource
- Workforce Framework for Cybersecurity
- Upcoming cybersecurity events list



https://niccs.cisa.gov/

Cybersecurity Training

FedVTE enables cyber professionals to continue growing skills.

FedVTE is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees.

- Quarterly catalog of existing and future courses
- Courses for all proficiency levels (beginner to advanced)
- Certification prep courses
- Select courses available to the general public

FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

https://fedvte.usalearning.gov/

Visit www.CISA.gov for more information.

Jennilyn LaBrunda
Cybersecurity Advisor, Guam/CNMI/AS
Jennilyn.Labrunda@cisa.dhs.gov
808-260-3143


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY