

TRAINING GUIDE

SLTT GOVERNMENTS

Recommended cybersecurity training to protect against the top threats to state, provincial, local, territorial and tribal governments.

SANS

GIAC
CERTIFICATIONS

Serving the Public Good

Cyber attacks on the public sector are multiplying.

No target is too big or small for today's cyber criminal.

From attacks on rural water authorities to freezing the networks of major cities, threats are getting more sophisticated and unpredictable. Every state, province, local, territorial and tribal agency is at risk.

The public sector now must add cyber defender to its list of duties.

The SANS Institute is making it our mission to make every community safer from cyber threats.

We want to make sure that those who keep our governments running have what they need to do so. That's why we offer public organizations a specialized program to strengthen their security posture.

In addition to our comprehensive catalog of training and certifications, we invite state and local organizations to become part of our community. This includes participating in summits, networking events, webinars, and access to our research and experts.

We hope that you will join us on this mission to make our communities safe.

Sincerely,

Brian Hendrickson
Chief Mission Officer

Comprehensive Cybersecurity Training

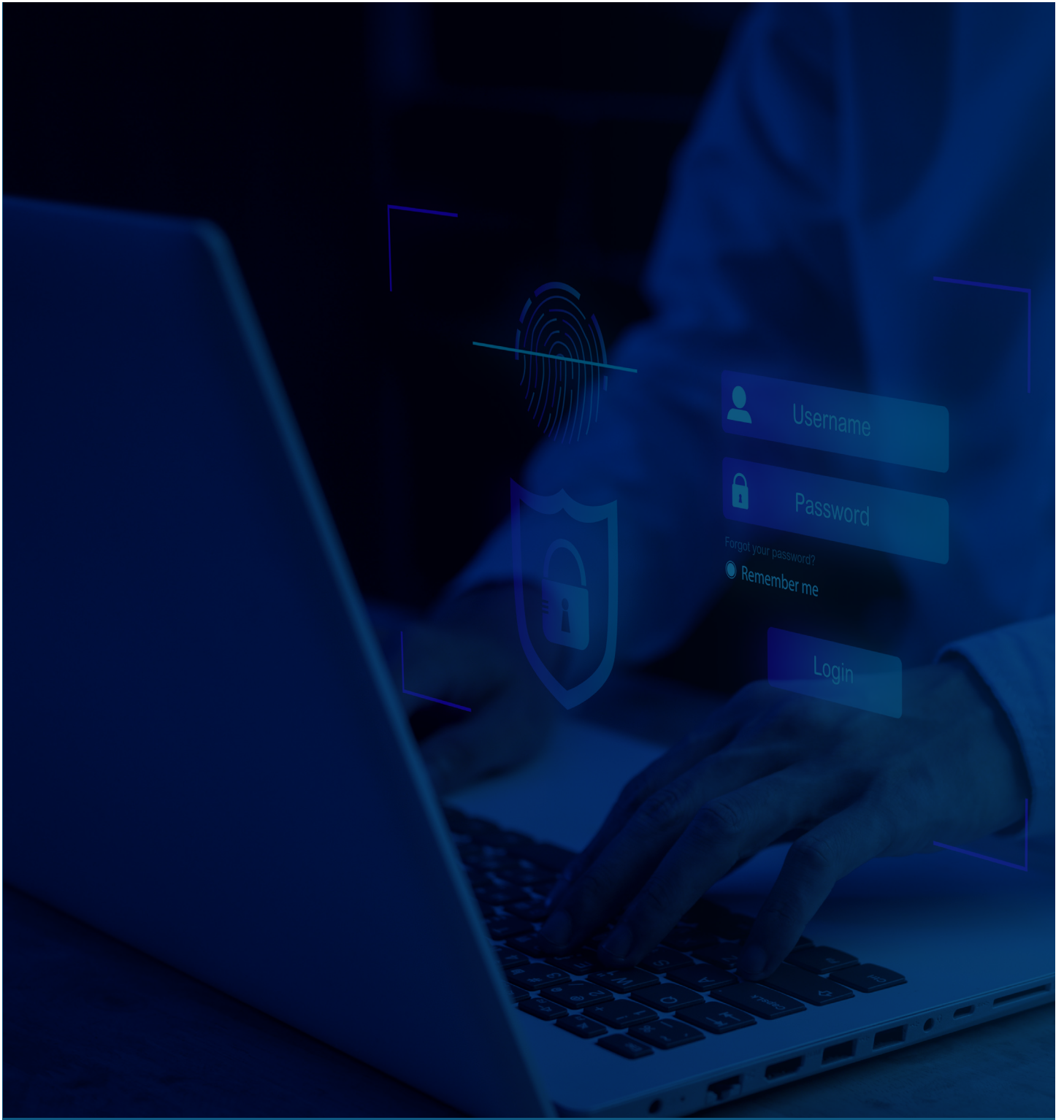
The SANS Institute has been training the public sector in cybersecurity since 1989. We've seen threats to state and local governments skyrocket in the past three years.

We also have seen budgets and resources stretched. This is making it harder for organizations to invest in proactive cybersecurity strategy.

SANS offers state and local governments in the United States and Canada the world's best cybersecurity training at a discounted price. In partnership with CIS, qualifying organizations get 50% off cybersecurity training when purchased during two program buying windows: December 1 - January 31 and June 1 - July 31.

Our program ensures that your staff will get the training needed to prevent, defend, and protect against cyber threats at a price your budget can afford.





PUBLIC SECTOR

4 Major Threats to Watch

**Anywhere there is data, there is a threat actor trying to steal it.
Even the smallest entities serving the public good are at risk.**

As a monitor of threats across the globe, SANS has seen the threats against the public sector multiply. The more our systems connect online, the greater the risk becomes.

The best way to arm against a cyber threat is to make sure you know what to look for.

Providing security awareness training for all staff can reduce the number of vulnerable entry points. Upskilling your IT and cyber professionals can rectify issues faster, lower the damage that an attack may cause, and increase organizational capacity to prevent future attacks and lower future risk.

There are always new threats on the horizon. We believe these are the top threats that every municipal, educational, or public service organization need to be ready for this year.

And of course, the training you need to keep ahead of them.

**Nearly one-third of U.S. local governments would be
unable to tell if they were under attack in cyberspace.¹**

Forno, 2022

Cloud Insecurity

Movement to the cloud accelerates internal operations - making process more efficient, effective, and vulnerable to new threats.

Connection, automation, and nearly limitless advancements make utilizing the cloud attractive for the public sector.

As the technology matures and organizations shift to multi-cloud environments, organizations need to amp up specialized cloud expertise. Infrastructure and architecture must be maintained with precision.

While many on-premise attacks are known, threat actors are finding new methods to attack the cloud. In 2023, Cloudflare, Google and Amazon Web Services (AWS) faced the largest attack on cloud. The 2-minute denial-of-service attack relied on a previously undisclosed vulnerability in a key piece of internet architecture.²

Cloud attacks at such a high level compromise the integrity of millions of connected systems. It means that your organization needs to have additional controls in place to safeguard your systems.

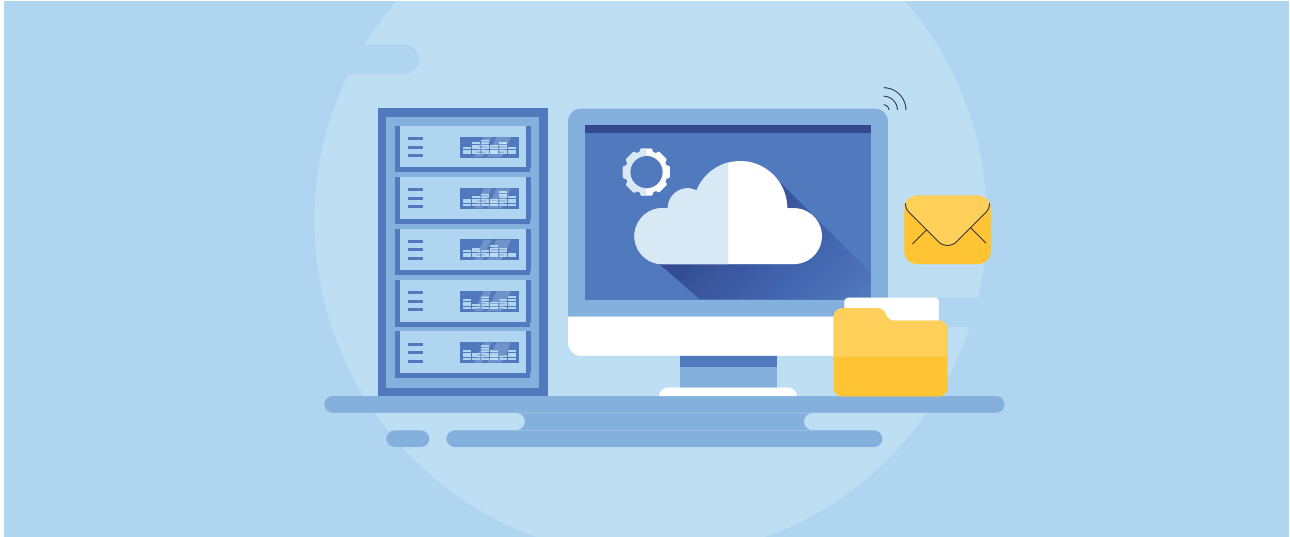
In October 2023, The SANS Institute hosted the CloudSecNext summit.

Phil Venable, Chief Information Security Officer at Google gave his thoughts on the next cloud mega trends.

Access the presentation at sans.org.

Cloud & IT Mega Trends 2024

- Artificial Intelligence
- Economies of Scale
- Shared Fate
- Healthy Competition
- Cloud as Digital Immune System
- Software Defined Infrastructure
- Increasing Deployment Velocity
- Simplicity
- Sovereignty Meets Sustainability



Security or resilience-related concerns with public cloud providers were cited by 74% of public sector executives in a 2022 report³

Zosel, 2022

Commonsense changes such as secure design, proper configuration by cloud provider, enforcing secure API access, and up-to-date detection engineering can start to deflect threats. Training your infosec team on how to configure your architecture can reduce vulnerabilities. Properly configured and secured systems can level and maintain cost while reducing risk.

Not keeping systems current against emerging threats is an attack waiting to happen. The public sector must make cloud a focus for 2024.

Recommended Training

SEC488: Cloud Security Essentials
Learn the foundation of cloud security
GCLD Certification

SEC510: Attack-Driven Cloud Security Controls & Mitigations
Prevent cloud security breaches with proper configuration.
GPCS Certification

SEC540: Cloud Security & Dev Ops Automation
Secure the DevOps toolchain.
GCSA Certification

LDR520: Cloud Security for Leaders
What every manager needs to know about the cloud.

Phantom Phishing

From fake LinkedIn accounts posing as recruiters to robocalling and 'smishing,' there are more ways for threat actors to enter your systems. Just one slip can take down your entire network.



Phishing attacks are costing our communities.

Nevada was the state most affected by phishing scams, while Kansas was the lowest.

The District of Columbia reported the most phishing attacks of any municipality, at 25.42 attacks per 100K residents.

Victims in New Hampshire had significant financial losses per phish at \$47,477.⁴

Forbes, 2023

Every InfoSec professional is on alert for that one false click.

Threat actors are getting more sophisticated in how they lure victims. Emails that once were obviously scams, now mimic professional corporate communications. Job boards are filled with false postings that gain access to personal data and credentials. Texts come in that appear to be real while it's become harder to recognize whether a phone call from an unknown number is legit.

In the 2023 SANS Security Awareness Report, social engineering tactics are the top risk to network security.

It's not just employees who put networks at risk, contractors, vendors, students, and guests open up access. One school district experienced a cyber attack that cost over \$10M in expenses to recover after a contractor accidentally clicked a phishing link.⁵ One city had its systems frozen including their 911 call center⁶

The constant influx of phishing threats can overwhelm an already stressed information security team. The most effective ways to reduce the burden is through prevention:

1. Security Awareness training for all who access your network.
2. Continuous reinforcement of awareness techniques through interactive measures.
3. Upskilling all IT professionals with role-based security standards.

SANS expects to see more phishing threats to the public sector in 2024. It's imperative to make sure that anyone with access to your network stays safe.

Recommended Training

SANS Security Awareness offers interactive training for your entire workforce and role-based modules for IT professionals.

- End User: Comprehensive security awareness training for all computer users
- Phishing: Test your employees through real-world phishing simulations
- Developer: Train your developers in secure coding techniques and how to recognize current threat vectors in web applications
- ICS Engineer: Rigorous computer-based training for industrial control systems
- IT Administrator: Level up your technical staff with advanced training
- NERC CIP: Relevant training addresses NERC CIP reliability standards for the utility industry



Ransomware Everywhere

Ransomware is a threat to public safety.



Once threat actors find a way into your system, Ransomware can cause mass disruption of thousands or even millions of people's lives.

The rate of ransomware attacks is alarming. Six in 10 local governments faced a ransomware attack or were breached. While a 2023 study by Sophos revealed that the rate of ransomware attacks in state and local government has increased from 58% to 69% year over year.⁷

It's not only major metro areas, a small city in Ohio faced a Ransomware attack in late 2023. It took down multiple government systems and functions while releasing 65,000 records.⁸

The term "Ransomware" no longer refers to a simple encryption that locks down resources. Human-Operated Ransomware (HumOR) along with the evolution of Ransomware-as-a-Service (RaaS) have created an entire ecosystem that thrives on hands-on-keyboard attacks. Some cyber extortion actors carry out the full attack life cycle and skip the encryption phase.

Ransomware cases increased by 73% in 2023.⁹

Threat Risk & Intelligence Services

Extortion is especially a threat for public officials and law enforcement. One moment of weakness can disrupt the delicate balance of public safety.

Police log-in credentials and personal information fetch a high price on the dark market.

In a 2021 attack on a major metropolitan police department, cyber criminals released the personal information of police officers, witnesses, and victims when a \$4M ransom was denied.¹⁰

Public Preparation

The public sector must be prepared to respond. This includes training your information security team and the leaders of your organization.

One false move can compromise the security of your community and cost millions to rectify.

Recommended Training

SEC401: Network, Endpoint & Cloud
Implement a winning defensive strategy.
GSEC certification

SEC504: Hacker Tools, Techniques, and Incident Handling
Get into the mindset of attackers.
GCIH Certification

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
Hunt, identify, counter, & recover from threats.
GCFA Certification

FOR528: Ransomware and Cyber Extortion
Hands-on training for ransomware response

LDR553: Cyber Incident Management
Leaders learn to handle and recover from an attack.

Executive Cybersecurity Exercises

Organizational leaders practice cyber crisis management incident response with an expert facilitator to speed response and reduce risk.

Control System Threats

Industrial control systems (ICS) are targets of threat actors seeking to disrupt our critical infrastructure, supply chain, and the utilities we depend on.

A municipal water authority serving rural counties was attacked in late 2023. The attack targeted a vulnerability in their industrial control system at their booster station.¹¹ Luckily, there was no impact on the drinking water -- this time.

Anything networked can be weaponized. The SANS Institute expects to see more industrial control system (ICS) ransomware attacks in the coming year. State-sponsored, organized threats will increase as geopolitical conflicts heighten. Small rural infrastructure can be as attractive a target as maritime ports.

No asset owner and operator is safe from state-sponsored threats.

The commoditization of IIOT has opened a new vulnerability. With more providers competing to sell their devices, the barrier for attacking vulnerabilities gets lower. Hacking toolkits for IIOT are on the horizon.

The recent evolution of ICS targeted attacks sends a clear message: proactive control system cyber defense requires engineering knowledge to preserve the safety of industrial control system (ICS) and operational technology (OT) operations.

In late 2023, The SANS Institute released our report [The ICS/OT Cybersecurity Survey in 2023](#) on the state of industrial control security.

Respondents to SANS' survey ranked deploying trained OT security defenders to leverage ICS-specific network visibility as the number one must-have capability.

As attacks on critical infrastructure and industrial control systems become brazen, ICS defenses must go beyond just preventative security.

Operators need to take the offensive: physical upgrades to equipment, precise security controls, and targeted training for every individual who operates or works with IIOT. This includes having an ICS specific incident response plan. Of the operators surveyed by SANS, only 52% of ICS facilities had an ICS/IOT response plan and 17% were unsure if they had one.¹²

Public organizations must not leave ICS/OT cybersecurity up to chance.

Recommended Training

ICS410: ICS/SCADA Security Essentials
Learn how to keep the operational environment safe against cyber threats.
GICSP Certification

ICS456: Essentials for NERC Critical Infrastructure Protection
Understand & implement 5/6/7 standards.
GCIP Certification

ICS515: ICS Visibility, Detection, and Response
Gain visibility and control over your industrial systems.
GRID Certification

SEC503: Network Monitoring and Threat Detection In-Depth
GCIA Certification



Program Partner



Eligible entities include state, provincial, local, tribal, and territorial government entities and related non-profit organizations in the United States and Canada.

Accessing Programs for State, Local & Municipal Organizations

The SANS Institute has a dedicated program for public organizations to make accessing the leading cybersecurity training easier.

State, provincial, local, territorial and tribal governments can participate in SANS aggregate buying program. In partnership with the Center for Internet Security (CIS), SANS is able to offer 50% off training when purchased during two program buying windows.

This purchase program makes it easy to get the training you need for your entire organization. Courses are available to take at your own pace via SANS OnDemand platform, or scheduled In-Person or Live Online.

Our program also includes the opportunity to purchase GIAC certifications, NetWars Continuous, and Security Awareness training.

We understand the complexities of operating a public organization, that's why we have dedicated support to help you register, select, and track your training. SANS will walk you through the process step by step.

**To get started or answer questions, contact our experts
at partnership@sans.org today.**

Training Expertise

SANS has a wide variety of training from entry-level to expert. Courses are available at up to 50% off for eligible organizations in North America.



The instructor made this course worthwhile. I truly appreciated his teaching style and his excellent knowledge of the subject matter.” - City Employee

SANS SECURITY AWARENESS

Secure your entire organization with hands-on training on security awareness. Interactive learning reinforces key cybersecurity concepts while simulations keep your team alert.

SANS' security awareness platform enables access to both enterprise wide and role-based training to level up your workforce.

GIAC CERTIFICATIONS

Practice & Master Cyber Skills

GIAC Certifications are the world's most recognized assurance of cybersecurity mastery.

GIAC credentials have been shown to increase cybersecurity confidence, employee retention, and ability to apply new skills.

Public organizations may add GIAC certifications to their program. Learn more at www.giac.org

74% of breaches involved the human element, which includes social engineering attacks, errors or misuse.¹³

Verizon DBIR, 2023

Discounted pricing on SSA is available for eligible public organizations during the program buying windows.



Interactive simulations put your cybersecurity skills to practice. NetWars continuous is offered as a standalone purchase during the two program buying windows.

Frequently Asked Questions

The SANS Institute welcomes public, non-federal entities to access the benefits of the SLTT program.

What are the eligibility requirements to participate in the SLTT governments program?

The program is open to state, provincial, local, municipal, county, tribal and territorial government agencies and government or community related non-profit organizations geographically located in North America.

Do the training credits purchased through this program expire?

Training credits purchased through this program expire 12 months after we receive payment for your order. However, a future purchase of additional training credits through this program, will extend the expiration of any unredeemed training credits that remain in the account at the time of deposit.

Can the training credits purchased through this program be shared by multiple people in my organization?

Yes, training credits may be used by any staff member of your organization with the approval of the voucher account administrator specified by your organization at the time of purchase.

When can I purchase and receive the program discounts?

The best pricing is available for purchases placed during the two specified purchase program windows: Winter Dec 1 – Jan 31 and Summer Jun 1- Jul 31. Lesser discounts are available on voucher purchases between the two annual purchase windows.

What courses may be taken with the course credits purchased?

Course credits purchase through the program may each be redeemed for one seat in any single SANS Long course (24+ CPE) taken in either SANS OnDemand or Live Online modalities.

Stop breaches before they start by training your staff to identify risk.

Who creates SANS' awareness training modules? How often are they updated?

The same SANS experts that teach our world-renowned technical courses work with content experts and adult learning scientists to create short-form content specifically intended to inform, empower, and change behavior. Courses are fully updated every 3 years.

Is the training licensed per module or "category"?

Training is offered on a "library" basis – there are no "tiers" within the libraries. A purchase of our End User training provides access to the entirety of the library, including all updates and additions.

Are there resources we could use to "promote" awareness outside of required training videos?

"Engagement Materials" are offered for every topic area in our End User library and available for many of our shortform technical training topic areas as well. Co-brandable posters, newsletters, digital signage, and much more are available to help organizations promote cybersecurity awareness throughout the year.

Is there training available for technical roles that goes deeper than general awareness training?

In addition to End User training, SANS offers shortform technical trainings for roles like Developer, IT Admins, and Business Leaders and Managers. These libraries help bridge the gap between general cybersecurity awareness training and a SANS technical course to ensure key technical roles are aware of the unique risks associated with their elevated levels of privileged access.

For more information visit sans.org/partnerships/sltd

End Notes

1. Forno, R. (2022, March 28) Local governments are attractive targets for hackers and are ill-prepared. Stanford.edu; Center for Internet and Society.
2. Starks, T., & DiMolfetta, D. (2023, October 11). The largest cyberattack of its kind recently happened. Here's how. Washington Post; The Washington Post.
3. Zosel, S. (2022, July 11). Governments and the public sector lead the cloud sovereignty debate | Capgemini. Capgemini.
4. Main, K. (2023, July 17). Phishing Statistics By State In 2024. Forbes.
5. Barr, L. (2023, January 25). Baltimore schools cyber attack cost nearly \$10M: State IG. ABC News; ABC News.
6. Calif. city officials restore 911 dispatching after cyberattack. (2023, July 28). EMS1
7. Sophos (2023, August) The State of Ransomware in State and Local Government 2023.
8. Hancock, A. (2024, January 5). Area city's cyber attack: Functions restored, \$350,000 spent, personal data issue in limbo.
9. Chapman, R. (2024, January 16) Ransomware Cases Increased Greatly in 2023 | Sans.org.
10. Brewster, T. (2021, May 14). Ransomware Hackers Claim To Leak 250GB Of Washington, D.C., Police Data After Cops Don't Pay \$4 Million Ransom. Forbes.
11. Kovacs, E. (2023, November 27). Hackers Hijack Industrial Control System at US Water Utility.SecurityWeek.
12. Lee, R. & Conway, T. (2022, November 7). The Five ICS Cybersecurity Critical Controls. Sans.org.
13. Verizon, (2023, June 6) Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket.



Launched in 1989 as a cooperative for information security thought leadership, it is SANS' ongoing mission to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place.

We fuel this effort with high quality training, certifications, scholarship academies, degree programs, cyber ranges, and resources to meet the needs of every cyber professional. Our data, research, and the top minds in cybersecurity collectively ensure that individuals and organizations have the actionable education and support they need.

The SANS Institute
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852

+1 301-654-SANS
partnership@sans.org
www.sans.org