Cybersecurity Awareness Month: When Governments Are Targeted, We All Learn

This summer, the state of Nevada and the city of St. Paul, Minn., faced cyberattacks that forced critical systems offline for days.

In St. Paul, city services – from online payments to public library systems – were disrupted, while Nevada had to take several public-facing systems offline and reset passwords statewide.

These events are a reminder that governments are prime targets for attackers. Cities, states and even federal agencies face daily attempts to breach their systems.

Cyberthreats aren't slowing down. Hackers are using AI and emerging technologies to craft more convincing phishing emails and to automate attacks.

The results are more than an inconvenience: constituents go without critical services, public trust is eroded and government employees can lose productivity.

That makes your awareness our first and most critical line of defense.

Here are some simple, everyday practices that you can take:

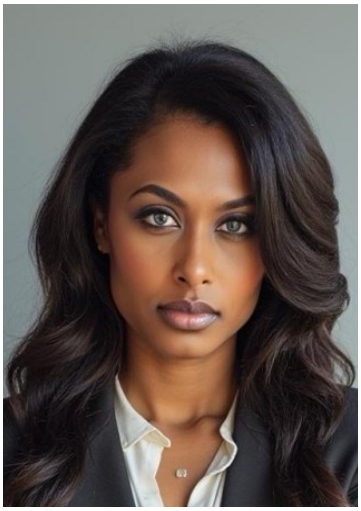
- Stay alert for phishing and unusual requests. Think before you open links, and use the Report button in Microsoft Outlook to report spam and suspicious messages.
- Use strong passwords, and never share them – not even with your help desk.
- Don't use your work equipment for personal use.
- Make sure you are regularly logging into devices and keeping software and operating systems up to date.
- Immediately report concerns or issues to your security team: If something seems suspicious, don't wait to let your security team know.
- Stay up to date on your cybersecurity and privacy awareness training in the Learning Management System.

Camille St. Omer and Andrew Albright Join NCDIT as Privacy Analysts

The N.C. Department of Information Technology welcomes Camille St. Omer and Andrew Albright as privacy analysts within the Office of Privacy and Data Protection. They will help protect North Carolina residents' personal data by ensuring state agencies follow privacy laws and policies and by advising agencies on how data is collected, used, shared and stored.

St. Omer brings more than a decade of experience in IT management and ethical data handling. With the prestigious Presidential Management Fellows program at the U.S. Department of Housing and Urban Development, she served as a federal privacy analyst and AI subject matter expert with the U.S. Department of Justice and U.S Department of Housing and Urban Development.

CONTINUED ON PAGE 2



Camille St. Omer

Andrew Albright

CONTINUED FROM PAGE 1

Camille St. Omer and Andrew Albright Join NCDIT as Privacy Analysts

St. Omer's previous roles also include data scientist, machine learning engineer and leading a private business registered with the U.S. Department of State's Overseas Security Advisory Council.

She holds a Bachelor of Science in business administration and information technology from Colorado Technical University and a Master of Science in unmanned systems from Embry-Riddle Aeronautical University.

Albright has more than 22 years of experience in both the government and private sectors. His expertise ranges from governance, risk and compliance to accreditation, policy administration, criminal justice and HIPAA.

Albright has been nationally recognized for his previous work related to accreditation and most recently served as privacy officer for the N.C. Department of Health and Human Services.|

He is a Certified HIPAA Privacy and Security Expert and holds a bachelor's and master's degree in criminal justice from John Jay College of Criminal Justice in New York.

NCDIT's Enterprise Security and Risk Management Office Updates Communication Methods

Stay tuned for significant enhancements to the way the Enterprise Security and Risk Management Office communicates.

A new layout for the ESRMO Cybersecurity and Risk Management website was rolled out the first week of October. Find answers to your questions quickly on pages for state government, local government, the public as well as active vulnerabilities and news.

Also, watch your inbox for brand-new digital version of the ESRMO newsletter to hit your inbox in December.

Attackers Abuse Google's AppSheet to Send Phishing Emails

Hackread, a news platform on infosec, cybercrime and privacy, reports that attackers are abusing Google's AppSheet platform to send phishing emails.

Attackers are sending messages that impersonate AppSheet and inform users of phony trademark violations. Sent from AppSheet's legitimate infrastructure, the emails are likely to bypass security controls and appear legitimate.

"As a Google Cloud service, AppSheet inherits the trust and reputation that organizations place in Google's infrastructure," the researchers write. "When employees see 'appsheet.com' in their inbox, they naturally associate it with the same security standards they expect from Gmail or Google Drive.

"With millions of business users building applications on the platform, AppSheet communications are common in corporate environments, making malicious emails appear routine."

Attackers have abused AppSheet since at least March 2025, accounting for many global phishing emails. Attackers are always looking for ways to slip past security filters and are increasingly abusing legitimate platforms to evade detection.

"This AppSheet campaign represents a broader trend of legitimate service abuse," the researchers explain. "Attackers are discovering they can achieve better results by using trusted platforms rather than building their own infrastructure."

Erich Kron, security awareness advocate at KnowBe4, told Hackread in a statement:

"The reliance on commonly used or well-known brands in social engineering attacks is nothing new; however, these attacks still remain quite effective. These types of attacks are meant to blend in with normal day-to-day activities, further increasing the trust level of the potential victim."

This article is redistributed with permission from KnowBe4.

Training & Continuing Learning Resources

TEEX: Texas Engineering Extension Service:

https://teex.org

NICCS: Free Online Training Environment:

https;//niccs.gov/education-training/cisa-learning

NICCS: National Initiative for Cybersecurity Careers & Studies:

https://niccs.cisa.gov

ICS-CERT Training:

https;//www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa

Additional Cybersecurity Newsletters

SAC Security Awareness Newsletter:
Monthly security awareness newsletter provided for all state employees by KnowBe4. Read the SAC newsletters**. Note: You must have a valid state employee Microsoft 365 account to access.**

SANS OUCH! Newsletter:
Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch

Be sure to follow the N.C. Department of Information Technology on X(formerly known as Twitter), Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness.

Remember … Stop. Think. Connect.

Disclaimer: *Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*