Monthly Cybersecurity Newsletter

October 2022
Issue

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Rob Main

October is National Cybersecurity Awareness Month

October 2022 is National Cybersecurity Awareness Month. Held every October, NCSAM is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online. Now in its 19th year, NCSAM continues to raise awareness about the importance of cybersecurity across the nation. The theme for NCSAM this year is:

"See Yourself in Cyber"

This year's theme focuses on the "people" part of cybersecurity, providing information and resources to help educate people and ensure that all individuals and organizations make smart decisions whether on the job, at home or at school – now and in the future. The Cybersecurity & Infrastructure Security Agency and the National Cybersecurity Alliance will focus on the following areas in promotions and outreach:

- Enable multi-factor authentication.
- Use strong passwords.
- Recognize and report phishing.
- Update your software.

More information about NCSAM can be found here. CISA is also providing several resources that you can share with others. Those resources are available throughout the year at https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-toolkit

The Center for Internet Security shares no-cost resources for creating your own public awareness campaign. These resources can help guide your organization on ways to increase understanding of cyberthreats and empower individuals in your community to be safer and more secure online. Find these resources at https://www.cisecurity.org/ms-isac/ms-isac-toolkit/.

Individuals, businesses, government and schools all play a vital role in improving the nation's collective cybersecurity preparedness. We live, work and play in an ever more connected world. Our increased reliance on remote environments reminds us that being more secure online is a ***shared responsibility***. Creating a safer cyber environment requires engagement from the entire community.

NORTH CAROLINA
CYBERSECURITY
AWARENESS SYMPOSIUM

2022 N.C. Cybersecurity Awareness Symposium | Oct. 4-5, 2022

Presented by the N.C. Department of Information Technology, the N.C. Cybersecurity Awareness Symposium is a free two-day virtual event on **Oct. 4-5, 2022**, that features cyber leaders and subject matter experts in the private, public and academic sectors on cyber-related topics including:

- Defending against cyberthreats
- Privacy and data protection
- Business continuity and resilience
- Workforce development

Choose from more than 20 online sessions and workshops presented by NCDIT and partners:

- N.C. Joint Cybersecurity Task Force
- N.C. Emergency Management
- N.C. National Guard
- U.S. Cybersecurity & Infrastructure Security Agency
- Amazon Web Services
- BitSight
- CrowdStrike
- Info-Tech Research Group
- KnowBe4
- Microsoft
- Splunk
- StateRAMP
- Tanium
- Tenable
- UNC-Wilmington
- VMware

Click to register for the free event.

CyberWeek – Oct. 17-21, 2022

Join over 10,000 influential leaders from the cybersecurity community at CyberWeek, the nation's largest week-long cybersecurity festival focused on digital threats, best practices and the U.S. government's work on improving cyberspace. This annual movement brings together top C-suite leaders from major technology companies, state and federal government agencies and other influential decision-makers to participate in hundreds of community-driven events.

The goal? Sharing best practices and sparking collaboration on big ideas that will revolutionize technology in the U.S. and fend off the next generation of attackers. CyberWeek will feature more than 100 virtual community events, interactive sessions, talks and networking opportunities across the nation with thousands of cybersecurity innovators, decision makers and influencers.

Get your pass to connect, collaborate and share the kinds of big ideas that will drive transformative change. Learn how to attend, sponsor or host an event at cyberweek.us.

State Chief Risk Officer Warns of Malicious Activity

Rob Main, State Chief Risk Officer, has issued a warning to agencies about malicious activity. Recently, a massive ransomware attack targeted the Los Angeles Unified School District, with a likely breach of student data and direct impacts to instruction. It could not have come at a worse time for the students, faculty and staff in that district who had just begun their fall semester.

Threat actors are paying particular attention to the education sector, targeting K-12 school districts and research institutions with high-value intellectual property assets at an increasing rate daily. Review the best practices that whole-of-state partners, education or otherwise, should be doing right now to defend themselves against malicious activity:

- Patch operating systems, software and firmware as soon as manufacturers release updates.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Set antivirus and anti-malware solutions to automatically update and conduct regular scans.
- Monitor privacy settings and information available on social media sites.
- Configure network firewalls and intrusion prevention appliances to block unauthorized IP addresses and disable port forwarding.

If you suspect your organization has been subjected to a significant cybersecurity incident, do not hesitate to report it to NCDIT. Please call NCDIT's Customer Support Center at 1-800-722-3946, or use the Statewide Cybersecurity Incident Report Form. It is imperative that it is reported as soon as possible, so we can mobilize the N.C. Joint Cybersecurity Task Force (as required) to assist with incident response and recovery efforts.

Cybersecurity and privacy are our collective responsibilities. Thank you for all you do to help keep North Carolina safe from cybersecurity attacks!

SANS 2022 Vulnerability Management Survey: Detecting and Combatting Cloud Environment & Supply Chain Vulnerabilities

With rapidly changing computing platforms, a growing threat landscape and a shift to a remote workforce, managing vulnerabilities is more challenging than ever. We are all looking for answers and want to know how our peers are doing in their fight. We can learn from each other to make our systems, applications and networks more secure and resilient.

SANS will host a webcast on **Wednesday, Oct. 19, 1 p.m.** to examine results from the **SANS 2022 Vulnerability Management Survey**. We will dig deeper into how organizations deal with supply chain vulnerabilities and vulnerabilities in cloud-hosted systems and services. We will analyze the maturity data collected from previous year's surveys and dive into trends and new insights found in this year's survey.

Register here for this event today, and receive the associated white paper written by SANS certified instructor David Hazar.

Red Flags!

Red flags are signs of danger or a problem. Protect yourself and your organization from cybercriminals by being aware of these warning signs and knowing actions to stay safe.

Common Red Flags	Actions to Stay Safe
Someone you don't know following you or your co-workers inside the office.	Contact security about unknown individuals.
Someone looking at your screen or watching what you type.	Pay attention to your surroundings and safeguard organizational information.
Someone you don't recognize looking through a desk.	Keep confidential information and devices locked-up/secured when not in use.
Social media connection requests from someone you don't recognize.	Don't accept unsolicited requests; report them to the service.
Receiving an unusual request from someone you know.	Contact the person directly to verify it's legitimate.
Requests that offer you something in exchange for private organizational information.	Be cautious before sharing any personal or organizational information.
Unexpected emails, phone calls, and voice or text messages.	Follow your organization's security policies for handling suspicious correspondences.
Urgent requests to take an action.	Never act on emotion and take the time to verify the request is legitimate.

Always stop, look, and think before you click on a link, open an attachment, or take any action!

KnowBe4

KnowBe4
Human error. Conquered.
ON-DEMAND WEBINAR
Learn How to Forensically Examine Phishing Emails to Better Protect Your Organization Today

Cybercrime has become an arms race. The cybercriminals constantly evolve their attacks while you, the vigilant defender, must diligently expand your know-how to prevent intrusions into your network.

Staying a step ahead may even involve becoming your own cybercrime investigator, forensically examining actual phishing emails to determine the who, where and how. In this on-demand webinar, Roger A. Grimes, KnowBe4's data-driven defense evangelist, shows you how to become a digital private investigator.

You will learn:

- How to forensically examine phishing emails and identify other types of social engineering
- What forensic tools and techniques you can use right now
- How to investigate rogue smishing, vishing and social media phishes
- How to enable your users to spot suspicious emails sent to your organization

Get inside the mind of the hacker, learn their techniques and how to spot phishing attempts before it's too late. Watch the webinar now: https://info.knowbe4.com/phishing-forensics-chn

84% of Americans Have Experienced Some Form of Social Engineering

Researchers at NordVPN have published survey results finding that 84% of Americans have experienced some form of social engineering – however, only 54% have heard of the term "social engineering." Of the respondents, 85% percent said they were aware of the term "phishing," and 36% said they had fallen victim to a phishing email.

The researchers found that phishing emails are the most common form of social engineering attacks, followed by text message phishing (smishing) and voice phishing (vishing):

- 48% – Suspicious emails with links and attachments and/or asking for their personal information
- 39% – Suspicious texts with links and attachments and/or asking for their personal information
- 37% – Pop-up advertisements that are difficult to close
- 37% – Suspicious email(s) containing links, attachments or asking them to reply and divulge work/business information
- 32% – Suspicious email(s) from someone posing as an important personal asking them to wire them funds
- 27% – Suspicious voicemail(s) asking the recipient to divulge personal information

- 26% – A virus on their computer or phone
- 19% – Malware on their device that redirected them to a fake version of a website

NordVPN offers the following advice to help users recognize these types of attacks.

"The point of a social-engineered attack is to get you to follow a link or sign up to something," the researchers write. "The best way to recognize a socially engineered attack is to analyze the language of the message.

"Is the language desperate? Does the message imply there's a time limit to whatever request it's asking for? Does the message sound urgent? Remember that most banks will never text you and ask for your login credentials. In fact, any text message or email you receive that requests any kind of login details is probably best suited for the trash bin."

This article was redistributed with permission from KnowBe4.

Next Monthly Privacy Meeting Is Oct. 25

NCDIT Chief Privacy Officer Cherie Givens will hold the department's next monthly privacy meeting from 10 a.m. to 11 a.m. on **Oct. 25**. All privacy points of contact and other state employees working on privacy matters or interested in privacy are invited.

Reminder for all privacy points of contact and security liaisons, please review the **updated PTA (Privacy Threshold Analysis) Template** and provide your **feedback via Microsoft form by 5 p.m., Oct. 14**. If you are a designated Privacy Point of Contact or Security Liaison and you did not receive an email inviting you to review the updated PTA, please send a message to ditprivacy@nc.gov, and let us know. Thank you for your help in building our State Privacy Program.

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment
  - https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service
  - https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies
  - https://niccs.cisa.gov/
- ICS-CERT Training
  - https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Cybersecurity Newsletters

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

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/resources/?type=newsletter

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

Be sure to follow the N.C. Department of Information Technology on 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.*