Monthly Cybersecurity Newsletter

October 2020 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

---

2020 National Cybersecurity Awareness Month

Gov. Roy Cooper has proclaimed October 2020 National Cybersecurity Awareness Month in North Carolina. Held every October, National Cybersecurity Awareness Month (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. NCSAM 2020, the 17th year, continues to raise awareness about the importance of cybersecurity across the nation. The theme this year is:

"Do Your Part. #BeCyberSmart."

This theme encourages individuals and organizations to own their role in protecting their part of cyberspace, stressing personal accountability and the importance of taking proactive steps to enhance cybersecurity. The Cybersecurity & Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCSA) will focus on the following areas in promotions and outreach of NCSAM:

- Week of October 5 (Week 1): If You Connect It, Protect It
- Week of October 12 (Week 2): Securing Devices at Home and Work
- Week of October 19 (Week 3): Securing Internet-Connected Devices in Healthcare
- Week of October 26 (Week 4): The Future of Connected Devices

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/cisa-cybersecurity-resources.

In addition to the CISA resources, the Center for Internet Security (CIS) is also providing no-cost resources that will aid in creating your own public awareness campaign. These resources can help guide your organization on ways to increase the understanding of cyber threats and empower individuals in your community to be safer and more secure online. These resources are located at https://www.cisecurity.org/ms-isac/ms-isac-toolkit/.

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

In support of National Cybersecurity Awareness Month (NCSAM), the N.C. Department of Information Technology's (DIT) Enterprise Security and Risk Management Office will be hosting the 2020 Annual Cybersecurity Awareness Symposium on **October 5 & 6**. Learn from cyber leaders and subject matter experts in the private, public and academic sectors on various topics related to maximizing cyber spend while protecting data and systems from compromise. All sessions will be online this year and will include the following (***Note:*** *Topics subject to change*):

- *The Evolution of Ransomware*
- *Partnering Through NC 2-1-1 for Easy Reporting of Cybercrimes by North Carolinians*
- *Automation & Security: A Match Made in Heaven*
- *Hands-On Defending Exercise*
- *Business Continuity & Pandemic Planning*
- *Role of DHS Assessments in Executive Risk Decisions*
- *Public Safety Information Security – Protecting Critical Infrastructure*
- *Cybersecurity: A Driving Force Behind Cloud Adoption*
- *TTX for K-12 Incident Response*
- *Virtual Threat Hunting Challenge*
- *Using Public Toolsets to Evaluate & Improve Your Organization's Security*
- *Managing COVID-19-Era Third-Party Risks with Real Data*

To register for this event, please visit here.

Triangle InfoSeCon

Triangle InfoSeCon is an annual Information Security conference in the Triangle area and the flagship event of the Raleigh Chapter of the Information System Security Association (ISSA). The mission of ISSA is to train and educate as many people as possible about the importance of Information Security. As an organization, ISSA believes that Information Security is both the present and the future, and it is incumbent upon us to try to influence the decision makers of today and to train the security leaders of tomorrow.

The Triangle InfoSeCon event will be virtual this year on **October 29-30, 2020**. For more information about the event and to register, please visit https://www.triangleinfosecon.com/.

10 CYBERSECURITY AWARENESS TIPS

1. Don’t click on direct links (in emails, text messages, etc.), especially those that are asking you to enter sensitive information. It's best to go directly to the source.
2. Don't overshare on social media. These details can provide hackers with your location, ammunition to craft spear phishing attacks, and answers to security questions. Think before you share!
3. Don’t go “out of bounds” for communication. E.g. if you’re buying something on eBay, and the other party wants to negotiate via email instead of the bidding system.
4. Never reuse passwords between any website or service.
5. Always be skeptical of any unexpected invoice, or request to get or pay for anything by using gift cards.
6. Never answer authentication recovery questions (e.g. What is your mother’s maiden name?) with real answers. Unfortunately, that means you’ll have to write down each question and answer for each website that requires them, but you’ll be far less likely to have your account hijacked.
7. Confirm an email sender's request, even if it is your boss, before processing it. Better safe than sorry.
8. Know who to report any suspicious emails to at your workplace. Don’t delete the email - report it.
9. Invest in a password management tool - ain’t nobody got the time to remember all those passwords!
10. Be vigilant with suspicious SMS messages. Your bank will NEVER ask you to access your account from an SMS.

SANS Security Awareness Planning Kit

The SANS Institute is providing a security awareness planning kit that consists of several helpful materials. The materials are listed in the order that people would most likely use them for building a ***new security awareness program***. For more established or mature awareness programs you most likely just want to select the specific resources you need. The resources in the kit include the following:

- **Example Project Charter**: The first step in planning any large-scale project or initiative. This covers the key elements of a Project Charter for a new Security Awareness Program.
- **Example Project Plan**: A detailed example of what a complete Project Plan can look like for a comprehensive Security Awareness Program.
- **Presentation**: The slide deck will help you gain leadership's support for your security awareness program.
- **Metrics Matrix**: This interactive matrix identifies and documents numerous ways to measure security behaviors, culture and strategic impact of your security awareness program.
- **Phishing Planning Guide**: This strategic guide walks you through the key elements of planning a successful phishing program.
- **Maturity Model**: A key part of planning and communicating your awareness program. Both the model and a detailed breakdown of each stage is provided in your planning kit.
- **Annual Program Schedule**: These templates provide examples of how you can visually document your overall security awareness plan.
- **SANS Security Awareness Report**: This annual data-driven report enables you to benchmark your program against other organizations and prioritize your resources and initiatives.
- **Working from Home Deployment Kit**: The kit includes everything you need to quickly plan and deploy a Work from Home security awareness training program, including a strategic planning guide, training videos and additional materials in over thirty languages.

The Security Awareness Planning Kit may be found here.

There is a reason more than half of today's ransomware victims end up paying the ransom. Cyber-criminals have become thoughtful; taking time to maximize your organization's potential damage and their payoff. Ransomware has gone nuclear. Join Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, in this webinar as he dives into the following:

- Why data backups (even offline backups) won't save you
- Evolved threats from data-theft, credential leaks, and corporate impersonation
- Why ransomware isn't your real problem
- How your end users can become your best, last line of defense

For more webinars provided by KnowBe4, click here.

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. ***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2020

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). 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

Stay Safe While Working from Home

Working remotely has its benefits, ***but*** it comes with added responsibility. Click here for tips on how to stay secure while working from home.

October 1-31: National Cybersecurity Awareness Month (NCSAM)

October 5-6: 2020 Annual Cybersecurity Awareness Symposium

October 7 @ 1:00pm: BCM New User Open Teams Session (Contact bcm@lists.nc.gov for more information)

October 8-9: SANS Cyber Solutions Fest 2020

October 8-9: Assurance CM application virtual training (Contact bcm@lists.nc.gov for more information)

October 13: Smart Devices Need Smart Security: Securing Your Business in an Internet of Everything World

October 29-30: Triangle InfoSeCon

November 1-30: National Critical Infrastructure Security & Resilience Month

November 30: 2020 Business Continuity and Disaster Recovery Plans due!

Also…for a list of upcoming SANS webcasts, visit here!

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.*