Monthly Cybersecurity Newsletter

February 2022 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

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

Revised Statewide Information Security Policies Published

The Statewide Information Security Manual – the foundation for security and privacy in the state of North Carolina – was recently updated to align with the National Institute of Standards and Technology (NIST) SP 800-53 Revision 5. The policies were developed with the assistance of subject matter experts and peer reviewed by agency representatives using NIST 800-53 revision 5 controls as the framework.

The revised policies, which provide state agencies with a baseline for managing information security and making risk-based decisions, are located on the N.C. Department of Information Technology website. You can also view a list of changes from NIST 800-53 revision 4 to revision 5.

Effective January 19, 2022, all system owners, business owners, security liaisons and other responsible agents – including contractors and vendors – are required to start implementing and complying with the policies immediately. The following table lists the eighteen (18) revised policy documents that have been published.

ID	POLICY	ID	POLICY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Security Planning
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	SR	Supply Chain Risk Management

Agencies are to ensure that all internal security documentation is updated to reflect these policies and requirements. Use by local governments, local education agencies , community colleges, constituent institutions of the University of North Carolina and other executive branch agencies is encouraged, to the extent allowed by law.

NIST SP 800-53 has historically served as the foundation of federal government security controls and is widely adopted across state and local governments, health care entities, critical infrastructure and private sector organizations. Revision 5 marks the first substantial update in seven years to the NIST 800-53 framework and is representative of the ever-changing cyber landscape.

Have a High School Student in Your Life? If So, Listen Up.

Have a high school student in your life? The free online CyberStart America competition, supported by the N.C. Department of Information Technology, is an amazing opportunity for them to explore potential careers in cybersecurity and computer science while competing for scholarships.

No experience in IT or cybersecurity is needed.

Complete details, including registration, can be found at www.cyberstartamerica.org. (Although **registration is open until April 27**, students should sign up early to allow more time for game play and to qualify for scholarships.)

What is CyberStart America?

CyberStart America is a series of free challenges in which students act as "cyber protection agents" to solve cybersecurity-related puzzles and explore related topics, such as code breaking, programming, networking, and digital forensics.

They can use the game to qualify for the National Cyber Scholarship program to help with college.

Why is CyberStart America important?

There are approximately 21,000 vacant cyber-related positions in North Carolina. Nationally, that number tops nearly 600,000.

Introducing students – even those with little or no interest in computer careers – now to cybersecurity careers helps create educational pathways and opportunities to build a diverse and talented cyber pipeline to help address future threats and challenges.

Last year, Emily Chen, a senior at Panther Creek High School in Cary, was named a National Cyber Scholar with Honors after ranking among the top 30 of more than 30,000 U.S. high school students who competed in CyberStart America.

"Prior to this program, I honestly had no idea I could pursue a career in cybersecurity," Chen said. "I've gained skills that made me realize it's something I really enjoy doing. If you're hesitant, I just say give it a try. It's free. You just have to sign up."

How You Can Help

Last year, 1,165 students from 173 schools participated in CyberStart America. **Help us surpass that number this year.** Spread the word to the high school students in your life. Find videos, links, and other information you can share at it.nc.gov/cyberstart.

An Overview of Password Theft

Phil Muncaster, with ESET, an internet security company that offers anti-virus and firewall products, recently gave a useful summary of the most popular ways hackers can steal users' passwords. These techniques often involve some form of social engineering, such as tricking them into entering their credentials on a phishing site or installing malware on their devices.

"Human beings are fallible and suggestible creatures … prone to make the wrong decisions when rushed," Muncaster states. "Cybercriminals exploit these weaknesses through social engineering, a psychological con trick designed to make us do something we shouldn't."

Phishing is probably the most famous example of social engineering. Hackers masquerade as legitimate people or organizations, such as friends, family members or companies a person has done business with. These attackers will send email or text messages that look authentic but include a malicious link or attachment. If the unsuspecting recipient clicks the link or opens the attachment, that action can download malware or take the user to a fake webpage to fill in personal details.

Attackers can also use brute-forcing attacks, in which they use automated tools to guess a user's password. An extremely effective form of this attack is credential stuffing, which tests millions of leaked credentials against login pages.

Muncaster says hackers often do not need to put much effort into these attacks, since many people still use very simple and obvious passwords. "Even simple guesswork – as opposed to the more systematic approach used in brute-force attacks – can do the job," he states.

The most common password in 2020 was "123456," followed by "123456789." The fourth most was "password." Most people use the same password, or something close to it, across multiple accounts, which puts them at additional risk and makes password theft even easier for attackers.

Muncaster offers the following advice to help safeguard your passwords:

- Use only strong and unique passwords or passphrases on all your online accounts.
- Avoid reusing login credentials across multiple accounts.
- Switch on two-factor authentication on all accounts.
- Use a password manager, which stores strong, unique passwords for every site and account, making logins simple and secure.
- Change your password immediately if a provider tells you your data might have been breached.
- Only use HTTPS sites for logging in.
- Do not click on links or open attachments in unsolicited emails.
- Only download apps from official app stores.
- Install security software from a reputable provider for all your devices.
- Ensure all operating systems and applications are on the latest version.
- Beware shoulder surfers in public spaces.
- Never login to an account if you are on public Wi-Fi or use a VPN if you have to use one.

To review the state of North Carolina user account and password policy, read IA–5 - Authenticator Management in the statewide Identification and Authentication Policy.

U.S. Secret Service Electronic Crimes Task Force Ransomware Webinar

The U.S. Secret Service Electronic Crimes Task Force recently presented a three-hour webinar, titled **Ransomware: An Emerging Threat**. This presentation included members of government agencies and private corporations and contains a wealth of information. The presenters and panelists shared their expertise on ransomware.

The webinar is available in two parts. The first video includes the three presentations and concludes at the pause taken just before the panel discussion. The second video contains the panel discussion. For more information and to view the webinar, click here.

Beware of a New Google Vishing Scam

Vishing, or voice phishing, is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers.

A new FBI advisory, "Building a Digital Defense Against Google Voice Authentication Scams," warns of a scam that is designed as a precursor to additional vishing scams and can perform Gmail account takeovers. The scam works even if you do not use Google Voice.

Google Voice is a service where Google provides users with a virtual phone number to make and receive calls and texts. The FBI advisory describes a scam that involves a threat actor who responds to a personal ad – they use the example of selling a couch on Craigslist or some other site – and says they want to make sure you are legitimate by sending you an authentication code from Google.

What is really happening is the scammer is setting up Google Voice using your phone number as the primary number and using you to assist them with Google's authentication process during setup. Once completed, the threat actor has a new Google Voice account tied to your mobile phone, so they can carry on without worrying about having it tied to their phone. Additionally, the code being sent could be used to allow them access to reset the password to your Gmail account.

Organizations relying on Gmail for corporate email should be specifically concerned about this scam. With access to one of your internal email accounts, threat actors can easily send out phishing emails designed to gain access to devices or install ransomware.

The FBI offers the following advice to avoid getting scammed:

- Never share a Google verification code with others.
- Only deal with buyers and sellers in person. If you are exchanging money, make sure you are using legitimate payment processors.
- Do not give out your email address to buyers/sellers conducting business via phone.
- Do not let someone rush you into a sale. If they are pressuring you to respond, they are likely trying to manipulate you into acting without thinking.

To view the FBI advisory, click here. If you believe you are the victim of an online scam, report it to the FBI's Internet Crime Complaint Center at www.ic3.gov or call your local FBI office.

FEMA Offers Online Train-the-Trainer for CERT Basics Course

FEMA's Emergency Management Institute is offering for free an online version of its K0428 CERT Train-the-Trainer course, which prepares participants to deliver FEMA's Community Emergency Response Team (CERT) Basic Training course.

2022 Course Dates:

- Feb. 8, 9, 10, 15, 16 and 17 (1-5 p.m. EST)
- March 1, 2, 3, 8, 9 and 10 (12-4 p.m. EST)
- April 5, 6, 7, 12, 13 and 14 (1-5 p.m. EST)
- June 7, 8, 9, 14, 15 and 16 (12-4 p.m. EST)
- July 12, 13, 14, 19, 20 and 21 (1-5 p.m. EST)
- Sept. 6, 7, 8, 13, 14 and 15 (12-4 p.m. EST)

Each class size is limited to 20 students and meets four hours a day three days a week for two weeks. Students must attend all sessions.

These courses will be delivered in a via Adobe Connect, and participants should familiarize themselves with it beforehand. No Adobe Connect account or downloads are required.

Students must have a FEMA student identification number, computer with microphone, speaker, and stable access to the internet. Visit the FEMA Student Identification System to obtain a SID.

Prerequisites:

- A referral from a CERT-sponsoring agency, typically a local, regional, or state government agency, is required.
- If you are not a first responder, the CERT Basic Training is required.
- For current first responders, IS-317: Introduction to CERT will familiarize them with the CERT Program.

Prospective students should apply through the Emergency Management Institute's online admissions system. The course offers 1.3 continuing education units. Please refer to the FEMA Emergency Management Institute for course date availability.

Proofpoint's 2022 Threat Landscape

Every year, Proofpoint's threat experts examine trends from the prior year and anticipate changes in the threat landscape for the year ahead.

For 2022, some of the top concerns include the evolving threats presented by initial access brokers, ransomware affiliates, easy and widespread access to commodity malware, and rising insider threats.

Proofpoint is offering a one-hour deep dive into cybersecurity threats to look out for in 2022. Join the webinar on Wednesday, Feb. 2 at 1 p.m. EST.

FEMA - National Continuous Improvement Guidance

FEMA is seeking whole community stakeholder feedback to aid in the development of National Continuous Improvement Guidance. FEMA will host a series of webinars to gather input from whole community stakeholders who wish to participate and indicate what they would find most useful in establishing new or developing existing continuous improvement processes. Webinar sessions offered in February are as follows:

- Listening Session #4: 5-6 p.m. EST on Feb. 2
- Listening Session #5: Noon-1 p.m. EST on Feb. 8

For additional information on to register, visit https://preptoolkit.fema.gov/web/cip-citap/events. For questions or feedback, send an email to FEMA-CITAP@fema.dhs.gov.

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

Feb. 15: SANS Webinar: Emergence of a New Anti-Ransomware Technology: Moving Target Defense

Feb. 18: SANS Webinar: Log4Shell Vulnerability Solutions Forum 2022

Feb. 22: ISSA Webinar: 2021 DDoS Attack Trends: Year in Review

Feb. 23: SANS Webinar: SANS 2022 Cyber Threat Intelligence Survey

Feb. 24: Proofpoint's 2022 State of the Phish Webinar

View a list of upcoming SANS webcasts.

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.*