Monthly Cybersecurity Newsletter

October 2019
Issue

NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

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

National Cybersecurity Awareness Month 2019

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 2019 emphasizes personal accountability and stresses the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. This year's overarching message – **Own IT. Secure IT. Protect IT.** – focuses on key areas including citizen privacy, consumer devices, and e-commerce security.

The NCSAM 2019 Toolkit is a comprehensive guide to make it easy for you and your organization, regardless of size or industry, to engage and promote NCSAM. Click on the link below to use the guide and resources to help you engage your stakeholders and promote positive, lasting cybersecurity habits.

https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019

2019 Annual N.C. Cybersecurity Awareness Symposium

Hosted by the NC Department of Information Technology Enterprise Security and Risk Management Office, this year’s symposium was held at the McKimmon Conference and Training Center at NC State University on October 10 & 11. The Symposium featured briefings and workshops from NC DIT Secretary and State Chief Information Officer Eric Boyette and leading industry cyber partners including N.C. National Guard, IBM, CrowdStrike, Tenable Nessus, Tanium, BitSight, VMWare and GRIMM Cyber.

Interactive workshops hosted by NC DIT and leading industry cyber partners included Disaster Recovery Business Continuity; Business Continuity Plan Development; Managing Vendor Risk; Cyberthreat Hunting; Capture the Flag; Incident Response Plan Development; and State Cybersecurity Requirements & Considerations for IT Procurement.

Key points brought up during the symposium include:

- This year’s overarching message: **Own it. Secure it. Protect it.**
- We must continually strive to promote a culture of security awareness
- The human element is the weakest link in any computing system
- 92% of malware infecting network computer systems is introduced by email
- 50% of all crimes in the United Kingdom are cybercrimes
- Organized crime & nation-states are the greatest threats, not a teenager in a basement
- The “silver bullet” of cybersecurity is people and effective information sharing

NC Department of Information Technology

State Tech Workers Train to Foil Hackers

by Laura Leslie, WRAL Capital Bureau Chief – Oct 11, 2019

"Local Governments Becoming Frequent Targets for Hackers"

FBI: "High-Impact" Ransomware Attacks Threaten U.S. Businesses and Organizations

On October 2, 2019, the FBI issued a warning regarding "high-impact" ransomware attacks stressing the risk they pose to U.S. businesses and organizations. Ransomware is a form of malware designed to attack an individual's and/or an organization's computer network by encrypting the data, holding it hostage until a ransom is paid.

While the frequency of ransomware attacks has remained constant, the warning stated that the attacks are becoming more targeted, more sophisticated, and more costly. The losses from ransomware attacks have increased significantly, according to complaints received by the Internet Crime Complaint Center (IC3) and FBI case information.

Attacks against state and local governments continue, but the warning said that cybercriminals are also targeting healthcare organizations, industrial companies, and the transportation sector. The warning specifically urges organizations to protect themselves against email phishing campaigns, software, and Remote Desktop Protocol vulnerabilities.

The FBI does not recommend paying a ransom. There is no guarantee that by paying the ransom the organization will regain access to its data. In some incidents victims who paid the ransom never received the decryption keys. The FBI urges all ransomware victims, regardless of whether they paid the ransom or not, to immediately report the incident to law enforcement, including the FBI. Doing so provides investigators with critical information necessary to apprehend ransomware attackers and prevent future attacks. Additionally, all NC state agencies are required to report ransomware incidents to the ESRMO Threat Management Team.

For the complete and unedited article, to include FBI technical recommendations on how to protect computer networks from these types of attacks, click on the link below.

https://www.meritalk.com/articles/fbi-high-impact-ransomware-attacks-threaten-u-s-businesses-and-organizations/

New Wire Fraud Scam

There's a recent new phone scam you may not be aware of. You receive a phone call that says, "Are you there?" or "Is this Mr./Ms. so and so?" Do not answer with a "Yes." Your voice is recorded and your "yes" statement is spliced into a recording as an answer to an authorization question such as, "Do you agree to this purchase (or something worse)." It is very difficult to dispute this false charge on your credit card because after all, they have your voice authorizing the purchase. One suggestion might be to simply answer such a phone call with a question such as, "May I ask who's calling?"

CYBERSECURITY NEWSLETTERS

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

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month the newsletter covers ***Own IT. Secure IT. Protect IT.***

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Four Simple Steps to Staying Secure.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

Protect Your Access Badge

If you work in a facility that requires an access badge for entry, remember to protect it when you're away from your work facility. Do not leave it unattended in plain view inside your car. A bad actor intent on gaining unauthorized access to your facility can follow you to see where you may leave it. Remember, PROTECT YOUR BADGE!

November 6 – The Persistent Pernicious Myths and Hidden Truths of Cybersecurity

November 26 – SDLC – Is it Useful

Be sure to follow DIT on Twitter Facebook LinkedIn for more tips throughout October. You are also encouraged to review the Stay Safe Online NCSAM page and the DHS NCSAM page for additional information and details on cybersecurity awareness events.