Monthly Cybersecurity Newsletter

October 2018 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

---

October is National Cybersecurity Awareness Month

October is National Cybersecurity Awareness Month (NCSAM). NCSAM is a collaborative effort between the Department of Homeland Security (DHS) and its public and private partners to raise awareness about the vital role cybersecurity plays in the lives of U.S. citizens. Each week of the month focuses on the following topics:

- **Week 1: Make Your Home a Haven for Online Safety**
  Week 1 underscores basic cybersecurity essentials the entire family can deploy to protect their homes against cyber threats.
- **Week 2: Millions of Rewarding Jobs: Educating for a Career in Cybersecurity**
  Week 2 addresses ways to motivate parents, teachers and counselors to learn more about the field and how to best inspire students and others to seek cybersecurity careers.
- **Week 3: It's Everyone's Job to Ensure Online Safety at Work**
  Week 3 focuses on cybersecurity workforce education, training and awareness while emphasizing risk management, resistance and resilience. NCSA's CyberSecure My Business™ sheds light on how small and medium-sized businesses can protect themselves, their employees and their customers against the most prevalent threats.
- **Week 4: Safeguarding the Nation's Critical Infrastructure**
  Week 4 emphasizes the importance of securing our critical infrastructure and highlights the roles we all can play in keeping it safe. In addition, it will lead the transition into November's Critical Infrastructure Security and Resilience Month, which is spearheaded by DHS.

You are encouraged to review the Stay Safe Online NCSAM page and the DHS NCSAM page for additional information and details on cybersecurity awareness events.

In support of National Cybersecurity Awareness Month, the Department of Information Technology (DIT) and the Enterprise Security and Risk Management Office (ESRMO) will be hosting a **Cybersecurity Awareness Symposium** on **October 18 & 19, 2018**. This event is open to anyone and will be held at the NC Rural Economic Development Center, Room 150/151, located at 4021 Carya Drive, Raleigh, NC 27610. To register, go to https://www.surveymonkey.com/r/2018_CybersecuritySymposium.

DIT is also posting cybersecurity tips on social media during NCSAM. Be sure to follow DIT on Twitter Facebook LinkedIn for more tips throughout October.

Triangle InfoSeCon

The 14th Annual Triangle InfoSeCon will be held at the Raleigh Convention Center in Downtown Raleigh, North Carolina from 8:00 AM to 6:00 PM on **October 26, 2018**. For more information about this event, please visit http://www.triangleinfosecon.com/.

Is Your Credit on Ice?

If you are concerned about identity theft, data breaches, or someone gaining access to your credit report without your permission, you should consider placing a *credit freeze* on your report. Many people mistakenly believe that credit monitoring services will protect them from identity thieves. However, these services **do not** prevent thieves from stealing your identity to open new accounts in your name, or from damaging your reputation. The most that credit monitoring services will do is alert you *after* someone steals your identity. According to KrebsonSecurity, a better solution is to prevent thieves from stealing your identity in the first place by freezing your credit report.

A new federal law makes it *free* for people in the United States to place and lift freezes on their credit file, for their dependents under the age of 16, and for incapacitated adult family members. A credit freeze basically blocks any potential creditors from being able to view or "pull" your credit file, unless you first unfreeze your file. A credit freeze will help prevent ID thieves from applying for credit in your name and will help protect your credit score, and it will not prevent you from using your existing lines of credit. A *credit freeze* is not the same as a *credit lock*, though! Unlike freezes, credit locks are typically provided *for a fee*, and they are not governed by any law. This means credit bureaus can change the terms of these arrangements.

To file a credit freeze, consumers should contact each of the three major credit bureaus online (Equifax, Experian and TransUnion), by phone or by mail. When you place a freeze, each credit bureau will assign you a personal identification number (PIN) that you will need to provide to the credit bureau when you wish to open a new line of credit. Keep in mind that it is a good idea to keep your credit freeze PINs somewhere safe in the event you wish to unfreeze your credit. It is also a good idea to periodically order a *free copy* of your credit report. While a credit freeze and credit monitoring are good things to do, it is important to regularly review your credit file with the major bureaus for any signs of unauthorized activity. For more information about credit freezes, please visit the article at KrebsonSecurity.

PCI Webinar by Coalfire

The final webinar by Coalfire on PCI-DSS that will be presented in 2018 is scheduled for 12/4/2018 @ 10:00-11:00 AM ET. An announcement regarding the webinar will be sent prior to the scheduled date. The topic of the webinar will be *Managing Service Providers*.

Don't forget the other **monthly newsletters** that are available to you. The following are some other cybersecurity newsletters the ESRMO recommends to you. We hope you find them beneficial.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month is on ***National Cybersecurity Awareness Month – October 2018.***

- https://www.cisecurity.org/resources/newsletter

SANS OUCH! Newsletter: A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Email Oops, and How to Avoid Them.***

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

---

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link:

https://www.sans.org/security-awareness-training/video-month

The SANS Institute free webcasts may be accessed via the following link:

https://www.sans.org/webcasts/upcoming.

Upcoming Events…

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

October 7 – 13: Fire Safety Awareness Week

October 18 – 19: NC Cyber Awareness Symposium at NC Rural Economic Development Center in Raleigh, NC

October 25 – 26: InfraGard's Healthcare CyberGard in Charlotte, NC

October 26: Triangle InfoSeCon

October 30 @ 11:30 a.m. EST: MS-ISAC / EI-ISAC Webinar: *Ballot Check – Securing Election Systems Beyond the Perimeter*

November 1 – 30: Critical Infrastructure Security and Resilience Month

November 8: Women in BCM Focus on Education and Safety

December 4: PCI-DSS Webinar *Managing Service Providers*

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.

Top 10 Security Practices *For Work*

- **Report anything unusual. Whether it be a suspicious package or someone who doesn't belong, if you see or hear something, say something!**
- **Think before you click. CEO scams—social engineering attacks that spoof the email of an executive—are on the rise.**
- **Trust but verify. If you do receive an email requesting financial transactions or sensitive information, verify that it's legit. Sometimes a quick phone call is all it takes.**
- **Use strong, unique passwords for every account! In fact, use passphrases with symbols, numbers, and letters for added security. Turn on two-factor authentication wherever possible.**
- **Keep it clean. A messy desk is a security risk. Keep your work area clean and organized.**
- **Be aware of unsolicited hardware. Never plug in random USB drives or optical discs. Even a keyboard or mouse can be a security threat!** (Read more: secaware.co/2lp5Rki)
- **Be aware of the kind of data you handle. Understanding data classification is essential for knowing what needs to be protected!**
- **Only use approved devices. We put a lot of effort in maintaining a safe and secure network. Be sure to ask before connecting with a personal device at work.**
- **Know how to properly dispose of sensitive info. Shred sensitive documents. Ask about disposing of old computers or devices.**
- **Always follow policy. Policies are in place for the benefit of everyone within the organization. If you're not sure, please ask!**

– WHY IS – *data classification* so important?

A better question to ask is, "**How can you protect information unless you know what exactly you are trying to protect?**" Data classification is a way of categorizing sensitive information so you can be familiar with where it exists, how it needs to be protected, and why it needs to be protected. Read more: secaware.co/2lp5Rki.

What is CEO Fraud?

Also known as a Business Email Compromise (BEC), a CEO fraud is an exponentially growing scam by which the attacker spoofs the email address of a high-level executive and emails requests for information or financial transactions to other employees. Over the last three years **this scam has cost organizations billions globally**, and attacks are expected to increase this year. So, it's imperative that we **always confirm the source of an email**, be on the lookout for anything that seems odd or off, and, if you even have so much as a shadow of a doubt, report it! Trust your instincts and use common sense!

NC DIT

NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Cybersecurity Awareness Symposium

October 18 - 19

Information Share to Close the Cyber Gap

In support of National Cybersecurity Awareness Month (NCSAM), the Department of Information Technology (DIT), Enterprise Security and Risk Management Office (ESRMO) will be hosting a two-day Cyber Awareness Symposium.

During these sessions, state and local government employees will hear from industry, state and federal leaders on the importance of information sharing to combat the ever-increasing cyber threats, as well as how cybersecurity integrates within non-IT roles within an organization.

All state and local government employees are welcome to attend.

Opening Remarks:

NC DIT Secretary & State Chief Information Officer Eric Boyette

---

Industry Leaders Present on Insider Threat Mitigation, Information Sharing, Current Cyber Threats & More

---

Incident Response Workshop

Sponsored by Tanium LLC

Capture the Flag Workshop

Sponsored by Fortinet

Location:

NC Rural Economic Development Center
Room 150/151

4021 Carya Drive
Raleigh, NC 27610

October 18
9 a.m. - 4:30 p.m.

October 19
9 a.m. - 3 p.m.

For More Info & Awareness Tips:
https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management