Monthly Cybersecurity Newsletter

October 2021 Issue

Enterprise Security and Risk Management Office (ESRMO)

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

October is National Cybersecurity Awareness Month

October 2021 is National Cybersecurity Awareness Month (NCSAM). 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 18th year, NCSAM continues to raise awareness about the importance of cybersecurity across the nation. The theme for NCSAM this year is:

"Do Your Part. #BeCyberSmart."

This theme encourages people 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 and the National Cybersecurity Alliance will focus on the following areas in promotions and outreach:

- **Week of Oct 4 (Week 1):** Be Cyber Smart.
- **Week of Oct. 11 (Week 2):** Phight the Phish!
- **Week of Oct. 18 (Week 3):** Explore. Experience. Share. – Cybersecurity Career Awareness Week
- **Week of Oct. 25 (Week 4):** Cybersecurity First

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 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 cyberthreats 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/.

Individuals, 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 community.

2021 N.C. Cybersecurity Awareness Symposium is Oct. 6-7

The 2021 N.C. Cybersecurity Awareness Symposium, hosted by the N.C. Department of Information Technology, will be Oct. 6-7. This is a virtual event that open to those in government, military, and academic institutions. The symposium will provide learning opportunities for how to help secure an organization amid current trends in the following areas: *ransomware attacks, Zero Trust architecture, threat intelligence* and *work force development*. Registration with your official organization email account is required for all sessions. For more information and to register for this event, visit it.nc.gov/symposium.

The Cybersecurity & Infrastructure Security Agency will host its fourth annual National Cybersecurity Summit on Wednesdays in October. The 2021 summit will be held as a series of four virtual events bringing stakeholders together in a forum for meaningful conversation:

- **Oct. 6:** Assembly Required: The Pieces of the Vulnerability Management Ecosystem
- **Oct. 13:** Collaborating for the Collective Defense
- **Oct. 20:** Team Awesome: The Cyber Workforce
- **Oct. 27:** The Cyber/Physical Convergence

Register for this free summit and read more about the presentations at CISA.gov/cybersummit2021.

Triangle InfoSeCon is the largest annual information security conference in the area and is the flagship event of the Raleigh chapter of the Information System Security Association. Its mission is simple: train and educate as many people as possible about the importance of information security.

This year's event will be **Thursday, Oct. 28** and **Friday, Oct. 29**. For more information and to register for this event, please visit https://www.triangleinfosecon.com.

YOU are a target!

Cybercriminals are quite effective at getting what they want. They've learned that the easiest way around your organization's defenses isn't hacking and cracking, it's tricking you into letting them in.

DIGITAL ATTACKS

Phishing: Email-based social engineering targeting an organization.

Spear Phishing: Email-based social engineering targeting a specific person or role.

Stop, look, and think before you click that link or open that attachment.

IN-PERSON ATTACKS

USB Attacks: An attack that uses a thumb drive to install malware on your computer.

Tailgating: When a hacker bypasses physical access controls by following an authorized person inside.

Stop, look, and think before allowing someone in that you don't recognize or plugging any external media into your computer.

PHONE ATTACKS

Smishing: Text-based social engineering.

Vishing: Over-the-phone-based social engineering.

Stop, look, and think before you surrender confidential information or take action on an urgent request.

Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.

The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network.

Red Flags

Red flags are a sign of danger or a problem. They can be as subtle as an uneasy feeling or as obvious as an email about "suspicious charges" from a bank that you don't even have an account with.

Pay attention to these warning signs as they can alert you to a social engineering attack!

Since phishing is the most common form of social engineering, let's take a closer look at seven areas in an email and their corresponding red flags.

FROM

- An email coming from an unknown address.
- You know the sender (or the organization), but the email is unexpected or out of character.

TO

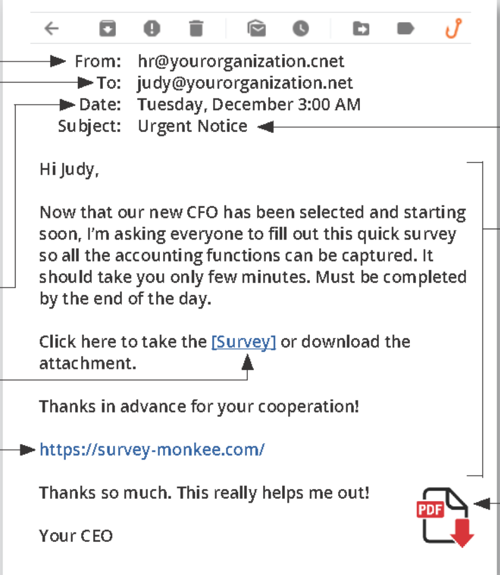
- You were copied on an email and you don't know the other people it was sent to.

DATE

- You receive an email that you would usually get during normal business hours, but it was sent at 3:00 a.m.

HYPERLINKS

- There are misspellings in the link.
- The email contains hyperlinks asking you to take an action.
- When you hover your cursor over the link, the link address is for a different website.



From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Urgent Notice

Hi Judy,

Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

https://survey-monkee.com/

Thanks so much. This really helps me out!

Your CEO

SUBJECT

- The subject line of an email is irrelevant or doesn't match the message content.
- It's an email about something you never requested or a receipt for something you never purchased.

CONTENT

- The sender is asking you to click on a link or open an attachment.
- The email is asking you to look at a compromising or embarrassing picture of yourself or someone you know.
- You have an uncomfortable feeling, or it just seems odd or illogical.

ATTACHMENTS

- Any attachment you receive that you aren't expecting.

© 2019 Knowbe4 Inc. All rights reserved. | www.KnowBe4.com

KnowBe4

October 18-22, 2021

CYBERWEEK

PRESENTED BY CYBERSCOOP

The nation’s largest week-long cybersecurity festival is back. U.S. CyberWeek will take place both in person in the Washington D.C. area and digitally across the U.S., bringing together the most influential cybersecurity leaders from major tech companies, government agencies and education.

The goal? Sharing the kinds of big ideas that will have the power to revolutionize technology in the U.S. and fend off the next generation of attackers. Learn how to attend, sponsor or host an event at cyberweek.us.

International ShakeOut Day is Oct. 21, when many drills will happen. However, you can hold yours on any day. Make sure to register for 2021 to be included among millions of people worldwide who will practice Drop, Cover, and Hold On. Whether you register as an individual, family or organization, your involvement will inspire others to participate in ShakeOut and become better prepared to survive and recover. To register for this event, click here.

Learn more about these options, and download ShakeOut drill leader presentations, at ShakeOut.org/covid19.

And, there is always more you can do ahead of ShakeOut. When was the last time you checked on your disaster supplies? Have you “Secured Your Space” to prevent damage and injury? What changes are there to your emergency plans and contacts? Use the Seven Steps to Earthquake Safety as a guide from now until October.

FEMA Virtual Cybersecurity Symposium

The Federal Emergency Management Agency is offering a virtual cybersecurity symposium for technical personnel and focuses on information sharing, vulnerability assessments and other cyberthreats impacting the emergency management community. Attendees will be able to share best practices and key lessons learned between government and industry. Read more in Training Opportunity 1678.

Course Dates: Oct. 20-21 and Oct. 27-28
Location: Virtual using Zoom.

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/2021

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

October 1: FEMA National Exercise Process Overview Webinar

Oct. 3-9: National Fire Prevention Week

Oct. 4: FEMA Comprehensive Preparedness Guide**,** also on 10/13

Oct. 5-6: 2021 N.C. Cybersecurity Awareness Symposium

Oct. 18-22: CyberWeek

Oct. 28-29: Triangle InfoSeCon Virtual Conference

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.*