Monthly Cybersecurity Newsletter
September 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

Feds Warn of Vishing Threat

Some people say you should never waste a crisis. That certainly seems to be true for the COVID-19 pandemic which has resulted in a shift to increased working from home. The pandemic has made it easier for threat actors to take advantage of lax security practices and less in-person verification. In response to a new voice phishing campaign, commonly called "vishing", the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) recently issued a joint cybersecurity advisory.

Vishing usually involves threat actors collecting public information about people through a variety of sources, such as social media platforms, recruiter and marketing tools, and other publicly available services. Collected information about an individual often includes name, address, phone numbers, employer, job position, and duration of employment at a company. Using publicly collected information, the actors then call targeted employees, sometimes using spoofed numbers of other offices and employees in the victim's company to appear legitimate. The attackers will use social engineering techniques, such as posing as help desk or IT personnel and using personal knowledge about the victim to gain trust. The goal of this deception is to convince the victim to divulge sensitive information or to login to a site (that may appear legitimate!) with valid account credentials. When the victim accesses the site with his or her credentials, the attacker can then log that information and use it to gain access to other information or resources with the employee's account or to fraudulently obtain funds.

So…What can be done?

One of the best defenses against this type of attack is multi-factor authentication (MFA) with physical security keys. This method of authentication requires a user to have a physical device ***in addition to*** his or her username and password to access a system. However, MFA is not widely used, so organizations still need to focus on employing the principle of least privilege (allowing *only* the amount of access needed for users and systems), restricting what can be installed on devices, and active monitoring of anomalous activities. Along with these technical controls, organizations need to *continuously* raise awareness among staff on how to spot and respond to social engineering attempts. They need to make security awareness and training an integral part of their operations and consider periodically sending test phishing messages to their employees to gauge their awareness levels in a safe environment.

The FBI and CISA suggest the following tips for individuals:

- Verify web links do not have misspellings or contain the wrong domain (*e.g. micosoft.com*).
- Bookmark the correct work/business URLs and do not visit alternative URLs on the sole basis of an inbound phone call.
- Be suspicious of unsolicited phone calls, visits, or email messages from unknown individuals claiming to be from a legitimate organization. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. If possible, try to verify the caller's identity directly with the organization.
- If you receive a vishing call, document the phone number of the caller as well as the web site the caller tried to send you and report it using your organization's procedures.
- Limit the amount of personal information you post on social networking sites. The internet is a public resource; only post information you are comfortable with *anyone* seeing.
- Evaluate security and privacy settings for all social networking accounts: sites change their options periodically. Review them regularly to make sure your choices are still appropriate.

For more information on how to stay safe on social networking sites and to avoid social engineering and phishing attacks, visit the CISA Security Tips below.

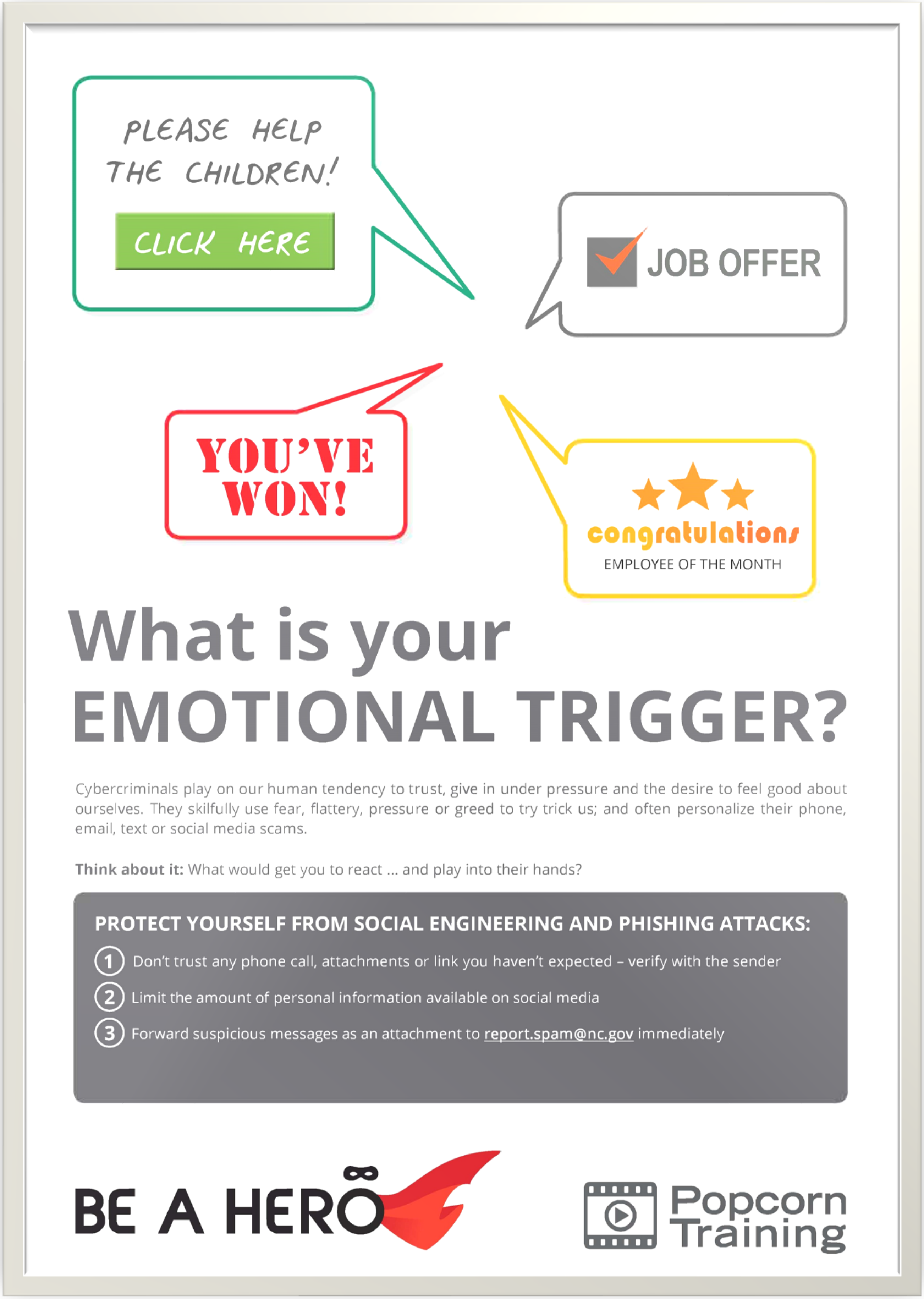
- Avoiding Social Engineering and Phishing Attacks https://us-cert.cisa.gov/ncas/tips/ST04-014
- Staying Safe on Social Networking Sites https://us-cert.cisa.gov/ncas/tips/ST06-003

2020 Annual Cybersecurity Awareness Symposium
Hosted by the N.C. Department of Information Technology Enterprise Security and Risk Management Office
#CyberSecureNC
NCDIT
NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY
OCT.
5 & 6

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*):

- *Virtual Capture the Flag*
- *Cyber Pandemic Planning*
- *Cybersecurity Risks & Emerging Threats*
- *Protecting Biomedical Devices*
- *Navigating Cloud Security*
- *Threat Hunting*
- *Business Resilience*

To register for this event, please visit here.



PLEASE HELP THE CHILDREN!

CLICK HERE

JOB OFFER

YOU'VE WON!

congratulations

EMPLOYEE OF THE MONTH

What is your EMOTIONAL TRIGGER?

Cybercriminals play on our human tendency to trust, give in under pressure and the desire to feel good about ourselves. They skilfully use fear, flattery, pressure or greed to try trick us; and often personalize their phone, email, text or social media scams.

Think about it: What would get you to react ... and play into their hands?

PROTECT YOURSELF FROM SOCIAL ENGINEERING AND PHISHING ATTACKS:

1. Don't trust any phone call, attachments or link you haven't expected – verify with the sender
2. Limit the amount of personal information available on social media
3. Forward suspicious messages as an attachment to report.spam@nc.gov immediately

BE A HERO

Popcorn Training

This year will be the third year of the National Cybersecurity Summit, which is moving to a virtual format while still providing meaningful opportunities to discuss cybersecurity. Last year's summit, which drew more than 1,700 attendees, focused on providing cybersecurity strategies, policies and/or initiatives that facilitate collaboration between the full range of government, defense, civilian, intelligence and law enforcement entities.

This year, the summit will be held as a series of two-hour webinars every Wednesday for four weeks, beginning **Sept. 16 until Oct. 7**. Each week will have a different theme, highlight relevant topics and include keynote speeches and remarks from leadership across the government and private sectors.

For more information and to register, visit www.cisa.gov/cybersummit2020.

What is Security and Privacy? PCI and Beyond Webinar

Coalfire, a PCI compliance validation services vendor, will be hosting a 1-hour webinar for the State of NC's merchant community on **September 9, 2020 at 10:00am**. The title of the webinar will be "What is Security and Privacy? PCI and Beyond". The speaker Bill Franklin, Senior Director Payments, will lead a discussion about Security and Privacy Requirements and Regulations. As a Senior Director in Coalfire's Cyber Assurance Services organization, Bill is responsible for client engagements focused on projects and advisory services regarding the Payment Card Industry Data Security Standards. Bill has over 25 years of experience conducting and managing IT Governance, Risk, and Compliance assessment and audits in the areas of PCI, HIPAA, FFIEC, NIST 800-53, ISO and COBIT.

You may join the meeting from your computer, tablet or smartphone via the following link:
https://global.gotomeeting.com/join/748146141

You can also dial in using your phone. (Toll Free): 1 866 899 4679
Access Code: 748-146-141

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.

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

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/.

September 9: What is Security and Privacy? PCI and Beyond Webinar

September 16, 23, 30, Oct. 7: CISA's Annual National Cybersecurity Summit

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

October 5-6: 2020 Annual Cybersecurity Awareness Symposium

October 8-9: SANS Cyber Solutions Fest 2020

October 29-30: Triangle InfoSeCon

October 31: 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.*

***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.*