Monthly Cybersecurity Newsletter

March 2021 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

---

What Can You Do to Improve Cybersecurity?

Cybersecurity is everyone's responsibility. We are all targets of those who wish to steal our data or cause us harm. We must be vigilant to do what we can to improve the security of our systems and reduce the risk we will become victims. The following six tips can help protect yourself and others.

Avoid being social engineered: According to one source, social engineering is responsible for 70% to 90% of all malicious digital breaches. Cybercriminals will attempt to trick you into clicking a link, opening an attachment, downloading a file or divulging personal information, such as your login ID and password, banking or credit card information. The best thing you can do to prevent cyberattacks is to focus on mitigating social engineering.

Keep software up to date: Unpatched software is responsible for 20% to 40% of all computer attacks. Installing software updates for your operating system and programs is ***critical*** to have a more secure system. Always install the latest security updates for your devices. Turn on automatic updates for your operating system. Keep installed applications and browser plug-ins up to date.

Practice good password management: The most common method of protecting access to information is a username and password. You must keep your passwords *strong*, *unique,* and *safe*. A long, complex password or a passphrase are good ways to protect access to your information. Never divulge your passwords to anyone. An approved password manager can also help keep your passwords secure.

Physically secure your computing devices: The physical security of your devices is just as important as the technical security. If you need to leave your laptop, phone, or tablet for any length of time – lock it up so no one else can use it. If you keep protected data on a flash drive or external hard drive, make sure they are encrypted and locked up as well. For desktop computers, lock your screen or shut down the system when they are not in use.

Install and maintain antivirus protection: A good anti-malware program is essential to detect and quarantine malicious programs. Only install these programs from known and trusted sources. Also, keep the software and virus definitions up to date to ensure these programs remain effective.

Safeguard sensitive data: Keep sensitive data (e.g., Social Security numbers, credit card information, health information, etc.) off your computing devices, if not needed. Always use encryption when storing or transmitting sensitive data. Securely remove sensitive data files from your devices when they are no longer needed. Lastly, do not share sensitive information on social media networks.

Work-from-Home Phishing Emails on the Rise

KnowBe4, a security awareness training provider, has released its latest quarterly report on top-clicked phishing email subjects. Phishing is a cybercrime where an attacker poses as someone legitimate via email to lure the targeted person to take a negative action, Such actions include clicking a link to a malicious website, opening a malicious attachment in an email, downloading a malicious file or divulging sensitive information to an attacker.

While COVID-19-related phishing messages have declined, there have been a lot of subjects related to working remotely. Since the pandemic began, many organizatoin have increased their remote working, so it makes sense that cybercrminals have targeted this topic for their schemes. Along with remote work subjects, social media-related subjects are also a concern. The most prevalent social media subjects were related to LinkedIn. These messages continue to dominate the top social media email subjects.

KnowBe4 examined tens of thousands of email subject lines from simulated phishing tests and email subjects of actual emails users received and reported to their organizations as suspicious. The following list includes the Top 10 Most-Clicked General Email Subject Lines around the world for Q4 of 2020:

- Password Check Required Immediately
- Touch Base on Meeting Next Week
- Vacation Policy Update
- COVID-19 Remote Work Policy Update
- Important: Dress Code Changes
- Scheduled Server Maintenance – No Internet Access
- De-activation of [[email]] in Process
- Please Review the Leave Law Requirements
- You Have Been Added to a Team in Microsoft Teams
- Company Policy Notification: COVID-19 - Test & Trace Guidelines

The full report and an infographic may be found here. Remember to always think before you click. Examine every email to determine if it is legitimate and safe. For more information, click here.

Avoid Scams

A recent advisory from the Federal Emergency Management Agency (FEMA) warned about scams. Do not trust anyone who offers financial help and then asks for money or personal information. The U.S. Department of Homeland Security, FEMA, U.S. Department of Health and Human Services and the U.S. Centers for Disease Control and Prevention staff never charge for disaster assistance.

- The best information on legitimate sources of help in your area will come from local officials.
- Do not disclose information to any unsolicited telephone calls and emails.
- Federal and local disaster workers do not solicit or accept money.
- Beware of visits, calls or emails from people claiming to be from FEMA asking for your Social Security number, bank account or other sensitive information. Giving out this type of information can lead to identify theft.

For more information about Fraud and Scam Artists, please review FEMA's press release here.

PCI Webinars by Coalfire

The N.C. Office of the State Controller is pleased to announce that Coalfire, a PCI compliance validation services vendor for the state of North Carolina, will be presenting four webinars in 2021. The scheduled dates are as follows:

Date	Topic (tentative)
March 9, 2021	Policies, Procedures, Standards and Guidelines, What Are They?
June 15, 2021	Vulnerability Scanning and Penetration Testing – What is the Difference?
Sept. 7, 2021	Authentication and Access Control – Who Are You?
Dec. 7, 2021	Risk Assessments – Do you Feel Lucky?

All webinars will begin at 10 a.m. EST and will be approximately 1 hour. Additional details (including registration information) will be sent out in advance of each webinar. For the current list of webinars being provided by the Office of the State Controller, please visit the Office of the State Controller's website.

Please Note: The PCI webinar announcements are distributed through the eCommerce listserv. If you are interested in receiving this information directly, please register online. The eCommerce listserv also provides updates for products and services on the Merchant Card and EFT Master Services Agreements, as well as webpage and enrollment form updates and reminders regarding annual PCI Compliance, SAQs and Quarterly Scans.

Severe Weather Preparedness Week Coming Soon

The week of March 7-13 is **Severe Weather Preparedness Week**, with the statewide tornado drill scheduled for Wednesday, March 10 at 9:30 am. Materials and graphics for your use in promoting Severe Weather Preparedness are available here for easy visual browsing and download.

Along with the National Weather Service, schools, workplaces, and families at home are encouraged to observe the drill and practice their tornado safety plan in a way that is COVID-19 safe and maintains social distance.

The N.C. Division of Emergency Management will **not** be organizing tornado drill news media events in schools during the pandemic this year. If there is actual severe weather in the state on March 10, the tornado drill will be postponed to **Friday, March 12**.

For additional materials for Severe Weather Preparedness Week, or if you need help with emergency planning in any way, please reach out to the Joint Information Center via email at pio@ncem.org.

Resources on preparing for a variety of different emergency situations may also be found on ReadyNC website. The more prepared you are, the better you will be able to respond to an actual emergency.

Don’t be phish bait.

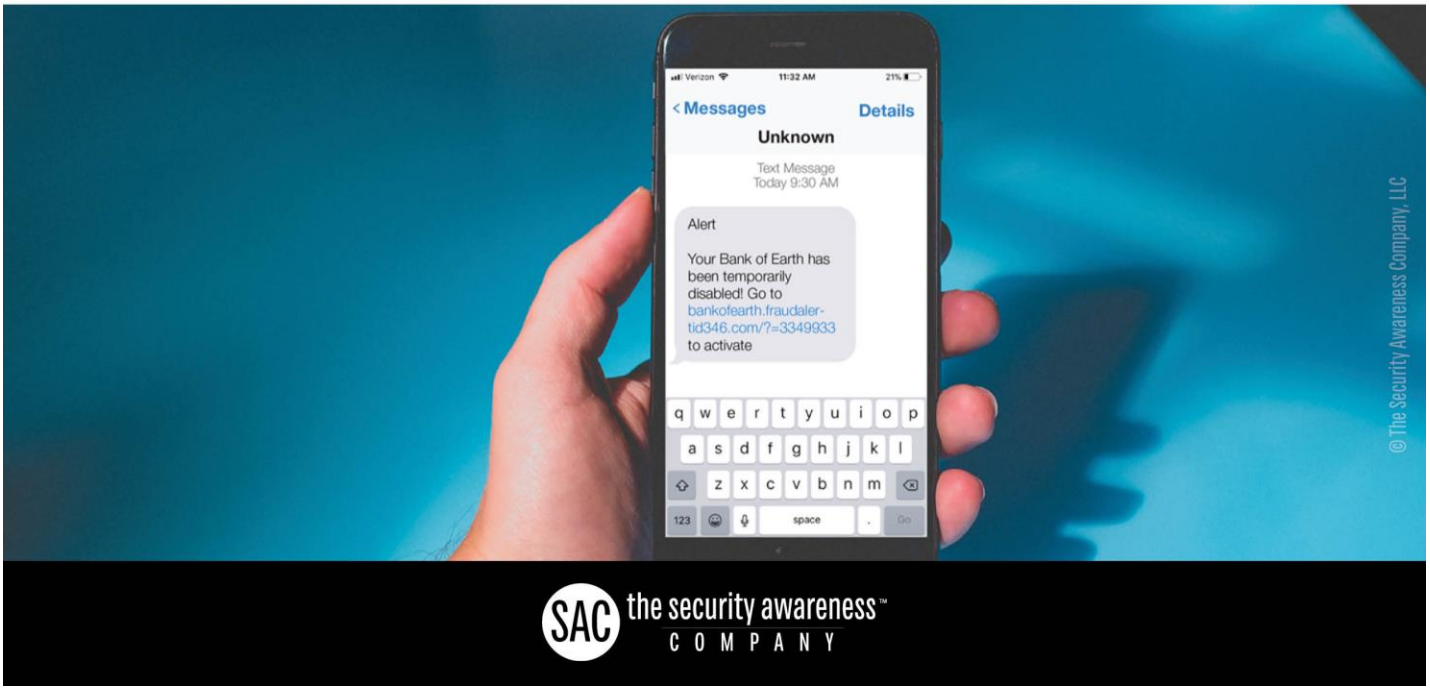
Use common sense.

Stay focused.

Slow down.

Think before you click.

If you suspect a phishing attack, report it immediately.



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/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

March 9: *Policies, Procedures, Standards and Guidelines, What Are They?* PCI Webinar by Coalfire (*See information in newsletter.*)

March 31: SANS webinar *Hybrid Security: Protecting Your Supply Chain*

April 2: Good Friday (State Holiday)

April 7: SANS webinar *Taking a behavioral approach to security- how to stay one step ahead of your adversaries*

April 15: Tax Day

May 17-21: Business Continuity Awareness Week (BCAW)

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.*