Monthly Cybersecurity Newsletter

November 2022
Issue

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

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

FBI, CISA Publish Public Service Announcement on Information Manipulation Tactics for 2022 Mid-Term Elections

Ahead of the 2022 mid-term elections, the Federal Bureau of Investigation and U.S. Cybersecurity and Infrastructure Security Agency have published a joint public service announcement describing methods foreign actors use to undermine trust in election infrastructure by spreading and amplifying false information, including reports of alleged malicious cyber activity.

The four-page PSA indicates "the FBI and CISA have no information suggesting any cyber activity against U.S. election infrastructure has impacted the accuracy of voter registration information, prevented a registered voter from casting a ballot or compromised the integrity of any ballots cast."

The PSA describes the extensive safeguards in place to protect election infrastructure. It also includes recommendations to help the public understand how to find trustworthy sources of election-related information. Some of the recommendations include the following:

- Rely on state and local government election officials for information about registering to vote, voting and election results.
- Visit the U.S. Election Assistance Commission website (https://www.eac.gov) for verified and reliable elections-related information and resources.
- Be aware that sensational content can be created or shared by foreign actors with the intent to incite anger, mobilize and to promote amplification of false information.
- Seek information from trustworthy and reputable media and social media sources, considering the author and their intent.
- Be wary of phone calls or emails from unfamiliar callers and senders that make suspicious claims about the elections process. Also be aware of social media posts that appear to spread inconsistent information about election-related problems or results.
- Be cautious with websites not affiliated with local or state government that solicit voting information, like voter registration information. Websites that end in ".gov" or websites affiliated with your state or local election offices are usually trustworthy. Use your state and local elections office websites to avoid providing your information to nefarious sites or actors.
- Report potential election crimes — such as intentional disinformation about the manner, time, or place of voting — to your local FBI field office.

To read the full PSA, click here.

NORTH CAROLINA CYBERSECURITY AWARENESS SYMPOSIUM

The 2022 N.C. Cybersecurity Awareness Symposium sessions are available online. This year's annual symposium was a success with a variety of topics in support of Cybersecurity Awareness Month.

Presented by the N.C. Department of Information Technology, the N.C. Cybersecurity Awareness Symposium was a free two-day virtual event on **Oct. 4-5,** that featured cyber leaders and subject matter experts in the private, public and academic sectors. Cyber-related topics included the following:

- Defending against cyberthreats
- Privacy and data protection
- Business continuity and resilience
- Workforce development

Security Isn't Just a Job, It's a Lifestyle: Tips for Ransomware Prevention

SANS Security Awareness has provided an online video with tips for ransomware prevention with SANS Certified Instructor, Ryan Chapman. Chapman has a passion for researching ransomware to help as many people as possible learn to deter, detect, and respond to it.

In this video he discussed best practices for ransomware prevention from a security awareness perspective including tips for password hygiene, phishing avoidance, and device security.

To view the video, click here.

Business Continuity/Disaster Recovery Plans Now Due Nov. 30

This year's annual due date for submitting the Business Continuity/Disaster Recovery Plans has been moved from Oct. 31 to **Nov. 30**.

The Business Continuity Management team, part of the Enterprise Security and Risk Management Office, helps state agencies develop their business continuity and disaster recovery plans, as prescribed by N.C.G.S 143B-1331. The team reviews agency plans annually and evaluates them based on the Statewide Information Security Manual, other legal and regulatory requirements and best practices.

If you have any questions about submitting your agency plan or the annual review process, please reach out to BCM team at BCM@lists.nc.gov.

WHEN IN DOUBT
CHECK IT OUT!

Ask yourself these questions before you share any information.

Is the headline trying to cause a strong emotional reaction?

Is the date current?

Is the author credible?

Has the image been altered?

Are all the facts accurate?

Is the source of the information legitimate?

✓

Check sources and articles by using fact-checking websites before posting or forwarding any information.

KnowBe4

| www.KnowBe4.com

FEMA Releases National Continuous Improvement Guidance

The Federal Emergency Management Agency has published the "National Continuous Improvement Guidance." This guidance provides an approach to conduct consistent and rigorous continuous improvement activities before, during and after real-world incidents. It is intended for the whole community, including state, local, tribal and territorial partners; nongovernmental organizations; the private sector; and other organizations with emergency management functions.

To download the guidance, please visit https://preptoolkit.fema.gov/web/cip-citap/ncig.

FEMA will also host the following 60-minute webinar sessions to provide an overview of the guidance and discuss revisions based on feedback from the national engagement period held earlier this year.

- Webinar 1: 1-2 p.m. EST on Nov. 1. (Guest Speaker: MaryAnn Tierney, FEMA Region 3 Administrator)
- Webinar 2: Noon-1 p.m. EST on Nov. 7. (Guest Speaker: John Benson, Director, Iowa Department of Homeland Security and Emergency Management)
- Webinar 3: 4-5 p.m. EST on Nov. 17. (Guest Speaker: Melanie Bartis, Deputy Coordinator, Harris County Office of Homeland Security and Emergency Management)
- Webinar 4 – Spanish-speaking session: 11 a.m. – Noon EST on Dec. 2. (Guest Speakers: Jose Marchand, Lead Continuity Analyst, and Michelle Ortiz, Continuous Improvement Coordinator, FEMA Region 2, Puerto Rico Caribbean Area Office)
- Webinar 5: 10-11 a.m. EST on Dec. 13. (Guest Speaker: Clint Osborn, Deputy Director, District of Columbia Homeland Security and Emergency Management Agency)

For questions, please contact FEMA-CITAP@fema.dhs.gov.

FEMA Seeks Feedback on Cyber Incidents Planning Guidance

The Federal Emergency Management Agency seeks feedback on the draft "Planning Considerations for Cyber Incidents: Guidance for Emergency Managers." This document provides state, local, tribal and territorial emergency managers with foundational knowledge of cyber incidents to increase cyber preparedness efforts in their jurisdictions. Key aspects of cyber incident preparedness include:

- Understanding the types of cyber incidents likely to occur
- Engaging service owners and operators
- Identifying cyber dependent critical services and related dependencies
- Prioritizing and planning for service and system disruptions
- Identifying roles and responsibilities
- Providing integrated communication and public messaging
- Developing a cyber incident response plan

FEMA is hosting a series of 60-minute webinars to give an overview of the draft document and gather feedback from partners. The sessions will include facilitated discussions with stakeholders to help improve the existing draft. The draft guide is available to allow individuals to provide comments on specific areas within the document by **Nov. 22**. To review the document and learn more about the webinar sessions, please visit FEMA.gov.

Next Monthly Privacy Meeting Is Nov. 22

NCDIT Chief Privacy Officer Cherie Givens will hold the department's next monthly privacy meeting from 10 a.m. to 11 a.m. on **Nov. 22**. All privacy points of contact and other state employees working on privacy matters or interested in privacy are invited to attend.

If you are a designated privacy point of contact and do not have an invitation to the privacy monthly meeting, please email ditprivacy@nc.gov. Thank you for your help in building the State Privacy Program.

Microsoft Launches Cybersecurity Awareness Page

Cybersecurity Awareness Month might be over, but cybersecurity awareness should never end. Everyone has a role to play in cybersecurity. Microsoft has provided many resources to educate and empower people to stay ahead of an evolving threat landscape with fresh security insights and best practices. Improve your cyber resiliency and help educate yourself and others with these resources.

Visit the Microsoft Cybersecurity Awareness page to:

- Download the Be Cyber Smart Kit for practical tips and security best practices to share with colleagues and friends.
- Explore valuable learning paths and certifications for your organizations and your community.

You can also get in-depth insights into how the threat intelligence landscape has changed from the experts who wrote the Microsoft Digital Defense Report. Join a virtual event on Nov. 14 at 2 p.m. EST to learn what is new and how you can help protect your organization.

Training and Continued Learning Resources

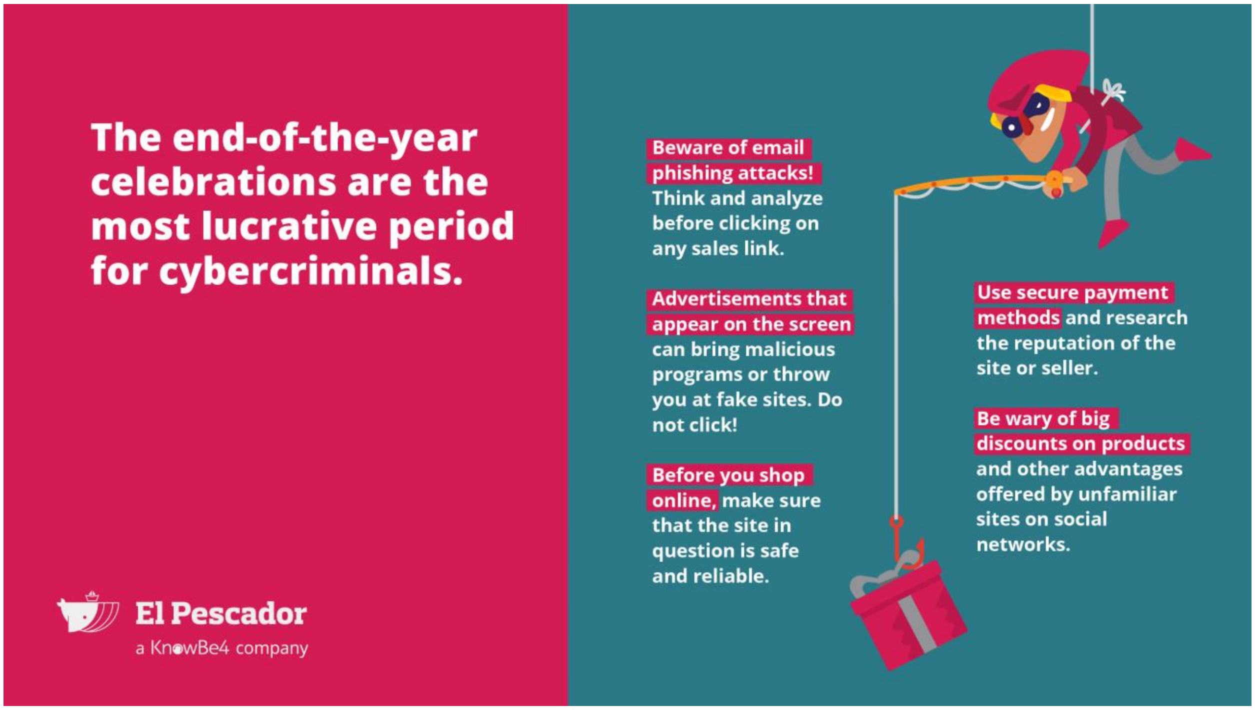
- FedVTE: Free Online Training Environment
  - https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service
  - https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies
  - https://niccs.cisa.gov/
- ICS-CERT Training
  - https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Click here to access. ***Note**: You must have a valid state employee Microsoft 365 account*.

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/



The end-of-the-year celebrations are the most lucrative period for cybercriminals.

Beware of email phishing attacks! Think and analyze before clicking on any sales link.

Advertisements that appear on the screen can bring malicious programs or throw you at fake sites. Do not click!

Before you shop online, make sure that the site in question is safe and reliable.

Use secure payment methods and research the reputation of the site or seller.

Be wary of big discounts on products and other advantages offered by unfamiliar sites on social networks.

El Pescador
a KnowBe4 company

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.*