Monthly Cybersecurity Newsletter

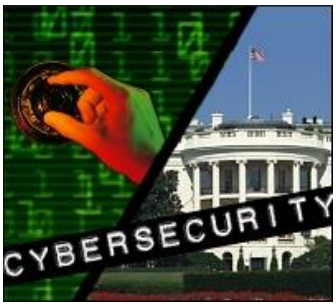
April 2022 Issue

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

White House Alert: Train Your Users Against Cyberthreats



With recent geo-political tensions in Europe, and the current "evolving intelligence" that the Russian government is "exploring options for potential cyberattacks," the White House is encouraging organizations to shore up their defenses and implement various cyber controls to protect their data and systems.

That includes prepping personnel on good cyber hygiene, according to a March 21 fact sheet urging companies to take steps to protect against potential cyberattacks:

> "Educate your employees to common tactics that attackers will use over email or through websites and encourage them to report if their computers or phones have shown unusual behavior, such as unusual crashes or operating very slowly."

Organizations should ensure their employees receive cybersecurity awareness education so they know about the latest attack methods and are vigilant for all unexpected emails requiring any urgency for action. Security awareness training is essential, and it is the first step toward having a robust security culture for an organization's overall cyber resiliency.

According to KnowBe4, a security awareness training provider, an organization with a strong security culture is 52 times less likely to provide credentials to cybercriminals unsuspectingly, exposing the organization to unnecessary brand reputation, loss of revenue or data loss.

Anne Neuberger, the White House's deputy national security adviser for cyber and emerging technology, told reporters it is not certain that there will be a cyber incident on critial infrastructure in the U.S., but that the fact sheet "is a call to action and a call to responsibility for all of us."

The White House is also calling on organizations to harden their cyber defenses immediately with measures such as multi-factor authentication, up-to-date security software and tools, secure data backups and routine training drills.

According to the U.S. Cybersecurity & Infrastructure Security Agency's Shields Up guidance, some of the measures that offer the quickest return on investment and implementation time include reviewing incident plans and recovery strategies in the event of an attack.

Other guidance: Review and mitigate risks to external facing systems and verify they are fully patched and current on all security updates.

Virtual Meeting Platforms and Business Email Compromise Scams

The FBI Internet Crime Complaint Center has observed over the last three years a rise in business email compromise scams involving the use of virtual meeting platforms, according to a February public service announcement.

Criminals began using them in multiple ways due to the rise in remote work because of the COVID-19 pandemic, which caused more workplaces and individuals to conduct routine business virtually.

In one scenario, the FBI says, a bad actor compromises the email of an employer or financial director (such as a CEO or CFO) and requests employees participate in a virtual meeting platform. The criminal inserts a photo of the email sender with no audio, or "deep fake1" audio, and claims the video or audio is not properly working. The criminal then instructs employees to initiate transfers of funds via the chat or in a follow-up email.

Other techniques bad actors are using, the FBI says, include:

- Compromising employee emails to insert themselves in workplace meetings via virtual meeting platforms to collect information on a business's day-to-day operations.

- Compromising an employer's email, such as the CEO, and sending spoofed emails to employees instructing them to initiate transfers of funds, as the CEO claims to be occupied in a virtual meeting and unable to initiate a transfer of funds via their own computer.

The FBI offers the following recommendations to help people avoid falling for these attacks:

- Confirm the use of outside virtual meeting platforms not normally used in your internal office setting.

- Use secondary channels or two-factor authentication to verify requests for changes in account information.

- Ensure the URL in emails is associated with the business/individual it claims to be from.

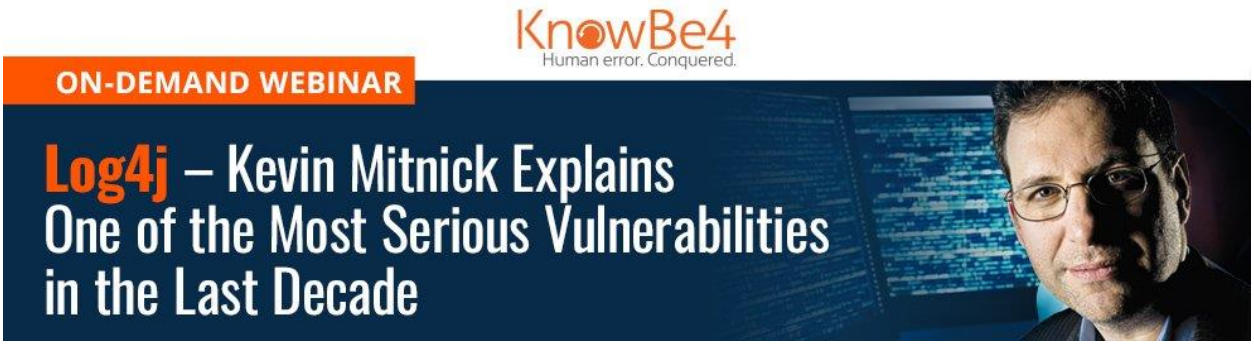
- Be alert to hyperlinks that contain misspellings of the actual domain name.

- Refrain from supplying login credentials or personally identifiable information of any sort via email. Be aware that many emails requesting your personal information might appear to be legitimate.

- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.

- Ensure the settings in employees' computers are enabled to allow full email extensions to be viewed.

- Monitor your personal financial accounts on a regular basis for irregularities, such as missing deposits.



The Log4j vulnerability caused widespread panic for IT professionals when it was uncovered. Sleepless nights followed for many. But a shortage of time and manpower has left this vulnerability wide open in many organizations. Is your organization one of them?

In this on-demand webinar, Kevin Mitnick, KnowBe4's chief hacking officer, and Colin Murphy, KnowBe4's chief information officer, share their experience with the Log4j vulnerability. Hear their first-hand accounts of testing network environments with an incredibly easy hack.

In less than 30 minutes, you will learn:

- Real life examples of this bug bounty bonanza
- Potential consequences of these attacks
- Remediation – blocking the perimeter is not enough
- The future for this class of exploits

You will also see a demo showing how easy it is to hack this exploit. The implications of this vulnerability are huge. Learn how you can protect your organization from this dangerous threat now. Watch now!

CISA Compiles List of Free Cybersecurity Services and Tools for Network Defenders

The U.S. Cybersecurity & Infrastructure Security Agency has compiled and published a list of free cybersecurity services and tools to help organizations reduce cybersecurity risk and strengthen resiliency. This non-exhaustive living repository includes CISA services, widely used open source tools and free tools offered by private and public sector organizations across the cybersecurity community.

Before turning to the free offerings, CISA strongly recommends organizations take certain foundational measures to implement a strong cybersecurity program:

- Fix known security flaws in software.
- Implement multi-factor authentication.
- Take steps to halt bad practices, including the use of end-of-life software products and systems that rely on known/default/unchangeable passwords.
- Sign up for CISA's Cyber Hygiene Vulnerability Scanning service.
- Reduce your attack surface by getting your "Stuff Off Search (S.O.S.)."

CISA encourages network defenders to take the measures above and consult the list of free cybersecurity services and tools to reduce the likelihood of a damaging cyber incident, detect malicious activity, respond to confirmed incidents, and strengthen resilience.

Avoiding QR Code Phishing

A QR code, short for Quick Response code, is a type of matrix barcode that is a machine-readable optical label that can be used to point to a website or application.

Since these codes can be used to link to websites, they should be treated with the same suspicion as unknown links, according to Neil Clauson, regional CISO at Mimecast.

In an interview with Help Net Security, Clauson explains that these links are easy to use, but they are inherently difficult to scrutinize.

"A QR code can easily be embedded anywhere an image can – into the body of an email, as an attachment, printed onto a sticker or in a website," Clauson said. "And just like a malicious URL, they are designed to blend in and not make an unsuspecting user think twice before scanning it."

"Legitimate QR codes are typically leveraged for their ease of use – you simply point your phone's camera at the code and it's instantly scanned taking you to the desired webpage," Clauson continued. "These codes seem so convenient on the surface but that's really what makes them so attractive as a threat vector. It's easiest to trick someone when they aren't suspecting it."

Individuals should be cautious of these codes, especially if they open a login page or ask them to download a file to their device.

"Any QR code that arrives via email is most likely suspicious," Clauson said.

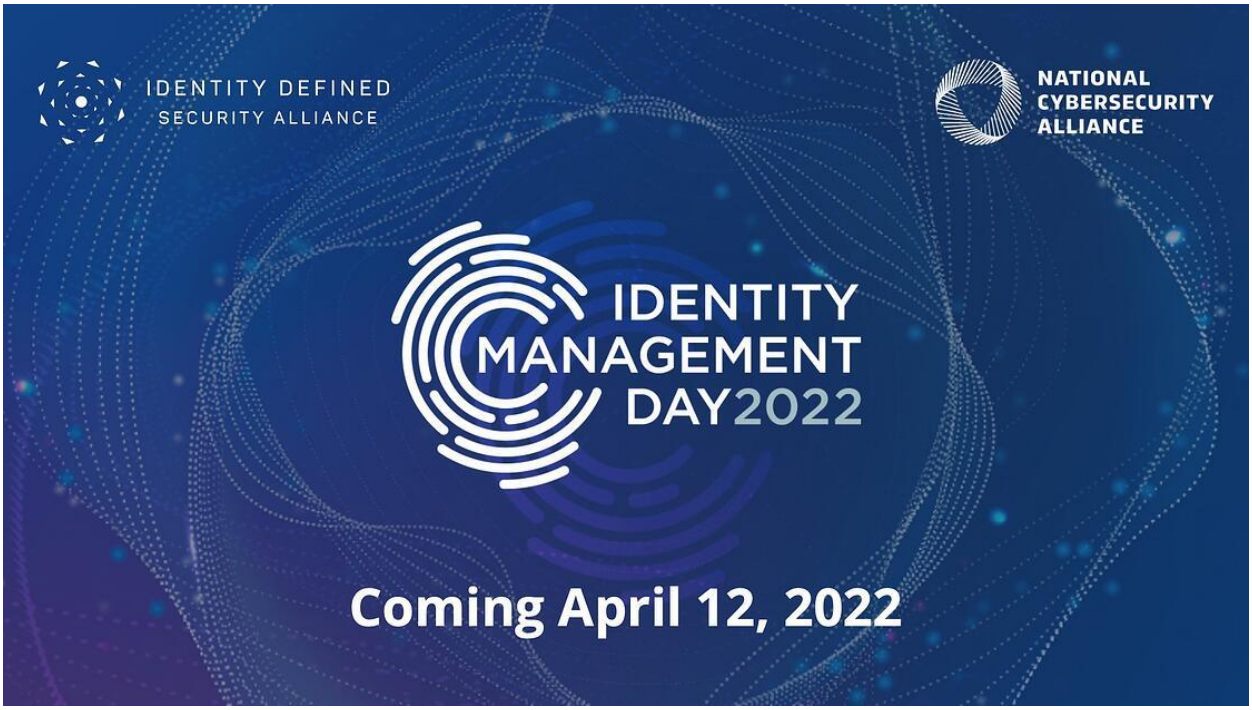
Individuals should always use sound judgment and ask questions:

- Is this too good to be true?
- Is this trying get me to act quickly?
- Does the website ask for any credentials?
- Is it "out of context?" (Did you get an email about work on your personal email or vice versa?)
- If it is a printed QR code, does it look like a second image was "pasted over" the original?

Clauson concludes that a defense-in-depth strategy is the best way to thwart these types of attacks, which includes employee training.

"A strong, multi-layered set of security solutions will resist many types of cyber threats, but as always, end users are the final line of defense against clever attackers," Clauson said. "Human error can play a major role when it comes to all types of cyber threats and making sure employees are educated, aware and thinking twice before clicking or scanning QR codes and links is key to preventing a successful attack."

Technical controls, such as email filtering and anti-virus scanning can protect to an extent. But any technical security solution can be defeated by a malicious link. Cybersecurity awareness training should include teaching individuals that QR codes can be used in phishing scams, and then give them the skills to identify and report anything suspicious to their IT and security teams.



FEMA Offers Online Train-the-Trainer for CERT Basics Course

FEMA's Emergency Management Institute is offering for free an online version of its K0428 CERT Train-the-Trainer course, which prepares participants to deliver FEMA's Community Emergency Response Team (CERT) Basic Training course.

2022 Course Dates:

- April 5, 6, 7, 12, 13 and 14 (1-5 p.m. EST)
- June 7, 8, 9, 14, 15 and 16 (12-4 p.m. EST)
- July 12, 13, 14, 19, 20 and 21 (1-5 p.m. EST)
- Sept. 6, 7, 8, 13, 14 and 15 (12-4 p.m. EST)

Each class size is limited to 20 students and meets four hours a day three days a week for two weeks. Students must attend all sessions.

These courses will be delivered in a via Adobe Connect, and participants should familiarize themselves with it beforehand. No Adobe Connect account or downloads are required. Students must have a FEMA student identification number, computer with microphone, speaker, and stable access to the internet. Visit the FEMA Student Identification System to obtain a SID.

Prerequisites:

- A referral from a CERT-sponsoring agency, typically a local, regional, or state government agency, is required.
- If you are not a first responder, the CERT Basic Training is required.
- For current first responders, IS-317: Introduction to CERT will familiarize you with the CERT Program.

Prospective students should apply through the Emergency Management Institute's online admissions system. The course offers 1.3 continuing education units. Please refer to the FEMA Emergency Management Institute for course date availability.

Have a High School Student in Your Life? If So, Listen Up.

Have a high school student in your life? The free online CyberStart America competition, supported by the N.C. Department of Information Technology, is an amazing opportunity for them to explore potential careers in cybersecurity and computer science while competing for scholarships.

No experience in IT or cybersecurity is needed.

Complete details, including registration, can be found at www.cyberstartamerica.org. (Although **registration is open until April 27**, students should sign up early to allow more time for game play and to qualify for scholarships.)

Last year, 1,165 students from 173 schools participated in CyberStart America. **Help us surpass that number this year.** Spread the word to the high school students in your life. Find videos, links, and other information you can share at it.nc.gov/cyberstart.

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/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

April 6: SANS Webinar: Cloud data loss & SaaS backup: critical steps to protect yourself from disaster

April 8: AWS Technical Essentials Day

April 19: SANS Webinar: Mass Exploitation - How to Defend the Next Log4j

View a list of upcoming SANS webcasts.

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.*