Monthly Cybersecurity Newsletter

March 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

As Tax Season Begins, So Do IRS Scams

It's that time again – tax season. While we are filing our taxes and finding out if we owe any money, cybercriminals are banking on a wide range of scams to try to to steal your money and personal information. The most common way for cybercriminals to steal money, financial account information, passwords or Social Security numbers is to simply ask for them.

Criminals will send phishing messages often impersonating state, local, tribal and territorial government officials and/or IT departments. They might include a link in a phishing email that goes to a website that uses an official organization's logo. If you attempt to log in to the phishing website or provide any personal information, the criminals will see it. The more information they gather from you, the easier it is for them to use it to file a fake tax return in your name. Criminals might even embed malware into tax-related documents and send those via email to unsuspecting victims.

Most of the current scams revolve around simple premises that are designed to both get your attention and strike a little fear into you. According to Nerdwallet, an American personal finance company, some of these premises sound like the following:

- "We recalculated your tax refund, and you need to fill out this form."
- "This is the Bureau of Tax Enforcement, and we're putting a lien or levy on your assets."
- "If you don't call us back, you'll be arrested."
- "Click here to see some details about your tax refund."

Criminals like to impersonate the Internal Revenue Service or other tax agencies, demanding your money now and threatening you with penalties if you do not make an immediate payment. This contact can occur through websites, emails or threatening calls and text messages that seem official *but are not*. Sometimes, criminals request victims to pay "penalties" via strange methods such as gift cards or prepaid credit cards. The IRS has posted details about phishing attacks that impersonate them for years. Yet, people continue to fall for these scams – mostly because they do not know how the IRS contacts taxpayers.

The IRS has taken steps to not just let you know what to expect should they reach out, but they go as far as to tell you the types of tax scams you should be mindful of. So, the following are a few things to remember during the "tax scam" season:

- Pay attention to how you are contacted. The IRS does not call, text, email, leave voicemails or reach out to you on social media. They send you a letter in the mail.
- The IRS does not ask for payment over the phone – not credit cards and certainly not gift cards.
- The IRS cannot arrest you. Any threat of arresting you is an attempt to elicit an emotional response, which is what a phishing message is designed to do.

If you receive a tax-related email at work that is suspicious, report it, according to your organization's cybersecurity policy. If you receive a similar email on your personal account, do the following:

- Tell the Treasury Inspector General for Tax Administration. You can report IRS scams https://www.treasury.gov/tigta/reportcrime_misconduct.shtml.
- Forward email messages (*with email headers or as an attachment*) that claim to be from the IRS to phishing@irs.gov. Do not open the attachments or click on any links in those emails.
- Tell the Federal Trade Commission via the FTC Complaint Assistant on FTC.gov. Add "IRS Telephone Scam" in the notes.
- Report Social Security Administration phone impostor scams using the form on the Social Security Administration's website.
- If the IRS scams appear to be impersonating a state tax authority rather than the IRS, contact the N.C. Attorney General's Office.

2021 Trends Show Increased Globalized Threat of Ransomware

The Cybersecurity & Infrastructure Security Agency, the FBI, the National Security Agency, the Australian Cyber Security Centre and the United Kingdom's National Cyber Security Centre have released a joint cybersecurity advisory highlighting a global increase in sophisticated, high-impact, ransomware attacks against critical infrastructure organizations in 2021.

The advisory states that "ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally." The advisory provides observed behaviors and trends as well as mitigation recommendations to help reduce the risk of compromise by ransomware.

Phishing emails, remote desktop protocol (RDP) exploitation as well as exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021.Some of the mitigations that the advisory recommends include:

- Keep all operating systems and software up to date.
- Limit access to resources over internal networks (e.g., restrict RDP use).
- Require strong passwords, or implement multi-factor authentication (MFA).
- Implement a user training program and phishing exercises to raise awareness among users.

CISA encourages users and administrators to review joint CSA: 2021 Trends Show Increased Globalized Threat of Ransomware and visit StopRansomware.gov for more information on protecting against and responding to ransomware attacks.

Tax Season Identity Theft

The threat of identity theft exists all year long, but increases during tax season when scammers ramp up attacks. If successful, criminals can open accounts and file fraudulent tax returns in your name, leaving you on a long, difficult path to recovery.

Avoiding ID theft begins by ensuring that your private information remains private. That means sharing less on social media and maximizing the security settings of social media accounts, staying alert for phishing attacks that attempt to bait you into clicking on malicious links, and using common sense (you know, like not broadcasting your national ID number on Facebook).

During tax season, remember that tax collectors won't call you, email you, or text you to ask for a credit card payment for overdue taxes. Scammers will do anything they can to convince their targets to reveal confidential information, including posing as government entities, co-workers, friends, and family members.

If possible, file your taxes early to get a jump on any criminals that might have obtained your personal information. And to avoid ID theft all year long, consider placing a freeze on your credit reports, which will prevent anyone from opening accounts in your name.

Here at work, help protect the identities of our clients, customers, and business associates by following our organization's policies and considering the ramifications of what might happen if personally identifiable information ends up in the wrong hands.

Microsoft: 'Sophisticated Hackers Still Rely on Credential Theft'

State-sponsored hackers and sophisticated cybercriminals continue to exploit weak passwords and phishing attacks to compromise networks, according to a new report by Microsoft.

"Cyberattacks by nation-state actors are on the rise," Microsoft says. "Despite their vast resources, these adversaries often rely on simple tactics to steal easily guessed passwords. By so doing, they can gain fast and easy access to customer accounts.

In the case of enterprise attacks, penetrating an organization's network allows nation-state actors to gain a foothold they can use to move either vertically, across similar users and resources or horizontally, gaining access to more valuable credentials and resources.

Microsoft's researchers explain that these threat actors often have no reason to use more sophisticated methods, since credential theft is so effective.

"Spear-phishing, social engineering attacks and large-scale password sprays are basic nation-state actor tactics used to steal or guess passwords," the researchers write. Microsoft states that ransomware actors use the same techniques, exploiting social engineering, exposed remote desktop protocol (RDP) ports or technical vulnerabilities to gain access to organizations' networks.

"No matter how much ransomware is out there, or what strains are involved, it really comes down to three primary entrance vectors: RDP brute force, vulnerable internet-facing systems and phishing," Microsoft writes. "All of these vectors can be mitigated with proper password protection, identity management and software updates in addition to a comprehensive security and compliance toolset. Organizations should consider the following recommendations:

- Enable multi-factor authentication.
- Audit account privileges.
- Review, harden and monitor all administrator accounts.
- Establish and enforce a security baseline to reduce risk.
- Raise awareness on how to avoid phishing attacks.

2022 Proofpoint 'State of the Phish' Webinar

Join Proofpoint on **March 23 at 1 p.m. EST** for its eighth annual "State of the Phish" webinar for an overview of the latest threat landscape, as well as insights into user knowledge trends and security controls that allow you to effectively mitigate risk.

This year's webinar will present analysis of data from a variety of sources, including third-party surveys of more than 4,100 employees, 100 million simulating phishing attacks and 15 million reported emails. Find out more information or register for this event.

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.)

What is CyberStart America?

CyberStart America is a series of free challenges in which students act as "cyber protection agents" to solve cybersecurity-related puzzles and explore related topics, such as code breaking, programming, networking, and digital forensics.

They can use the game to qualify for the National Cyber Scholarship program to help with college.

Why is CyberStart America important?

There are approximately 21,000 vacant cyber-related positions in North Carolina. Nationally, that number tops nearly 600,000.

Introducing students – even those with little or no interest in computer careers – now to cybersecurity careers helps create educational pathways and opportunities to build a diverse and talented cyber pipeline to help address future threats and challenges.

Last year, Emily Chen, a senior at Panther Creek High School in Cary, was named a National Cyber Scholar with Honors after ranking among the top 30 of more than 30,000 U.S. high school students who competed in CyberStart America.

"Prior to this program, I honestly had no idea I could pursue a career in cybersecurity," Chen said. "I've gained skills that made me realize it's something I really enjoy doing. If you're hesitant, I just say give it a try. It's free. You just have to sign up."

How You Can Help

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.

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:

- March 1, 2, 3, 8, 9 and 10 (12-4 p.m. EST)
- 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 them 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.

PCI Webinar 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 hosting a 1-hour webinar for the state of North Carolina's merchant community on **Tuesday, March 15, 2022,** at 10 a.m. EST. The title of the webinar will be **Networks - Who Can Talk to Who?** Bill Franklin, senior director of payments, will be the speaker.

Additional details, including registration information, will be sent out in advance of each webinar. To be notified, sign up for PCI webinar announcements via the eCommerce listserv, which also provides updates about products and services on the merchant card and enhanced file transfer (EFT) master services agreements, annual PCI compliance, self-assessment questionnaires and quarterly scans.

ISAC Best Practices Webinar: 'Bootstrapping Your Cybersecurity Awareness Program'

The Information Sharing and Analysis Centers (ISAC) is holding a Best Practices webinar on **Thursday, March 10, 2022,** at 3 p.m. EST for attendees to learn more about how to create a cybersecurity awareness program. Whether your company has 15 employees or 50,000, a good cybersecurity awareness program is critical in maintaining a secure and safe working environment. Andy Warren, of Appalachia Tech, presents problems and stakes involved in User Security Awareness Training. Warren outlines an eight-step program for creating a sustainable program from scratch, as well as how to keep it viable for the long term. Seats are limited. To ensure you get in, register as soon as possible.

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

Mar. 9: SANS Webinar: SANS 2022 Ransomware Defense Report

Mar. 10: ISAC Best Practices Webinar: Bootstrapping Your Cybersecurity Awareness Program

Mar. 10: SANS Webinar: Cloud Security for Beginners: Part 2: Working in the Cloud

Mar. 15: Coalfire PCI Webinar: Networks - Who Can Talk to Who? (see information above)

Mar. 22: SANS Webinar: Mitigating Risks in Software Supply Chain Security

Mar. 23: 2022 Proofpoint "State of Phish" Webinar

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.*