Monthly Cybersecurity Newsletter

June 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

When Cryptocurrency Investments Really Are Too Good To Be True

The U.S. Federal Trade Commission (FTC) reports that victims have lost more than $***80 million*** in cryptocurrency scams since October 2020.

Cryptocurrency is a type of digital currency that generally only exists electronically. Individuals usually exchange cryptocurrency with someone online, with a phone or computer, without using an intermediary, like a bank. Bitcoin and Ether are well-known cryptocurrencies, but there are many others.

Scammers take advantage of misunderstandings that often surround cryptocurrency investments, and they use a variety of techniques, such as impersonating public figures, like Elon Musk. There are also fake investment sites that people cannot actually withdraw their "investment," giveaways that claim to multiply a person's cryptocurrency and even classic online dating scams that attempt to con would-be romantic partners into crypto investment scams.

The FTC says: "In fact, the FTC's new data spotlight shows that, since October 2020, nearly 7,000 people reported losses to bogus cryptocurrency investments, adding up to more than $80 million. People ages 20-49 were more than five times more likely than other age groups to report losing money on those scams. But here is an even more striking point: People in their 20s and 30s have lost more money on investment scams than on any other type of fraud. And more than half of their reported investment scam losses – $35 million – were in cryptocurrency."

The FTC offers the following advice to avoid falling for these scams:

- Research before you invest. Search online for the name of the company and cryptocurrency as well as the terms "review," "scam" or "complaint."
- Be wary of guarantees and big promises. Scammers often promise you will make money quickly or that you will get big payouts or guaranteed returns. They might offer you free money paid in cash or cryptocurrency – but even if there is a celebrity endorsement, do not buy it. You will make money if you are lucky enough to sell your crypto for more than you paid. Do not trust people who say they know a better way.
- Anyone who says you must pay by cryptocurrency, wire transfer or gift card is a scammer. If you pay, there is usually no way to get your money back.

CISA/FBI Issue Advisory on Spear Phishing Campaign

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the FBI are warning about an ongoing spear phishing campaign targeting government organizations, intergovernmental organizations and non-governmental organizations. A sophisticated cyberthreat actor leveraged a compromised end-user account from Constant Contact – a legitimate email marketing software company – to spoof a U.S. government organization and distribute links to malicious URLs.

In response, CISA and the FBI have released Joint Cybersecurity Advisory AA21-148A: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs and Malware Analysis Report MAR-10339794-1.v1, providing tactics, techniques and procedures, downloadable indicators of compromise, and recommended mitigations. CISA strongly encourages organizations to review these resources and apply the necessary mitigations.

Some ways to respond to this threat include the following:

- Implement multi-factor authentication for every account.
- Keep all software up to date.
- Implement centralized log management for host monitoring.
- Use strong account mananagement policies for user and admin accounts.
- Implement a cybersecurity training program for end users that includes simulated attacks for spear phishing.

Be sure to review the tips on avoiding phishing attacks, published by the N.C. Department of Information Technology.

Upcoming Ransomware Webinar

BITSIGHT®
The Standard in SECURITY RATINGS

How can security professionals avoid joining the growing list of ransomware victims?

BitSight, a cybersecurity ratings company that analyzes companies, government agencies and educational institutions, recently found that organizations with less mature patching programs are ***seven times more likely*** to experience a ransomware incident.

On **Thursday, June 10 at 11 a.m. EST**, BitSight will host a webinar, *Ransomware: Leveraging Data Insights to Avoid Becoming a Victim Customer,* that will share insights into the following:

- New sector-specific insights from BitSight's data science team tied to recent ransomware trends
- Security performance gaps and challenges that lead to successful ransomware incidents
- Vulnerabilities that indicate heightened risk of ransomware
- Programmatic areas that security professionals should address to reduce the likelihood that they will be a victim of a ransomware incident

Register for the webinar here.

Interested in more information? Be sure to check out BitSight's recent blog post, Evidence-Based Strategies to Lower Your Risk of Becoming a Ransomware Victim.

Spear Phishing *in Action*

Unlike traditional phishing scams that are usually sent at random from an aggregated list, spear phishing targets specific people. In this attack, the scammer researches the target to gather as much information as possible, such as place of work, job title, and any personal details available to the public. They then use this information to gain and abuse the victim's trust, sometimes posing as a co-worker, friend, or even law enforcement.

To the right is an example of what a spear phishing email might look like. At first glance, the email seems legitimate. It addresses the recipient by name. The signature includes a phone number. How would Jordan know this is a scam?

1. ***Who is Robert? In the email he claims to be part of IT, but Jordan knows that IT at his company uses the email IT@company.com.***
2. ***Normally, system updates are done remotely. Why would Robert need Jordan to download and install something manually?***
3. ***This sense of urgency represents a classic red flag that the email is a phishing attack. The scammer wants Jordan to feel pressured into taking immediate action.***

What should you do if you receive an email like this? Use extreme caution when handling requests to download attachments, click on links, or divulge sensitive information. Report all suspicious emails to the appropriate parties immediately. And always follow organizational policies.

Monday 11/15/2020 9:42 AM
From: Robert MacMahn <tech@company.com>
To: Oswin, Jordan
Subject: Jordan Oswin - System Update required

Hey Jordan,

This is Robert from IT. We are pushing out new security software and I need you to download the attachment and run it on your workstation immediately.

Thanks,
Robert MacMahn
IT Desk
(234) 326-4634

sec-update-786.zip

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 several webinars in 2021.

Date	Time	Topic (Tentative)
June 15, 2021	10-11 a.m. EST	Vulnerability Scanning and Penetration Testing – What Is the Difference?
Sept. 7, 2021	10-11 a.m. EST	Authentication and Access Control – Who Are You?
Dec. 7, 2021	10-11 a.m. EST	Risk Assessments – Do You Feel Lucky?

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.

Cybersecurity Asset Management Trends 2021: *The Pandemic's Impact on Cybersecurity and Priorities for the Future*

Last year's overnight shift to remote work drove rapid changes in security and IT priorities – resulting in more challenges than ever before. Now, as teams prepare for a post-pandemic "new normal," IT and security teams are facing fresh obstacles.

Axonius – a cybersecurity company that provides a platform for asset inventory, uncovering security solution coverage gaps and validating and enforcing security policies – partnered with Enterprise Strategy Group for a global survey of IT and cybersecurity professionals to explore how the pandemic had an impact on IT complexity and what security initiatives teams are prioritizing post-pandemic.

Register now for *Cybersecurity Asset Management Trends 2021: The Pandemic's Impact on Cybersecurity and Priorities for the Future* on **June 16 at 1 p.m. EST**. Noah Simon and Jake Munroe, of Axonius, will dive into the survey's findings to share key insights and takeaways from security leaders and practitioners worldwide, including the following:

- 72% of respondents report increased complexity over the past two years.
- 55% cite increased remote workers as the top cause of complexity (compared to only 22% in 2020)
- 87% say the pandemic has accelerated cloud infrastructure adoption
- 82% plan to increase investment in asset inventory

Register for this webinar here.

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.
***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

June 10: BitSight webinar: Ransomware: Leveraging Data Insights to Avoid Becoming a Victim Customer

June 10: SANS webinar: Measuring Risk Using the Open, Collective Risk Model (CRM)

June 15: Coalfire PCI webinar: *Vulnerability Scanning and Penetration Testing – What Is the Difference?*

June 18: SANS webinar: What's New with the CIS Controls v8

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.*