Monthly Cybersecurity Newsletter

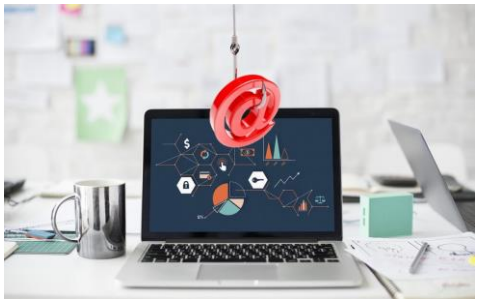
May 2021 Issue

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

Business Email Compromise Scams on the Rise



Government organizations are frequently targeted by Business Email Compromise (BEC) scams that attempt to deceive people into sending money, personally identifiable information (PII) or material goods – and even modifying direct-deposit information.

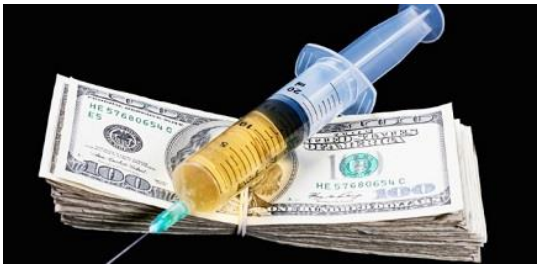
The Enterprise Security and Risk Management Office (ESRMO) sent an advisory in April about an increase in business email compromise activity targeting North Carolina state government and attempting to defraud both payroll deposit as well as purchasing payments. In all cases, the use of compromised email accounts was involved – whether it was internal or external partners.

In a white paper, Security Primer – Business Email Compromise, the Center for Internet Security provides good guidance to help secure the work force.

- Train staff how to identify potential business email compromise scam emails and the policies concerning them. Indicators of business email compromise can include:
    - Poorly crafted emails with spelling and grammar mistakes
    - The wrong or an abbreviated signature line for the supposed sender
    - An indication that the email was sent from a mobile device
    - The use of full names (instead of nicknames)
    - A language structure that may not match how the supposed sender normally communicates
    - Direction that the only way to contact the sender is through email
    - Requested transactions are for a new vendor or new contact at a known vendor
- Ensure employees have a policy for out-of-band verification (e.g., verbal confirmations, etc.) of requests and that an office culture exists so they are comfortable asking if requests are authentic.
- Ensure HR and finance policies are supported by technological solutions.

In addition, state employees are strongly encouraged to make any changes to their personal or financial-related data in the Employee Self Service (ESS) portal (also known as Beacon), which has process controls to mitigate fraud.

Please report any confirmed security incidents to the N.C. Department of Information Technology (DIT) at https://it.nc.gov/report.



U.S. Justice Department Warns of COVID-19 Vaccine Scams

The U.S. Department of Justice is warning people that fraudsters are creating fake COVID-19 vaccine surveys for consumers with the promise of receiving a prize or cash. The surveys, however, are really used to steal money and personal information from consumers.

People receive these fraudulent surveys via email and text messages that claim the recipient need only pay shipping and handling fees to receive their prize.

Victims who provide their credit card information are charged for shipping and handling fees but never receive the promised prize. They also expose their personally identifiable information to scammers, thereby increasing the probability of identity theft.

Unless from a known and verified source, never click on links in text messages or emails claiming to be a vaccine survey. More tips for avoiding COVID-19 scams are available on the NCDIT website.

If you receive a suspicious message and link about a COVID-19 vaccine survey, the DOJ encourages you to call the National Center for Disaster Fraud, at 866-720-5721, or submit an online report. If you believe you may have entered information into a fraudulent website, find resources on how to protect your information at www.identitytheft.gov.

To learn more about identifying and protecting yourself from phishing attempts, visit the following:

- https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

PCI Webinars by Coalfire

The N.C. Office of the State Controller (OSC) 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 (SAQ), and quarterly scans.

Phishing Attacks Using PDF Files Skyrocket 1,160%

PDF attachments are increasingly becoming a common type of phishing, according to researchers at Palo Alto Networks, a cybersecurity company that produces advanced firewalls and cloud-based solutions.

From 2019 to 2020, they noticed a spike in malicious PDFs – from 411,800 to 5.2 million – a dramatic 1,160% increase.

PDF files are an enticing phishing vector because they are a common document format that works across a wide platform of devices. They also make phishing schemes appear more believable opposed to a text-based email with just a link.

The most common form of PDF phishing lures used an image of a fake CAPTCHA – a type of challenge used in computing to determine whether a user is real – to trick victims into clicking a "Continue" button, which leads to a malicious site.

Another common PDF lure is an image claiming to be a coupon that a victim clicks to get a product discount. A third type of PDF phishing attack uses images that appear to be paused videos but lead the to a phishing site when users click them.

The bottom line, researchers say: Stop and think when you receive a suspicious file. Verify and double-check files you receive unexpectedly, even if they appear to be from someone you know and trust.

More Than One-Fifth of PCs Still Run Windows 7

Kaspersky Lab, a Russian cybersecurity and anti-virus provider, says that 22% of PC users are still running end-of-life Windows 7, which was released in July 2009.

Microsoft discontinued support for Windows 7 in January 2020, meaning the operating system no longer receives updates for vulnerabilities or technical support.

Kaspersky says that 72% of PC users are running Windows 10, the current OS from Microsoft.

Except for extraodinary circumstances, all computing devices should run on a supported OS.

Devices that run on unsupported operating systems are vulnerable to attack and pose a significant risk to other computing devices that are connected to them. Cyberattackers actively look for and exploit known vulnerabilities on unsupported devices to carry out their nefarious schemes.

Computers running Windows 7, or any unsupported OS, should be isolated from other networked devices.

The good news is that new versions of applications are unlikely to run on Windows 7 because its not supported or the hardware is not sufficient for its needs.

For more information about the risks of running outdated and unsupported software, please visit the blogpost from BitSight.

MOST COMMON TYPES OF CYBERATTACKS

PHISHING

Phishing attacks come in many different forms that vary in sophistication. They typically attempt to leverage human emotions to convince someone to click on a malicious link, download an attachment, or disclose confidential information.

BUSINESS EMAIL COMPROMISE

Also known as CEO fraud, this scam involves a cybercriminal accessing or impersonating an executive's email account and phishing that executive's employees. For example, the attacker could send requests for wire transfers of money to an employee in finance. Since the email appears to come from someone the employee knows, they're likely to assume it's a legitimate request.

RANSOMWARE

Ransomware is a form of malware that encrypts data or locks systems until a specified ransom is paid. This attack represents one of the biggest concerns for organizations worldwide due to its disruptive nature. Hospitals, for example, enter dangerous territory if they can't access the charts and data needed to effectively treat patients.

CREDENTIAL STUFFING

Major data breaches sometimes leak hundreds of thousands of login credentials (usernames and passwords). Cybercriminals then use those credentials to perform an automated attack known as credential stuffing, which attempts to log into multiple other accounts using the stolen username and password combos.

DISTRIBUTED DENIAL OF SERVICE (DDOS)

Many organizations rely heavily on the internet to provide goods and services. When the internet goes down, so do operations. That's the intent behind DDoS attacks, which flood internet servers with more traffic than they can handle, causing them to crash and disrupting services.

ADVANCED PERSISTENT THREATS (APTS)

APTs are labeled "advanced" because they utilize a full spectrum of intelligence-gathering and infiltration techniques, and can take months or even years to discover. The end goal of these attacks can be anything from data theft to well-funded political agendas that disrupt government entities.

Stay Safe While Working from Home

Working remotely has its benefits, ***but*** it comes with added responsibility. Visit the NCDIT website 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

May 4-6: National Hurricane Program to Host Online Training

May 10-14: AI Week: Week-long tech festival dedicated to artificial intelligence (AI)

May 11: NCSA webinar: Cybersecurity: How's Your Hygiene?

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

May 18: SANS webinar: The Cloud Conundrum: Parsing the Cloud Visibility Problem

May 21: SANS webinar: Debunking Top Cloud Misconfiguration Myths

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.*