Monthly Cybersecurity Newsletter

June 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

Preventing Data Exfiltration

Data exfiltration is the unauthorized copying, transfer, or retrieval of data from a computing device. It can be accidental or malicious activity that occurs in two main ways: *outsider attacks* and *insider threats* (from within the organization). Both are major risks. Organizations with sensitive or confidential data are particularly at risk of these types of attacks.

Data exfiltration from outside an organization can occur when an attacker infiltrates the organization's network to steal data or sensitive information, such as personally identifiable information (PII) or protected health information (PHI). This can be a result of cybercriminals directly breaching devices or networks or injecting malware onto a device, such as a computer, smartphone or a USB drive that is connected to the organization's network.

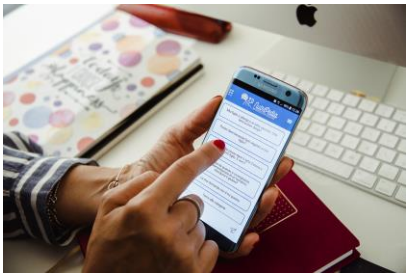
Insider threats are one of the top causes of data exfiltration. Insider threats can involve malicious insiders (i.e., employees or contractors) stealing their own organization's data and selling sensitive information to competitors, cybercriminals, or nation-states. According to Proofpoint, which provides software as a service and products for email security and data loss prevention, ***two out of three*** insider threat incidents are ***accidental***, and most of these are via email.

Accidental data loss from an insider threat could prove equally costly to an organization. Careless employee behaviors can result in sensitive data falling into the hands of bad actors. For example, an employee can exfiltrate data by sending it out through email, losing the company's computing or storage device, or by loading company data onto a personal external storage device, such as a USB drive or external hard drive.

The following tips can help organizations minimize the risk of data exfiltration.

- **Implement multi-factor authentication**: MFA adds a layer of protection to user credentials that makes it less likely that passwords will be compromised, and sensitive data will be breached.
- **Implement data loss prevention**: Data loss prevention is used to detect data-use policy violations and to prevent data loss. It involves data discovery and classification to find, categorize and understand sensitive data and then prevent such data from leaving an organization's network/devices.
- **Identify and redact sensitive data**: Not all data carries the same level of risk for exfiltration. Identifying systems on which sensitive data resides and ensuring that it is properly secured helps prevent exfiltration. Where sensitive data is not needed, it should not be stored.
- **Block unauthorized communication channels**: Some strands of malware use external communication channels to exfiltrate data, which can be blocked.
- **Educate users**: Ensure employees can detect the signs of a cyberattack and that they know not open malicious attachments or click links in unsolicited emails. Organizations should also educate employees about company policies about data sharing as best practices for keeping data secure.

A New Threat in Town: Interactive Phishing



Phishing threats are typically delivered via website links in email messages. Once a user clicks the link, the malicious website often shows a single webpage that asks for sensitive information, such as account login credentials, credit card details and other personally identifiable information (PII). However, there is a new method of catching sensitive information from an unsuspecting victim.

Trustwave, an American company that provides managed security services, database security and email security, recently found a package delivery phishing scam that contained an *interactive* component: a chatbot. A chatbot is a software application that is used to conduct an online chat conversation via text or text-to-speech and is designed to simulate the way a human would behave in a conversation. Unlike other phishing websites, the one Trustwave discovered establishes a conversation first and then guides the victim to the actual phishing pages.

Although the use of a chatbot to conduct the "phish" is unique, it still uses the common vector of email as the delivery channel. Clicking a link in the initial email opens the end user's browser and directs them to a downloadable PDF file, which then redirects the user to the same website where the chatbot-like page tries to "communicate" with the victim. Through a series of predefined questions and responses, the page tries to elicit trust from the user. To gain more confidence from the victim, a fake CAPTCHA is presented right after the victim clicks the "Schedule delivery" button.

If the victim clicks the button, they are prompted for **login credentials** (i.e., email address and password), **delivery address**, *as well as* **credit card data**.

Adding common and widely used features such as a chatbot and CAPTCHA pages to a popular shipping brand makes this phishing threat seem more legitimate. Individuals must be very careful what they click online (i.e., in an email and on a webpage), and they need to be aware of sophisticated phishing campaigns such as the one described above.

Click here for tips on avoiding phishing threats.

Monthly Privacy Meeting - June 28, 10-11 a.m.

NCDIT Chief Privacy Officer Cherie Givens will hold the department's monthly privacy meeting from 10-11 a.m. on June 28.

All privacy points of contact and other state employees working on privacy matters or interested in privacy are invited. If you have been identified by your agency as the privacy point of contact, you should be receiving an invitation in early June.

If you are a state employee with an interest in privacy, please send your name and contact information to ditprivacy@nc.gov to be added to the meeting invitation list.

Adoption of the Fair Information Practice Principles

Pursuant to N.C.G.S. 143B-1376 - *Statewide Security and Privacy Standards*, the state chief information officer is responsible for the security and privacy of all state information technology systems and associated data. The state CIO manages all executive branch information technology security and shall establish a statewide standard for information technology security and privacy to maximize the functionality, security and interoperability of the state's distributed information technology assets, including, but not limited to, data classification and management, communications and encryption technologies.

In support of this duty, the N.C. Department of Information Technology's Office of Privacy and Data Protection adopted the Fair Information Practice Principles (FIPPs) in January 2022. The FIPPs provide guidance to agencies on reducing privacy risks and supporting the creation of reliable records to inform decision-making. The FIPPs are widely accepted in the United States and around the world as a general framework for privacy. They are reflected in policies and guidance adopted by NCDIT. These principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. The eight guiding principles are:

1. **Transparency:** The organization should be transparent and provide notice to the individual regarding its collection, use, dissemination and maintenance of personally identifiable information (PII).
2. **Individual Participation:** Consent should be sought from the individual for the collection, use, dissemination and maintenance of PII. A mechanism should also be provided forappropriate access, correction and redress regarding the organization's use of PII.
3. **Purpose Specification:** The organization should specifically articulate the authority that permits the collection of PII and the purpose(s) for which the PII is intended to be used.
4. **Data Minimization:** The organization should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as it is necessary to fulfill those purpose(s).
5. **Use Limitation:** The organization should use PII solely for the purpose(s) specified in the notice. Sharing PII outside of the organization should be for a purpose compatible with the purpose(s) for which the PII was collected.
6. **Data Quality and Integrity:** The organization, to the extent practicable, should ensure thatPII is accurate, relevant, timely and complete.
7. **Security:** The organization should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification or unintended or inappropriate disclosure.
8. **Accountability and Auditing:** The organization should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

If you have any questions about the adoption of the FIPPs, please send an email to ditprivacy@nc.gov. For more information, please see NCDIT's Data Protection & Privacy page.

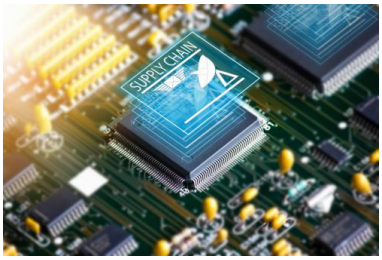
Smishing Alert Targets State Employees

The Enterprise Security and Risk Management Office is warning state employees about a malicious text message (aka "smishing") scam purporting to be an account alert from the State Employees Credit Union. See the image, to the right, of a malicious text message several state employees have received.

If you receive this message or any other suspicious text message requesting personal information or asking you to resolve an alleged account issue, simply delete the text message without taking further action. If you are concerned, contact your financial institution through a verified method of contact, such as the phone number or website listed on your bank card or financial statement.

Fraudsters are getting increasingly more sophisticated, so it is important to stay focused on being able to identify the signs of malicious activity. Thank you for your continued vigilance.

For more information about smishing and tips to avoid it, review KnowBe4's Smishing 101 and Defenses.



NIST Updates Supply Chain Risk Guidance

The U.S. National Institute of Standards and Technology (NIST) has published updated guidelines for software supply chain risk management.

NIST defines supply chain risk management as "the process of identifying, assessing and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains." Modern products and services depend on their supply chains, which connect a worldwide network of manufacturers, software developers and other service providers.

Supply-chain attacks are becoming increasingly popular targets for threat actors, as it allows them to compromise a single product and have it impact numerous downstream companies who use it. An example of supply chain risk is the SolarWinds compromise, where Russian attackers compromised the popular Orion IT management tool that led to dozens of corporate and government network intrusions.

The new NIST publication, titled Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, provides guidance on identifying, assessing and responding to cybersecurity risks throughout the supply chain at all levels of an organization. It is part of NIST's response to Executive Order 14028: Improving the Nation's Cybersecurity and will help organizations improve their supply chain security efforts. Because cybersecurity risks can arise at any point in the life cycle or any link in the supply chain, NIST's guidance now considers potential vulnerabilities, such as the sources of code within a product or retailers that carry it.

Due to the length and complexity of the publication, NIST is planning to provide a quick start guide to help readers start to develop supply chain risk management processes. The primary audience for the revised publication is acquirers and end users of products, software, and services. Ultimately, the solution rests with suppliers, such as their transparency and accountability.

Best Practices Webinar on Device Security Planned for June 8

The ISACs will be holding a Best Practices webinar on **Wednesday, June 8 at 3 p.m.** for attendees to take away some key insights on device security. In our modern work culture, proper device-level protection demands a security solution that extends beyond the reach of your network.

At this webinar, you'll hear from a state election official about how CIS endpoint detection and response (EDR), made a significant impact in cyber defense of the state's election infrastructure. Learn about endpoint protection best practices from CIS ESS/EDR vendor CrowdStrike and how the service helps defend against device-level cyberthreats.

Register for the webinar here. Please direct any questions to info@cisecurity.org.

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

FEMA's Emergency Management Institute is offering a free 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:

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

Each class 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 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.
- 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.

FEMA to Host HURREVAC Webinar Series

FEMA's National Hurricane Program will host a five-day HURREVAC training for emergency managers from **June 6-10**. Each day, sessions will start at 2 p.m. and run from 60 to 90 minutes.

Webinar topics include the following:

- Introduction to HURREVAC and Overview of the National Hurricane Program (June 6)
- Wind Forecast Features (June 7)
- Evacuation Timing Features (June 8)
- Storm Surge and Other Water Hazards (June 9)
- Exercise Tools and Applying HURREVAC (June 10)

HURREVAC is a free web-based decision-support tool that assists emergency managers by providing information and tools to inform hurricane response decisions in advance of a threatening storm. Interested emergency managers can register now for this annual webinar series.

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

Upcoming Events

- June 8: Organizations Preparing for Emergency Needs (OPEN) Part 1 Webinar (1-2:30 p.m.)
- June 15: Organizations Preparing for Emergency Needs (OPEN) Part 2 Webinar (1-2:30 p.m.)
- June 19: National Lighting Safety Awareness Week
- June 22: Psychological First Aid Webinar (1-2 p.m.)
- June 28: Privacy Monthly Meeting (10-11 a.m.)

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.*