Monthly Cybersecurity Newsletter

May 2019 Issue

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

Being Safe and Secure on Summer Vacation

It's that time of year to pack our bags and go on vacation. While we look forward to relaxing at our favorite vacation spot, we should not relax our safe computing habits. The summer season can be a lot of fun, but it also when cybercriminals exploit people who are unaware of the risks. The following is a checklist of things you can do to help you be safer and more secure while on vacation.

- ✓ Leave some lights turned on at home or set up a schedule to automatically turn on/off your lights. This makes it appear you are home, as criminals target houses that appear vacant.
- ✓ Wait until after your vacation to post your moments on social media. Also, avoid "checking in" to a location on social media as this lets people know where you are.
- ✓ Update your device operating system (OS) and apps, and make sure you have your firewall and anti-virus (AV) enabled and up to date.
- ✓ Be leery of public Wi-Fi networks. Connect to secure Wi-Fi networks with strong encryption (e.g. WPA2). If you do not need to use Wi-Fi or Bluetooth, disable it on your devices.
- ✓ Avoid charging your devices with a public charging station such as those found in an airport or hotel. Public charging stations/kiosks can be used to install malware and/or to steal data.
- ✓ Keep your devices close and locked when not in use. Be sure to use a strong password, pattern lock, or PIN on all your devices.
- ✓ Use a device locating application. If you lose your device while on vacation, a location application can help you find it, lock it, or erase your device's data, if necessary.
- ✓ Use credit cards or cash, *not* your debit cards. While your bank may protect you from fraud, it can be a hassle if your bank does not catch fraudulent transactions in time.
- ✓ Be careful using credit card readers and look out for card skimmers. Also, protect your PIN against shoulder-surfers and hidden cameras by shielding the key pad.
- ✓ Get cash on weekdays. Experts say that illegally installed skimming devices are at their worst on weekends. Thieves know ATMs are inspected regularly during the week.

- ✓ Use bank ATMs if possible. Avoid using the freestanding ATMs found on streets and in bars, restaurants, and convenience stores. These are riskier because they are so exposed.
- ✓ Choose gas pumps wisely. Skimmers are often found on pumps that lack security cameras, are close to a major highway, and are *not* close to the station or the attendant.

Following these tips can reduce the risk of you becoming a victim so that you can focus on what really matters…enjoying your vacation!

Is Your Home Spying on You?

The number of "smart" devices that we can connect to our homes has exploded. These devices can be anything from security cameras, thermostats, and refrigerators to electrical plugs, lightbulbs, and voice assistants. These devices add convenience to our lives, but they can also make us more vulnerable. For instance, vulnerabilities, vendor mishaps, or poorly configured devices can invite hackers into our homes. Recently, a security researcher found that a development lab used by Samsung engineers was leaking highly sensitive information for its SmartThings and Bixby services, which could allow someone to inject malicious code without the company knowing. Attacks from massive botnets (networks of devices that are infected with malicious software and controlled as a group without the owners' knowledge) have compromised numerous smart devices in recent years.

To make matters worse, those smart devices that are intended to add convenience could be used to spy on you. It is possible for hackers to compromise those devices and listen to your conversations or view video from connected cameras. Even device manufacturers could spy on you. For example, Amazon staff recently stated they reviewed recordings from Amazon's Echo products that included what seemed to be a woman singing in the shower, a child screaming, and a sexual assault. Amazon claims they review "an extremely small sample of recordings" to improve the service. This is a reminder, however, that you need to be careful of those smart devices that could be used to listen or watch you. The following tips may help reduce your risk.

- Do your research! Ensure manufacturers take cybersecurity seriously. It is best to stick with reputable brands when buying smarthome products.
- Disable Internet access for devices that do not need Internet access.
- Place your devices behind a firewall on your network.
- Change default account names / passwords. Enable two-factor authentication (if available).
- Keep devices updated with the latest software updates.
- Avoid devices that advertise Peer-to-Peer (P2P) capabilities built-in.
- Turn off devices when they are not in use or not needed for a period of time.
- Disable the microphone when that feature is not needed. If you would rather keep something private, then you may want to unplug the device.

THE CIA OF DEVICE HYGIENE

Confidentiality: keeping secrets secret

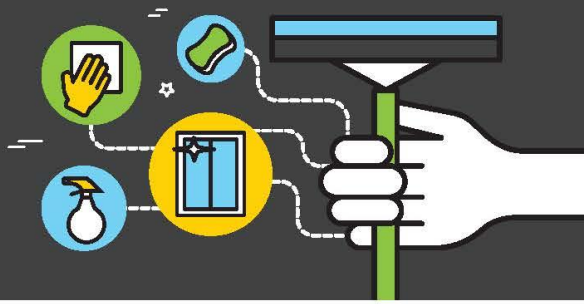
Secrets require strong passwords! Every device should be protected with a strong passcode, and lock screens should automatically initiate after a short period of non-use. That way, if it ends up in a stranger's hands, they won't easily gain access to all of your sensitive info.

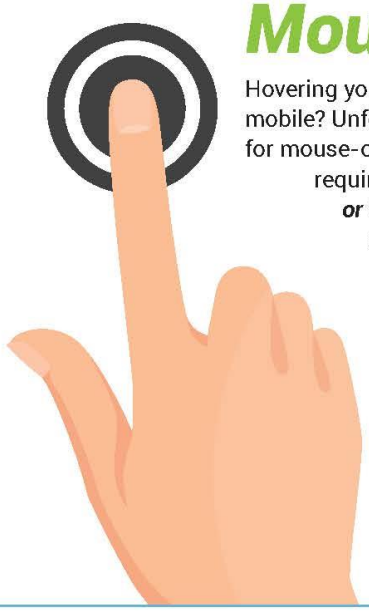
Integrity: preventing flaws

One of the easiest security incidents you can avoid is the exploitation of outdated software and firmware. Most devices and apps allow you to enable auto-update, which keeps them functional and upgraded with the latest security patches. Cybercriminals can sometimes use outdated software as a backdoor to gain unauthorized access to devices and computers.

Availability: ensuring secure access

Data is useless if it can't be accessed or located. Since devices can't last forever, we should always view them as temporary and keep them backed up. And don't underestimate the benefits of proper file management! If you can't find it, you can't secure it.





Mouse over on mobile

Hovering your pointer over a link to display the full URL helps keep systems safe. But how is it done on mobile? Unfortunately, with so many different manufacturers and app developers, no standard exists for mouse-overs on mobile. A long-press displays the URL on some devices and some apps. Others require a third-party app to achieve that same function. ***But regardless of whether your device or the app allows you to long-press a URL, it's best to avoid doing so unless you're 100% confident the URL is safe!*** A long-press could lead to an accidental click, which in turn, could lead to a security incident.

POLICY = SECURITY

Every airline enforces a policy that requires cockpits to remain locked during flight. Most businesses are required to provide evacuation routes in the event of an emergency. And our organization develops policies designed to keep data secure and systems safe. ***It's your responsibility to know and always follow our policies. If you need more info, please don't hesitate to ask!***

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided by KnowBe4 for all State employees.
***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month is on ***Securing Online Accounts with Multi-factor Authentication***.

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***A Career in Cybersecurity.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at **no cost** to government staff and contractors. With more than 60 courses, all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated regularly.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ More than **60** available self-paced courses from beginner to advanced.
- ✓ Many popular certification courses including the following:
  - Network +
  - Security +
  - Certified Information Systems Professional (CISSP)
  - Windows Operating System Security
  - Certified Ethical Hacker (CEH)
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework.
- ✓ Individuals can take courses to build their knowledge, skills, and abilities in cybersecurity.
- ✓ Taught by experienced cybersecurity subject matter experts.

For more information, visit FedVTE at https://fedvte.usalearning.gov.

PCI Webinar Series

Coalfire, a Payment Card Industry (PCI) compliance validation services vendor, will be hosting a 1-hour webinar for the State of NC's merchant community on **June 4, 2019 @ 10:00am**. Information regarding the webinar is provided below:

Webinar Title: Vulnerability Scanning with Coalfire

Webinar Description: The webinar will provide a walkthrough of scanning – what it is used for, how it compares to and compliments a penetration test, and how scanning works. It will show some typical scans scenarios and results, and what to do when remediation is needed. It will also dive into how to deal with false positives, compensating controls, and interference issues.

Speaker: Beck Larson

Speaker Bio: Beck Larson is a twice-awarded Director of the CoalfireOne Scanning Services team within the Labs practice at Coalfire – she earned Team Member of the Quarter for successfully navigating the company's annual ASV Lab in 2015 and was recognized as a Rising Star within the Labs organization at Hexacon 2018. She is responsible for all things ASV-related at Coalfire, including ensuring that Coalfire maintains its company-level ASV licensure by passing the PCI SSC's validation Lab annually, managing Coalfire's ASV staff, and ensuring satisfaction across Coalfire's vulnerability scanning client base. She has been heavily invested in helping redesign and support the new CoalfireOne Scanning Platform, launching in Q2 of 2019.

Beck joined Coalfire in August 2014, bringing nearly 10 years of experience in management and vulnerability scanning. Before joining Coalfire, she managed all internal endpoints and led internal scanning efforts of 110,000 targets for First Data Corporation (FDC), while conducting risk assessments to recommend corrective actions. Prior to that, she wrote and deployed code to Prod/DR/UAT/QA/Dev environments and collaborated with her team on their proprietary automation tool for code deployment. Prior to FDC, she brought her leadership skills and keen ability to improve internal environments to Lehman Brothers and Time Warner Cable.

Webinar Credentials:

Join from your computer or mobile: https://fuze.me/16199734
Standard Dial-In:
- Call United States (855) 346-3893 (toll free)
- Enter the meeting ID 16199734 followed by the # key

Download the Fuze app ahead of time for the best experience.
Visit https://www.fuze.com/download?utm_source=Meeting-Invite

The following are some other scheduled webinars to be presented by Coalfire in 2019.

Date	Time	Topic	Presenter
9/3/2019	10:00-11:00 AM ET	Penetration Testing – From a Hacker's Perspective	Luke McOmie
12/3/2019	10:00-11:00 AM ET	Changes to PCI going into 2020	Jon Bonham

Cybersecurity Training and Awareness Plan

To combat the increasing security threats to the State's information systems and data, the Enterprise Security and Risk Management Office (ESRMO) will be providing, through the statewide Learning Management System (LMS), a series of cybersecurity awareness courses to be distributed every other month thoughout the 2019 calendar year. All Executive Branch employees and contractors are required to complete the assigned training modules by the end of each designated month. This training will be maintained in all employees' training records. The following is this year's Cyber Awareness Training Schedule:

Release Month	Lesson Topic	Lesson Title
March	Employee's Cyber Roles and Responsibility	Your role: Internet Security and You
May	Social Engineering	Phishing Fundamentals
July	Hardening Against Attacks	How to be a Human Firewall
**** JULY – ROLE-BASED TRAINING [DBA & APPDEV] ****		
September	Information Protection	Understanding and Protecting PII
October	***** OCTOBER - CYBERSECURITY AWARENESS MONTH *****	
November	Insider Threat	Insider Threat

This year, the ESRMO will also add **role-based training** for those who are Application Developers or Database Administrators. Agencies are required to identify those individuals with significant security responsibilities who operate in those two positions. These individuals will be assigned an annual training module geared to their specific roles. The role-based training modules will be assigned by **July 1, 2019**, and must be completed within a 60-day period. The role-based training will be delivered through the training vendor portal, **KnowBe4**, from the following email address: ESRMO.Training@nc.gov. Contractors with state email accounts will receive an email with instructions on how to access their assigned training. Contractors are required to furnish the completion certificate to their supervisor for verification and retention.

- **May 27** – Memorial Day
- **May 31** – Dam Safety Awareness Day
  - https://www.fema.gov/dam-safety
- **June** – National Safety Month (NSM
- **July 1** – Formal kick-off of annual BC/DR Plan reviews by agencies; runs July 1 – October 31
- **July 4** – Independence Day
- **September 1** – Agency Compliance Reports Due
- **September 2** – Labor Day