Monthly Cybersecurity Newsletter

June 2017
Issue

Enterprise Security and Risk Management Office (ESRMO)

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

Be Sure to Pack Security for Your Trip

Summer is here and it is time for a vacation! Along with swimming suits and sun tan lotion, people often take their mobile devices with them on vacation. Devices, such as our phones, tablets, and laptops, become extensions of ourselves and come along with us wherever we go. We check email, take pictures, text family and friends, post to social media, and check the daily weather forecast with them. While the summer travel season can be a lot of fun, it can also be a great time for cybercriminals who try to exploit people who are on vacation. According to a McAfee survey, thirty-one percent (31%) of respondents connected primarily using *publicly available Wi-Fi*. Fifteen percent (15%) considered their personal information to be *more secure* while traveling than it is at home. Even those who know better, many people on vacation prioritize *convenience over security*. Before you leave on vacation, don't forget to pack the following basic security precautions.

- Set strong passwords or strong pattern locks on your devices. Also, keep them locked when they are not in use.
- Disable Wi-Fi auto-connection features, which allow your device to automatically connect to available and accessible Wi-Fi networks.
- Avoid using publicly available Wi-Fi networks, leaving you open to potential security risks.
- Before connecting to any Wi-Fi network, be sure it uses strong encryption (e.g. WPA2).
- Update your devices. Make sure your device's operating system (OS) and applications are up to date.
- Install the latest security software on your device, if available. This can help your device remain clean from potential threats.
- 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.
- Avoid posting on social media that you are on vacation and where you are on vacation. Many criminals take advantage of people vacationing by burglarizing their homes.

When Advertising Turns Ugly

Digital advertising can be a nuisance. Those ads can get in the way of normal online activities, but sometimes they can be a real pain. A recent malware campaign that affected some universities in the United Kingdom infected users with ransomware, a type of malicious software that encrypts files and holds them hostage until the end user pays a fee. The twist with this recent attack was that the users were infected simply by visiting a site compromised with the malware, which left staff without access to their files. The attack was successful because of a “malvertising” campaign, which is malicious advertising that is used to spread malicious software. In this scenario, there is no need for the user to click on anything in order to be infected. If the user’s machine is vulnerable to the attack and it is targeted with the ad, then the infection occurs *without any user interaction*. So, how can you protect yourself from malvertising? The following are some tips that may help:

- Make sure your computer’s operating system (OS), antivirus software, and web browser software are patched and up-to-date.
- Make sure web browser plugins (e.g. Java and Adobe Flash) are up-to-date.
- Change browser settings to not *automatically* play ads.
- Disable or uninstall browser plugins that are not needed.
- Enable phishing and malware protection in the browser, if available.
- Use an ad / script blocking browser plugin.
- Do online activities with user accounts that have limited access to the system. This limits the damage malware can do to your system should you become infected.

Don’t forget, there are other monthly newsletters available to you that contain a wealth of information! The following are the various cybersecurity newsletters the ESRMO distributes each month. These newsletters contain information we hope you find beneficial.

SECURITYsense Newsletter: A licensed monthly newsletter that contains several articles that are usually relevant to current cybersecurity issues.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/SECURITYsense

Disclaimer: The SECURITYsense newsletter is a licensed product of the National Security Institute, Inc. (NSI) and is protected by the United States copyright laws. Distribution via an open Internet site (available to anyone with Internet access), Extranet, or other public access network is strictly prohibited.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month’s edition is titled ***Sun, Sand, and Cybersecurity***.

https://www.cisecurity.org/resources/newsletter

SANS OUCH! Newsletter: A free monthly information security awareness newsletter provided by The SANS Institute. This month’s edition is titled ***Lessons From WannaCry***.

http://securingthehuman.sans.org/resources/newsletters/ouch/2017

Did you know that The SANS Institute also provides *free* awareness **videos** and **webcasts**? The SANS Video of the Month may be accessed at https://securingthehuman.sans.org/resources/votm.

Also, The SANS Institute offers free webcasts on a variety of topics that may be accessed at https://www.sans.org/webcasts/upcoming.

Don't forget about the following upcoming training opportunities that are available through the statewide Learning Management System (LMS). These courses are used to meet the 2017 annual cyber awareness training requirement for State employees.

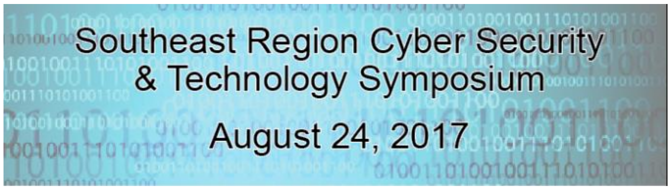
- **June** – Computer Security: Don't Let Your Computer's Defenses Down
- **August** – Mobile Security: Mobile Devices – The Future is Now
- **October** – Public Wi-Fi: Be Careful Out There
- **December** – Office Security: Keeping Your Office Secure

If you have questions about the training schedule or the training content, please contact Maria Thompson, State Chief Risk Officer, at maria.s.thompson@nc.gov or at (919) 754-6578.

The NC Office of the State Controller (OSC) is promoting a couple of more E-commerce/PCI Data Security Standards educational opportunities this year with the help of Coalfire. The following are training opportunities that coming soon:

- **August 15** at 10:00am – What is a Physical Security Assessment and Benefits?
- **October 24** at 10:00am – Implementing an Effective Employee Security Training Program

Each webinar will last approximately **1 hour**. Additional information for each of the webinars, along with a registration link, will be distributed a few weeks prior to each scheduled event.



Southeast Region Cyber Security & Technology Symposium

August 24, 2017

The Offices of United States Senator Richard Burr and United States Senator Thom Tillis, the North Carolina Defense Technology Transition Office (DEFTECH), the North Carolina Military Business Center, and the North Carolina Military Foundation will be hosting the Southeast Region Cyber Security & Technology Symposium on August 24 in Chapel Hill, North Carolina. This symposium will provide commercial and government entities information about operational cyber perspectives, threats, needs, teaming and business opportunities. More information about this event may be found at the following link: http://www.ncmbc.us/17cyber/

LDRPS to Assurance CM Migration

- Sungard completing the data mapping in Assurance CM: ~June 16 – 27
- ESRMO BCM Team validating data in Assurance CM: ~June 16 - 27
- Assurance CM F2F Training in Raleigh: June 27 & 28
- Assurance CM Go-Live: June 29

- **September 1, 2017** – Agency Compliance Reports due!
- **October, 2017** – National Cyber Security Awareness Month
- **October 27, 2017** – Triangle InfoSeCon

The Virginia Space Grant Consortium (VSGC) has made five short videos to provide background on the importance of cybersecurity in our computer and data-driven world. In the videos, practicing cyber professionals from the National Institute of Standards and Technology (NIST) and elsewhere discuss their work, their career paths, and offer tips on how to prepare for a career in cybersecurity. To view these videos, visit the following link:

https://www.youtube.com/playlist?list=PLKrkeCUPIKhuJxqo-CCSdKT35Qa568Vil.

Do you have something to share? Is there a topic you think we should cover in a future newsletter? We encourage all security professionals to send us topics that will be of value to other agencies in order to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider including it in a future newsletter, please send it to security@its.nc.gov.