Monthly Cybersecurity Newsletter

May 2018 Issue

NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

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

---

Don't Forget to Pack Security for Your Summer Vacation!

It's that time of year again when we pack our bags and go on vacation. We all need a break at times from the normal pace of life, but we should not break the habit of being safe and secure while on vacation. While the summer travel season can be a lot of fun, it can also be a time for cybercriminals to exploit people who are on vacation. The following are some things you can do to help you be safer and more secure while you are enjoying your 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. Criminals watch online posts to find people who are on vacation and have left their home unattended. 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 leary of using Wi-Fi in airports, hotels, cruise ships, coffee shops, etc. Before connecting to any Wi-Fi network, be sure it uses strong encryption (e.g. WPA2). If you do not need to use Wi-Fi while on vacation, disable it on all of 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 keep them locked when not in use. Never leave a device unattended in an airport, train station, restaurant, hotel lobby or anywhere else in public. Also, be sure to use a strong password, pattern lock, or PIN on all of 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 hassel 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 more risky because they are so exposed.
- Choose gas pumps wisely. Skimmers are frequently found on pumps that lack security cameras, are close to a major highway, and are *not* close to the station or the attendant.

Be sure to review the *5 Online Security Tips* from StaySafeOnline.org that is attached to the end of this newsletter.

Do You Tweet? Then Change Your Password!

If you have not heard yet, the social networking giant, Twitter, has asked all of its users to change their Twitter password. The reason for this was that they discovered all Twitter passwords were being stored on an internal system log in "plain text" without any encryption. This was due to a bug in the system and it meant that anyone with access to that internal log could have viewed the passwords of Twitter users and could have acccessed those accounts. Twitter has reported that there are no signs of an actual breach to any accounts, but they strongly encouraged their users to change the passwords to their accounts and update their Twitter password on all services that use their accounts.

Twitter is also encouraging users to enable a two-factor authentication service called "Login verification", to help prevent accounts from being compromised. With Login verification, a Twitter user enters a code to access his or her account which is sent to a mobile phone *in addition to* the user entering a password to log in. This feature helps make sure that only you can access your account, even if your passsword is compromised - like what happened with the Twitter bug! This latest incident involving Twitter passwords gives us an opportunity to review some basic password rules that can help keep *all* our accounts and information safer.

- ✓ Do select strong passwords that are eight (8) characters or more in length with a mixture of letters, numbers and special characters (!@#$%^, etc.).
- ✓ Do choose a *different* password for every account, service and system you use.
- ✓ Do use passphrases instead of simple passwords.
- ✓ Do enable multi-factor authentication (MFA), if it is available.
- ✓ Do change your passwords whenever there is the suspicion or likelihood that the password or system has been compromised.
- ✓ Do NOT use words that are in a dictionary or are easy to guess!
- ✓ Do NOT write down your password!
- ✓ Do NOT reveal your password to anyone else!

Remember to take a look at the following **monthly newsletters** that are available to you! The following resources are some cybersecurity newsletters from other sources that the ESRMO distributes each month. We hope you will find them beneficial.

- **SECURITYsense Newsletter:** A licensed newsletter for State employees that contains several articles involving current cybersecurity issues. **Note:** *You must have a Microsoft O365 account with access to the ESRMO external SharePoint site to access this resource*.

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 on ***Reducing your Information Footprint***.

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

- **SANS OUCH! Newsletter:** A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***What is GDPR?.***

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

---

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.

Spring 2018 Disaster Recovery Exercise

The Department of Information Technology (DIT) invites your State agency to participate in the Spring 2018 Disaster Recovery Exercise scheduled for **June 11 – 14, 2018**. This exercise is for agency mainframe customers. Please share this announcement with your mainframe application testers. The kickoff meeting date will be announced soon.

Thomas Tomczak (DIT) will be leading this exercise; please contact him with any questions you may have about the event. Thomas can be reached by phone at 919-754-6349 and via email at Thomas.Tomczak@nc.gov. We look forward to your participation!

Cyber Virtual Tabletop Exercise

FEMA's Emergency Management Institute (EMI) Virtual Tabletop Exercise (VTTX) Program will offer three cyber security breach scenarios **June 5, 6, and 7.** The VTTX occurs **12 p.m. – 4 p.m. ET**. To participate, send an email to Doug Kahn at douglas.kahn@fema.dhs.gov or call 301-447-7645. Also, send a courtesy copy email to the Integrated Emergency Management Branch at fema-emi-iemb@fema.dhs.gov or call 301-447-1381. Content is the same each day & participants attend only one session. More information is available at https://training.fema.gov/programs/emivttx.aspx.

Each month, EMI conducts a VTTX series using a Video Teleconference (VTC) platform to reach community-based training audiences around the country by providing a virtual forum for interactive disaster training. The VTTX is designed for a group of 10 or more people from state, local, tribal, and territorial emergency management communities of practice. It provides a unique opportunity for responders across the Nation to simultaneously participate in a hazard-specific, facilitated discussion. Participants will need to connect via a site equipped with the appropriate VTC capability (not Adobe Connect or FaceTime-based), but alternate ways to participate are also available upon request.

Don't forget the following resources…

- Department of Information Technology (DIT) Site: https://it.nc.gov/
- Cybersecurity and Risk Management Site: http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management
- Cybersecurity Awareness Page: https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness
- State of NC Cybersecurity Situation Report: https://it.nc.gov/cybersecurity-situation-report

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all 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 for a future newsletter, please send it to security@its.nc.gov.

On-the-Go WiFi Safety

5 ONLINE SECURITY TIPS FOR SMARTER TRAVEL

Don't let online security concerns derail your travel plans.

Whether you plan to explore the US on a road trip, hit the beach in the Caribbean, tour a castle in Europe, or hike in South America, these five WiFi safety tips will keep you secure throughout your journey.

1

Keep a clean machine.

Ensure your devices are up-to-date with the latest antivirus, firewall protection and operating system patches.

2

Stop and think before you connect to public WiFi.

WiFi is available everywhere you go, including in airports, hotels, restaurants, parks, and museums, but these networks are completely open and insecure. Use common sense when you connect to public WiFi and be cautious about the sites you visit and the information you send.

3

Paid WiFi doesn't mean safe WiFi.

Just because you paid for WiFi access, it doesn't mean it's safe. There's no encryption to stop anyone from eavesdropping on your communications, so make sure you protect yourself from hackers.

4

Beware of evil twins.

Hackers sometimes set up evil twins – WiFi networks that look real – near legitimate public WiFi networks. If you connect to them, all of your communications can be captured. It can be hard to tell the difference so confirm the name of the hotspot with the owner before you connect.

5

Use a VPN to encrypt information on all of your devices.

If you use public WiFi while you travel, the only way to guarantee your security is to use a virtual private network (VPN) like PRIVATE WiFi to encrypt your personal data in wireless hotspots. Remember, WiFi signals are just radiowaves. Anyone in range can "listen in" to what you send and receive. Antivirus or firewall software won't protect you – but a VPN encrypts all of your communications no matter where your travels take you.

STOP | THINK | CONNECT

Private WiFi®