Monthly Cybersecurity Newsletter

February 2017
Issue 2

Enterprise Security and Risk Management Office (ESRMO)

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

Pay Your Taxes – Not the Hacker!

The tax season is upon us and many people are working on getting their taxes done for the state and for Uncle Sam. It is also a time when many nefarious people take advantage of others though W-2 and tax financial scams. Criminals can get your personal information through phishing and malware schemes and then file a tax return in your name. Once they have your personal information, criminals can continue to commit identity theft well beyond the tax season. More information about tax scams, what they are, and what to do about them may be found via the following link: https://www.irs.gov/uac/tax-scams-consumer-alerts. The Internal Revenue Service (IRS) encourages taxpayers to send suspicious emails related to tax fraud to its phishing@irs.gov email account.

Also, if you suspect that you have been a victim of fraud or identity theft, the IRS encourages you to visit https://www.identitytheft.gov/. This is a site run by the Federal Trade Commission (FTC) that provides a step-by-step recovery plan and assistance in taking action. It allows you to report if someone has filed a return fraudulently in your name, if your information was exposed in a major data breach, and many other types of fraud. You can also call the IRS at 800-908-4490.

Are Your IoTs Breaking the Internet?

Last year, a botnet named Mirai managed to make much of the internet unavailable for millions of people. The botnet, which is a network of computers that are infected with malicious software and controlled as a group without the owners' knowledge, overwhelmed Dyn, a company that provides DNS services to a significant portion of the internet. Botnets like Mirai are used to disrupt individuals, businesses, government agencies, and other organizations, through "distributed denial-of-service" (DDoS) attacks. Mirai specifically disrupts the internet by compromising poorly secured Internet of Things (IoT) devices like wireless routers and security cameras and using them for large cyberattacks. These types of malicious attacks are a reminder of the importance of securing network devices. Some things to remember to make us all safer are the following:

- Disable internet access for devices that do not need internet access
- Change default account names and passwords on all network devices
- Download and install the latest firmware updates
- Disable any ports or services that are not needed on network devices

Don't forget the other monthly newsletters we provide! The following are the various cybersecurity newsletters we distribute each month. These newsletters contain a variety of information that 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 topic is about is about ***Staying Safe From Tax Season Scams.***

http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-tips-newsletters

SANS OUCH! Newsletter: A free monthly information security awareness newsletter provided by The SANS Institute. This month's topic is about ***Staying Secure on the Road***.

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

We would like to remind you of the following E-commerce/PCI Data Security Standards educational opportunities that the NC Office of the State Controller (OSC) is promoting with the help of Coalfire:

- April 11 at 10:00am – What is a Pen Test and How to Pick a Good Pen Tester?
- June 20 at 10:00am – What is P2PE Encryption?
- 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
- December 5 at 10:00am - *TBD*

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 the scheduled event.

OSC will also be hosting a 2017 E-Commerce Conference at the NCSU McKimmon Center on April 19, 2017. Additional information about this event, including topics, cost, registration process, etc., will be sent out in early March.

We want to also remind you of the new training opportunities we have through the statewide Learning Management System (LMS). The following is a list of the 2017 Cyber Awareness training modules that is provided through LMS.

- February - Incident Reporting: Recognize and Report Security Incidents
- April - Information Protection: Protecting Information
- June - Computer Security: Don't let your Computer's Defenses Down
- August - Mobile Security: Mobile Devices – The Future is Now
- October - Public WiFi: Be Careful Out There
- December - Office Security: Keeping Your Office Secure

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

Do you have somthing to share? 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 to share with others and would like for us to consider including it in a future newsletter, please send it to security@its.nc.gov.

Resources to Remember

Cybersecurity and Risk Management Site:
http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management

ESRMO SharePoint Site:
https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/default.aspx

State of NC Cybersecurity Incident Reporting Site:
https://it.nc.gov/cybersecurity-situation-report

Homeland Security Information Network (HSIN) Site:
https://hsin.dhs.gov