Monthly Cybersecurity Newsletter

November 2017
Issue

Enterprise Security and Risk Management Office (ESRMO)

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

The holiday shopping season is in full swing and people are making their lists and checking them twice, three times or more. This is a wonderful time of year, but it can be a stressful time as well as a dangerous time of year. Criminals prey upon people during the heightened shopping season seeking to steal your personal information, money, property, and peace of mind. There is usually an uptick in fraud and phishing scams this time of year. Also, roughly eighty percent of adults purchase products online. So, it is worth taking a few moments to remind ourselves of the following tips about how we can be more secure during the holiday season.

- Stay alert for phishing emails and deals that look "too good to be true"
- Shop at well-known retailers that you trust and have previously done business
- Research items you are interested in purchasing, reading vendor/product reviews
- Establish strong and unique passwords for each online shopping account
- Check out as "guest" to avoid giving personal/payment information online
- Use one credit card for all of your holiday shopping, limiting damage if your info is stolen
- Make sure your purchases are secured with encryption
- Avoid announcing on social media when you are away from home

The National Cyber Security Alliance (NCSA) has also published a *Happy Online Holiday Shopping* guide that may be accessed via the following link:

https://staysafeonline.org/wp-content/uploads/2017/11/NCSA_Holiday_Shopping_2017.pdf

In addition to the above information, the monthly newsletters for the month of November from the Center for Internet Security (CIS) and The SANS Institute provide information about safe shopping during the holiday season. ***Enjoy the holiday season and be safe!***

Did You Pull On That Card Reader?

People go to an automated teller machine (ATM) to get money, not to give information to others to steal their funds. Unfortunately, it is incredibly easy and common for thieves to steal people’s funds through “skimming” devices on ATMs and gas station card readers. Skimmers contain electronics that steal payment card data from the magnetic strip on a card. Paired with a miniature camera also attached to the ATM or gas pump that records individuals entering their Personal Identification Number (PIN), thieves have all of the necessary information to fabricate new cards and to withdraw cash from victim accounts. The best way to protect yourself from credit/debit card fraud is to inspect the card insert slot of a machine to make sure it is firmly attached. Pull on the card reader to make sure it is not fake. If the machine looks strange, find another ATM or gas station to use. Be sure to cover your hand when entering your PIN to prevent a hidden camera from recording it. Also, consider using a credit card, not a debit card, and use only machines or gas pumps that are located in well-lit, public areas, and avoid secluded spots. Finally, do not neglect your own physical security when getting cash from an ATM or pumping fuel at a gas station. You are more likely to get mugged withdrawing cash or pumping fuel than you are to find a skimmer attached to it. For more information about card skimmers, read the article “Why I Always Tug on the ATM” at https://krebsonsecurity.com/2017/03/why-i-always-tug-on-the-atm/.

IT Oversight Committee Meeting Update

Maria Thompson, State Chief Risk Officer, recently presented to the Joint Legislative Oversight Committee on Information Technology about the State’s cybersecurity efforts. Ms. Thompson stated that the Department of Information Technology (DIT) has developed a continuous monitoring plan that runs on a recurring three-year cycle that requires executive branch agencies to conduct an annual assessment. The assessment can be done by a third party or in-house through a self-assessment; however, each agency is required to use a third-party assessment at least once during the three-year cycle. Agencies are to report their assessment findings to DIT, which DIT will then report to the IT oversight and fiscal division. These reports allow the State to identify problem areas, the agencies that are at a higher risk, and those who are unable to meet compliance requirements.

Agencies may utilize a state contract for their security assessments, State Term Contract (STC) 918A, which allows them to fast-track requests for proposals to get security services and assessments done. This year, DIT added more services to STC 918A that allows the agencies to fast-track other services such as incident response retainers, support and cybersecurity training. DIT will be looking at what agencies do not have the necessary funds to update security measures and those that are trending under the 80 percent compliance mark. Ms. Thompson also promoted to the IT Oversight Committee on the need for a “Cyber Range” as a proofing ground for “our new and upcoming cyber warriors and as well as our current IT personnel so that they can hone their skills.” DIT has also been working to combat phishing attempts and alerting on any risky logins that take place, such as those from outside of the State, shutting them down before any data is compromised or more phishing happens.

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 involving 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 on ***Shopping Safely Online***.

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 on ***Shopping Online Securely.***

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

The final security module through the statewide **Learning Management System (LMS)** will be released in **December**. The title of the last module will be *Office Security: Keeping Your Office Secure*. This course is designed to meet the 2017 annual cyber awareness training requirement for all State employees.

Note: *Agencies need a minimum 90% completion to be compliant.*

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

PCI and Security – What to Expect for 2018 (December 5)

Like everything, PCI DSS and security technologies are constantly evolving. Coalfire, a PCI compliance validation services vendor, will be hosting a 1-hour webinar for the State of NC's merchant community on **December 5, 2017 at 10:00am**. The webinar will cover the expected changes to the PCI DSS and likely guidance to come from the PCI Council and what major trends are expected in payment issues. This session will also peek at what security issues are on the horizon for 2018, as well as how the white hats are likely to respond. Finally, the webinar will end with some thoughts about how you can position your organization to be more secure going forward whatever bad things are likely to happen. To register for the webinar, go to the following link:

https://attendee.gotowebinar.com/register/6069395831544633858.

National Cyber Security Awareness Month

NCSAM Resources

National Cybersecurity Awareness Month (NCSAM) may be over, but promoting cybersecurity awareness is not! The ESRMO wants to remind you of some resources and to encourage you to share them with your staff. The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides a Cyber Security Toolkit, a resource that features educational material designed to raise cybersecurity awareness. The Toolkit was developed and distributed by the MS-ISAC to all fifty states, and it can be widely shared across government, businesses, schools and citizens. The toolkit may be found online at https://www.cisecurity.org/ms-isac/ms-isac-toolkit/.

Additional cybersecurity resources are available at the following sites:

- **DHS Stop.Think.Connect:** https://www.dhs.gov/stopthinkconnect
- **StaySafeOnline:** https://staysafeonline.org/ncsam/
- **NC Cybersecurity Awareness Site:** https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

Upcoming Events…

- **November 30, 2017** – Agency BC/DR Plans due to the State CIO via the ESRMO
- **December 5, 2017** – *PCI and Security – What to Expect for 2018 Webinar*
- **December 25, 26, & 27, 2017** – Christmas Holiday
- **January 1, 2018** – New Year's Day Holiday
- **January 15, 2018** – Martin Luther King Jr. Birthday
- **January, 2018** – *NIST Risk Management Framework* training @ 3900 Wake Forest Rd., Raleigh NC. Date in January to be determined!!!
- **January 28, 2018** – Data Privacy Day

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.