Monthly Cybersecurity Newsletter

May 2017 Issue

Enterprise Security and Risk Management Office (ESRMO)

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

---

Are You Trading Security for Productivity?

A new end-user survey by Dell finds that nearly three in four (72 percent) of employees are willing to share sensitive company information online under certain circumstances. The most common circumstances include being directed to do so by management, determining that the risk to their company is very low and the potential benefit high, and feeling it will help them do their job more effectively. Those surveyed said they felt that company security policies got in the way of them doing their jobs. Employees are effectively determining for themselves whether it is acceptable to share sensitive company information regardless of what the company policies may say. That is one of the reasons why it is common for cyber criminals to pose as a trusted partner, employee or organization to convince employees to share sensitive data. The survey reveals that more than one in three employees (36 percent) will frequently open emails from unknown senders at work, potentially opening the door for spear phishing attacks that can lead to sensitive information disclosure. 35 percent of those surveyed said that it was common to take proprietary information with them when leaving an organization.

Clearly, employees are taking too many risks with their employer's data! The survey suggests that companies must focus on educating employees and enforcing policies and procedures that secure data wherever they go, *without* hindering productivity. The image to the right shows some of the responses from the survey. The complete survey may be found at the following link:

http://dellsecurity.dell.com/dell-end-user-security-survey

Image above is from Dellsecurity.dell.com.

Taking a Bite Out of Apple

Who says Apple products are not immune to malicious software? While they may be comparably fewer instances of malware on Apple products, it does happen. Take for instance a recent incident where a Mac developer had its software compromised. Creators of the open source video transcoder application called HandBrake issued a statement about a recent threat. They warned that anyone who downloaded their software onto a Mac OSX machine between May 2, 2017 and May 6, 2017 could be at risk. Apparently, the developer's download file was replaced with a variant of Proton RAT, a Trojan that is capable of keylogging, screen capture, and webcam operation. Anyone who has installed HandBrake for Mac during the time period mentioned above has a 50% chance of being infected and needs to check their system for the malware. Apple has since pushed out an update preventing any new infections. Additionally, users affected by this malware should change all passwords in their OSX KeyChain or passwords stored in their browsers. For more information about this threat, visit https://forum.handbrake.fr/.

Remember, 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 newsletter is titiled ***Are You Really Being Secure Online?***.

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

SANS OUCH! Newsletter: A free monthly information security awareness newsletter provided by The SANS Institute. This month's topic is on ***Securing Today's Online Kids***.

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.

For many people, Microsoft O365 can be challenging to use. There are also many features that may go unnoticed to the average user. Therefore, this month the ESRMO would like to highlight the following resource. The Unified Communications team at the Department of Information Technology (DIT) has put together an online resource to help end users with Microsoft O365 topics and issues. From this resource, you can click on "O365 Wiki" and browse through a list of articles on O365, or you can search for specific topics such as DLP, Encryption, IRM, etc. Users may access the resource from the following link: https://ncconnect.sharepoint.com/0365.

Mark Your Calendar

›› UPCOMING EVENTS

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 the following E-commerce/PCI Data Security Standards educational opportunities with the help of Coalfire:

- **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

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.

Did you know that Governor Roy Cooper proclaimed **May 7 – 13** as Hurricane Preparedness Week in North Carolina? North Carolina is one of the leading states for overall damage from hurricanes. The Governor's proclamation has excellent recommendations for preparing for hurricane season and may be viewed at https://governor.nc.gov/gov-cooper-declares-may-7-13-2017-hurricane-preparedness-week. Two other great resources that provide extensive details on hurricane planning and preparedness are www.ReadyNC.org and https://www.ready.gov/hurricane-toolkit. We encourage everyone to view these resources and to be better prepared.

On the heels of Hurricane Preparedness Week is Business Continuity Awareness Week (BCAW)! This year's theme is **Cyber Resiliency**! Held **May 15 – 19**, BCAW is dedicated to promoting awareness of business continuity within your organization. Each day of the week, the ESRMO will send email on Cyber Resiliency that you can forward to others. You can also use this week to conduct cyber exercises! More information about BCAW may be found at the following link:

http://www.thebci.org/index.php/bcaw-home

Remember… *Cyber Security is Everyone's Responsibility!*

LDRPS to Assurance CM Migration

- LDRPS Data Clean-up ends: NLT June 14
- Assurance CM Testing ends: NLT June 14
- LDRPS Date Freeze: June 14, End of day
- Final data migration LDRPS > Assurance CM: June 15
- 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

DIT Spring 2017 Disaster Recovery Exercise for Mainframe Customers

- Disaster declaration: June 16
- Disaster Recovery Exercise start: June 19, 8:00am
- Disaster Recovery Exercise end: June 22, 11:59pm

More to come…

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

---

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.