Monthly Cybersecurity Newsletter

April 2020 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

Telework: How to Be Safe While Working from Home

In response to the COVID-19 coronavirus, the state of North Carolina has taken the unprecedented approach of encouraging all employees who can to telework to create social distancing. The following tips will help you succeed at that task in just five easy steps. To ensure security controls are in place and in accordance with policy, always use work-provided computers when working from home. If you must use a personal device, keep network security in mind.

1. **Patch your desktop and/or laptop for both the operating system and applications.**
   - Windows 10: https://bit.ly/3dF2MpD
   - MacOS: https://apple.co/3bQHHXB
   - If you don't have Windows 10 or a Mac, search online for details on how to update your operating system

2. **Use strong passwords for all your user accounts.**
   - Where possible, use multi-factor authentication (e.g., receiving an authentication code from an email or text message)
   - Don't let the name fool you, "HaveIBeenPwned" is a very useful website for checking to see if your personal email addresses have been exposed in a data breach. You can also test your passwords to see if they are strong and part of a previously exposed or known password dictionary

3. **Use a modern browser that is up to date. Check your applications' requirements to determine which browsers work best.**
   - Chrome – How to update: https://shorturl.at/aeBKT
   - Firefox – How to update: https://mzl.la/2WX1LTS
   - Microsoft Edge – Updated through Windows 10 updates
   - Safari – Updates included with MacOS updates

4. **Have up-to-date antivirus software installed.**
   - Check with your internet provider to see if it provides security software with your subscription
   - Use the following to see a list of AV solutions:

- Windows: https://bit.ly/3bCPfNk
- Mac (yes, you're not impervious to viruses and malware!): https://bit.ly/2UxhTtw

5. **Consider configuring a DNS security filter on your personal device or your entire home network.**
   - This requires some hands-on changes to your desktop/laptop or router but should be easy enough for most people to accomplish
   - Doing this will offer additional protection against malware and ransomware beyond just working at home

Happy Easter! Protect Yourself from Online Scams

Did you know that nine out of 10 attacks start with an email? Many emails and Easter-themed e-cards from unknown senders contain malicious links. So, remember to stay safe when you open those e-gift cards. Here are three examples of online scams that occur specifically during the Easter period, often exploiting users' holiday cheer and generosity:

- Emails and Easter themed e-cards from unknown senders that may contain malicious links
- Fake advertisements or shipping email notifications with attachments infected with malware
- Spoofed email messages and phony posts on social networking sites requesting support for fraudulent Easter related causes

Coronavirus and Cybersecurity Crime

Hackers and other cybercriminals are taking full advantage of our fears surrounding the COVID-19 coronavirus pandemic.

Security Boulevard has five tips to help you improve your computer security during these times of uncertainty.

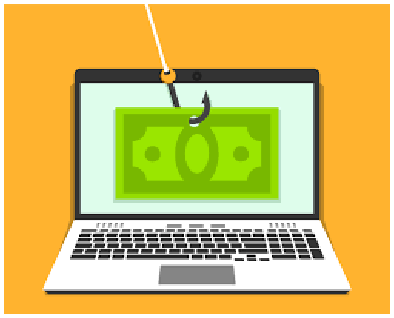
1) Don't use the same password for multiple sites and apps.
2) Consider using multi-factor authentication for as many accounts as you can.
3) Don't forget fraud can happen on the phone, too.

4) For businesses wanting to protect customer data, consider Payment Card Industry (PCI) compliance, the strongest standard for payment security.
5) Phishing scams relating to COVID-19 are common. This may include emails pretending to offer advice from government agencies.

Read the full article here.

Click here for NC DIT tips on how to stay secure while teleworking.

Phishing: Top 10 Types of Phishing Emails



Phishing is a major threat to anyone who uses email as cybercriminals seek to take advantage of our busy lives and now, in times of crisis, such as the one we face now with the COVID-19 pandemic.

Security Metrics identifies 10 types of phishing emails we all need to remember:

1. **The government agency:** An email purporting to be from a federal agency, such as the FBI, trying to scare you into giving out your personal information.
2. **A friend in need:** An email from someone you don't know who needs your help by sending them money.
3. **The online billing trick:** An email letting you know that the credit card you used for online purchases has expired.
4. **An expired account:** An email letting you know that your account is expiring, and you'll lose your data if you don't sign it.
5. **The computer scare:** An email prompting you download an attachment to remedy an infected computer or breached account.
6. **The prize winner:** An email claiming you've won a prize or are the beneficiary of an unknown relative's estate.
7. **Banking scam:** An email posing as a notification that money has been withdrawn from your bank account.
8. **The upset customer:** An email in which an "angry customer" threatens to contact authorities if you don't reimburse them.
9. **Income tax refund:** An email letting you know that you're eligible for a tax refund or have been selected to be audited.
10. **The computer update:** An email that a company is conducting a routine security procedure and needs you to verify or provide account information.

Get more information and see examples in the full article.

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4.
***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2020

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month's edition is titled ***Social Media: The Pros, Cons and the Security Policy***.

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition includes ***Digital Spring Cleaning AND Securing Today's Online Kids.***

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

April 16: Webinar – Using Detection Technologies to Defend Against Active Directory and Ransomware Attacks

April 23: Webinar – How to Better Understand HR to Accomplish our Cybersecurity Goals

April 30: Webinar – The New Normal: How Employees Stay Secure and Productive While Working-from-Home

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. You are also encouraged to review Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember…Stop. Think. Connect.*