Monthly Cybersecurity Newsletter

May 2020 Issue

Enterprise Security and Risk Management Office (ESRMO)

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

---

Telework: Protect Your Mental Health When Working from Home

We've all been affected by the emergence of the COVID-19 coronavirus – especially in the ways we carry out our work responsibilities. According to Dr. Jill Newby, associate professor of psychology at the University of New South Wales, working remotely can leave employees feeling isolated and disconnected from others. Among other common feelings are being unable to stay motivated or "switch off" from work.

In an article on Black Dog Institute website, Newby offers five tips and ways to help you not only stay productive while working from home but to take care of yourself mentally and emotionally:

- Set up a routine for each workday.
- Create a separate workplace within your home.
- Keep in touch with your managers and co-workers.
- Keep away from digital gadgets in the evenings.
- Keep a positive attitude and focus on the benefits of working from home.

The state of North Carolina encourages all its employees and partners to take special care in protecting their mental health during these challenging times. Employees can take advantage of the Employee Assistance Program, which offers free support and resources for addressing personal or work-related challenges and concerns.

Click here to read the full article and to see other helpful links on how to keep yourself psychologically healthy while working from home.

Click here for tips on how to stay secure while working from home.

Coronavirus and Cybersecurity Crime

- **Don't respond to texts, emails or calls about checks from the government or online offers for vaccinations**. There are no products proven to treat or prevent COVID-19 at this time.
- **Be wary of ads for test kits.** The U.S. Food and Drug Administration recently announced approval for one home test kit, which requires a doctor's order. But most test kits being advertised **have not been approved** by the FDA and aren't necessarily accurate.
- **Hang up on robocalls.** Scammers are using illegal robocalls to pitch everything from low-priced health insurance to work-at-home schemes.
- **Watch for emails claiming to be from the U.S. Centers for Disease Control and Prevention (CDC) or World Health Organization (WHO).** Use only trusted sites, like covid19.nc.gov and coronavirus.gov to get the latest and most reliable information. And don't click on links from sources you don't know.
- **Do your homework when it comes to donations**. Never donate in cash, by gift card or by wiring money.

Staying Cybersafe During Memorial Day

As Memorial Day approaches, the U.S. Cybersecurity and Infrastructure Security Agency reminds everyone to stay cyber safe. Be cautious of potential scams, such as unsolicited emails that contain malicious links or attachments with malware. Also be aware of the risks associated with online shopping and traveling with mobile devices.

CISA recommends users review the following tips for information on how to guard against these risks:

- Using Caution with Email Attachments
- Avoiding Social Engineering and Phishing Attacks
- Cybersecurity for Electronic Devices
- Shopping Safely Online
- Holiday Traveling with Personal Internet-Enabled Devices

10 Common Traits of Phishing Emails

Phishing is one of the most common attack methods used by cybercriminals and the one we're all probably most familiar with. Fortunately, there are signs that can help you identify whether or not that email in your inbox is a scam.

Asking for Personal Information	Most reputable organizations will never email you asking for your address, phone number, national ID number, or other personal data.
Inconsistencies in Links	Always hover over links with your mouse pointer to display the full URL. If it leads somewhere that doesn't logically belong within the context of the email, or generally looks nonsensical, don't click!
Unrealistic Threats	Phishing emails often feature threatening language, such as "Payment overdue!" or "Your account has been compromised!", in order to generate a response from their targets.
Generic Greetings	Unlike legitimate entities that will address you by your full name or username, phishing emails usually opt for generic greetings, such as Dear Customer or Dear Sir/Madam.
A Sense of Urgency	Similar to unrealistic threats, emails that urge you to click on a link or download an attachment or update your account immediately are likely scams.
You're Asked to Send Money	Whether it be overdue taxes or an upfront payment to cover expenses, any email that asks for money should immediately raise your suspicions.
Too Good to Be True	The old saying remains true to this day: if it's too good to be true, it's likely untrue. Keep that in mind any time you get an email claiming you won the lottery or are due a large family inheritance.
Poor Spelling & Grammar	Most generic phishing attempts contain spelling and grammar errors or feature awkward wording/phrasing.
Suspicious Attachments	Attachments aren't always malicious, but use extreme caution whenever you receive them unexpectedly.
From a Government Agency	In almost every case, government agencies don't use email to communicate anything of consequence. The IRS, for example, will never email you about your taxes or payments.

CYBERSECURITY NEWSLETTERS

SAC 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

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS).

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

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute.

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

May 14: Webinar – Making Work at Home Operations Safe and Productive

May 18: Webinar – Infosec Rock Star 2020: How to Accelerate Your Career

May 18-22 – Business Continuity Awareness Week (BCAW) is an annual global campaign facilitated by the BCI to raise awareness of the resilience profession and demonstrate the value effective business continuity management can have to organizations of all types of sizes. This year's theme is "***We are Stronger Together"*** and focuses on the idea of collaboration across teams, departments and disciplines to build and implement resilience within organizations and society in general. Look for a special message each day focusing on working together and collaboration.

May 26: Webinar – How to Leverage CTI to Defend From Ransomware

---

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.*