Monthly Cybersecurity Newsletter

November 2019 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

Holiday Shopping: Debit Card Dangers

"The season is upon us now, a time for gifts and giving…" - John Denver

The holiday shopping season is here once again. Debit or Credit… that is the question. Though some of us would rather use cash or debit cards than take the risk of being undisciplined with credit cards, there are some dangers or drawbacks associated with using debit cards.

Fraud Protection: With a debit card you could be responsible for up to $500 worth of charges you didn't make; whereas, with a credit card you typically will only be liable for around $50.

Building Credit: If you don't have a credit history yet or you're trying to rebuild your credit, a debit card won't help. Debit cards are the same as cash and are not considered credit.

Merchant Disputes: In a dispute regarding a purchase you made using a debit card, you'll be in a weaker position because the merchant will already have your money and it may take weeks to get it back; whereas, with a credit card you'll have time to dispute a charge before any money is actually paid out.

Bank Fees: If you use a debit card, you'll need to be extremely diligent. If you overcharge, even by a few dollars, the card may not be declined right away. The bank may allow your charges to go through, and then charge you with numerous overdraft fees up to $34 a piece.

Rewards and Services: Most debit cards usually don't have the perks credit cards have, such as cash back or other rewards programs. For most of us the rewards we earn each year on our credit cards could be up to $100. These rewards will be lost if you use your debit card.

Even knowing the dangers and drawbacks of using debit cards, some of us will still decide to avoid using credit cards altogether and that's ok. But if you do choose to use your debit card please follow these rules to make using your debit card as safe as possible:

- Treat your debit card like cash and keep it secure
- If your debit card is lost or stolen, report it immediately
- Never write down your debit card PIN or share it with anyone
- Avoid bank fees; keep a cushion in your checking account to cover accidental overdrafts

Louisiana Government Computers Knocked Out After Ransomware Attack

On Monday, November 19, a ransomware attack on Louisiana state government significantly impacted its computer systems, Governor John Bel Edwards revealed in a series of tweets. The state became a victim of the attacks as it awaits certification of the results from its close gubernatorial election. Many state agencies had their servers taken down in response to the attack. The governor said the agencies were coming back online but that it might take days before full restoration is complete. The state has no evidence of data loss and did not pay the ransom asked by the attackers. The ransomware that hit the state is potentially Ryuk, a variant that cybersecurity firms first identified in August of last year. *Source: Reuters*

Office Security Tip of the Month

Did you know you can lock your computer screen simply by pressing the L key while holding down the Windows key? Too easy! Right? So, every time you step away from your computer (even briefly) be sure to lock it down. We bear an enormous responsibility to keep our computer networks secure and the personal data of the citizens of North Carolina safe.

It's Not Necessarily Bad if Your Kid Spends Lots of Time Online. But Watch for These Warning Signs by Dr. Harold S. Koplewicz

Emerging research shows that it isn't just how much time kids spend online, but *how* and *why* they spend time online that impacts their social, emotional and behavioral health. As we try to better understand and help with the mental health challenges associated with internet use, researchers and clinicians are turning more to lessons from the substance abuse field for guidance.

Kids themselves seem to understand the risks of "using" the Internet. In a 2016 survey, half of teenagers said they "feel" addicted to their mobile device, and 72% said they felt the need to immediately respond to texts and social networking messages.

Just because kids are aware of their attachment to devices and the Internet doesn't mean they are impaired by this use — but a subset are. This impairment is captured by the concept of problematic internet use (PIU), which affects up to 10% of children and adolescents. PIU is assessed with a scale developed for substance abuse and focuses on the intensity and dysfunction of internet use rather than trying to define when use is "excessive" or "too much." Sample questions from the assessment include the following:

- How often do you find that you stay online longer than you intended?
- How often do you form new relationships with fellow users?
- How often do others complain to you about how much time you spend online?
- How often do you lose sleep due to being online?
- How often do you choose to spend more time online over going out with others?

At the Child Mind Institute, they asked these questions to more than 500 young people ages 7 to 15 who participated in a Healthy Brain Network study and found links between PIU and depressive disorders and attention-deficit hyperactivity disorder (ADHD). These preliminary results are summarized in the Child Mind Institute's 2019 Children's Mental Health Report on social media, gaming and mental health.

They also found that PIU is linked to impairment in everyday functioning at home, at school and with friends — even when accounting for the impairment of a co-occurring mental health disorder. Similar to drug use, PIU can make symptoms worse for kids who are already vulnerable or struggling with a mental health disorder. If a teen has PIU and ADHD, for instance, PIU adds an extra level of impairment above and beyond his ADHD symptoms.

When should you worry? Online habits are problematic when they become compulsive, are motivated by the desire for mood alteration or are related to offline interpersonal problems. Examples of this would be a teen disappearing into a game to forget about a breakup or using social media to avoid feelings of depression.

By the same token, there are online habits that may be benign or even beneficial despite the seemingly "excessive" amount of time young people devote to them. Many things kids do on their devices are age-appropriate activities that have simply been done offline in the past: socializing with peers, pursuing hobbies, shopping, listening to music, doing schoolwork and watching TV.

The therapeutic power of the Internet is just being unlocked. One example is from an online survey from Stony Brook University, which shows that a single "dose" of self-administered intervention can significantly reduce youth mental health problems, especially depression.

Parents can encourage the kind of online experiences that can be beneficial beyond the measure of their hours by being an engaged "digital neighbor" to kids. You can look out for signs of depression, model your own balanced use of connected devices and practice something called parental "mediation" of your kids' internet use — that is, co-viewing or co-playing and being online together. It's also a good idea to establish phone-free time before sleep for all family members. And finally, you can help your kids practice "mindful" use of social media by pausing to reflect on how being online makes them feel in the moment, whether it's bad or good.

The real challenge is not to let caution blind us to the incredible potential of the online world to help our kids learn, grow and even help themselves. *Source: Time*

LA “Juice Jacking” Scams

Los Angeles officials are warning travelers not to use public USB charging points for the fear of malware infection. LA County district attorney, Jackie Lacey, posted an official fraud alert warning of USB charging scams, also known as “juice jacking.” The alert read, “In the USB charger scam, often called ‘juice jacking,’ criminals load malware onto charging stations or cables they leave plugged in at the stations so they may infect the phones and other electronic devices of unsuspecting users. The malware may lock the device or export data and passwords directly to the scammer.” The officials are urging all travelers to use AC power outlets or car chargers to charge their devices. *Source: Infosecurity Magazine*

CYBERSECURITY NEWSLETTERS

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

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month the newsletter covers ***8 Shopping Tips for the Holiday Season***.

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

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month’s edition is titled ***Shopping Online Securely.***

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

December 11 – 7 Myths of Security Automation: Be Clear on What It Can Achieve

December 13 – 10 Visibility Gaps Every CISO Must Fill

December 17 – WhatsApp End to End Encryption Demystified

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