Monthly Cybersecurity Newsletter

July 2020 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

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

As We Enjoy Summer, Beware of ATM Theft

People go to ATMs because they want to withdraw money from their financial accounts, not to give information to someone else so they can steal their money.

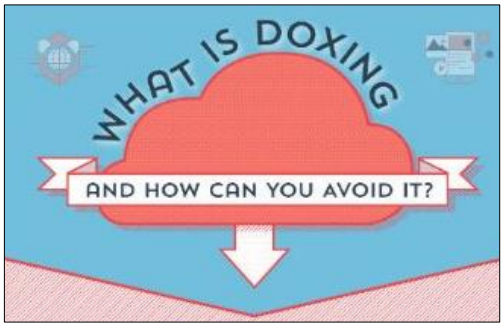
Unfortunately, it has become incredibly easy and common for thieves to steal other people's money by attaching skimming devices to ATMs.

ATM card skimmers contain electronics that store payment card data from the magnetic strip on the card. Paired with a miniature camera, also attached to the ATM, that records individuals entering their PIN, thieves have the necessary information to fabricate new cards and withdraw cash from victim accounts.

The best way to protect yourself from ATM fraud is to inspect the card insert slot of a machine to make sure it is firmly attached. If the machine looks strange, find another one. Also, be sure to cover your hand as you enter your PIN.

For more information about this topic, read Krebson Security's article, "Why I Always Tug on the ATM," or learn more about skimmers and how they work.

Doxing: What It Is and How to Protect Yourself



Doxing is the act of searching for people's personal information over the internet. The term comes from "document tracing," which involves collecting documents belonging to a person or company to learn more about them.

Often used as a revenge tactic, *doxing* involves the malicious targeting, compiling and public release of personally identifiable information (PII) to perpetrate harassment, revenge, identity theft or potential violence against a target.

Recent events have resulted in an increase of doxing targeting the public, law enforcement officers, their families and public officials.

Once a target is identified, hackers scour the internet for information such as home address, Social Security number, date of birth, private phone number and email addresses or photos. They use public records such as property records and tax documents and search social media and real estate websites. The hackers then publish the information online.

The N.C. Department of Information Technology strongly recommends that anyone who believes they might be a potential victim of doxing take proactive steps to limit their online presence and have PII removed whenever possible.

Checking social media is one of the best ways to take precautions:

- Check privacy settings on accounts and implement the strongest security controls possible.
- Deactivate or delete any social media or online dating profiles you no longer use.
- Review friends and followers. Unfollow and reject requests from anyone you do not know.
- Assume everyone can see information about your activities, personal or professional life that you post and share.
- Never post anything you would be embarrassed for everyone to see.
- Check your posts for PII (e.g., date of birth, telephone numbers, addresses) or images that identify your location, job, hobbies, family or friends. Remove those details or delete the post.
- Search social media for tagged photos of you and your family and remove the tags.

For more on doxing and other ways to help protect yourself from it, visit https://it.nc.gov/doxing.

Stay Safe While Working from Home

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

Looking for More Training?

The U.S. Department of Homeland Security provides Federal Virtual Training Environment (FedVTE) courses at no cost to government personnel, including contractors, and U.S. veterans.

Courses include a variety of cybersecurity-related topics as well as certification preparation courses ranging from beginning to advanced levels.

New courses are added or updated on a rolling basis.

If you are interested in this education opportunity, more information about the FedVTE offering can be found in the FedVTE course catalog.

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

July 20: Webinar – Learn to Think Like a Hacker to Stop Attacks Faster: Strengthen Your Security Posture with the MITRE ATT&CK Framework

July 23: Webinar – A New World of Endpoint Security: Unifying user and endpoint protection

July 24: Webinar – SANS Malware & Ransomware Solutions Forum

July 30: Webinar – Women in Cybersecurity Forum, presented by SANS Summits

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember… Stop. Think. Connect.*

***Disclaimer**: Vendors, references, and links in this newsletter are for informational purposes only and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*