SUMMER CYBER THREATS IN THE NEWS

Is your computer updated? Is your anti-malware up to date? Are you verifying the links you click-on are legitimate, expected and from a known source?

Two more of our sister states were impacted by Ransomware in July. One affected education the other law enforcement.

Louisiana Governor John Bel Edwards declared a state of emergency following a series of ransomware attacks. Hackers have deployed an unidentified malware program at the Morehouse, Ouachita, and Sabine Parish school districts that made school computer and telephone systems inaccessible. Following Governor Edwards' declaration, the Louisiana National Guard dispatched a team of cybersecurity experts.

Two Georgia agencies were hit by ransomware attacks in July: the Administrative Office of the Georgia Courts and its Department of Public Safety. The Georgia State Patrol, Georgia Capitol Police and the Motor Carrier Compliance Division are all under the Public Safety department. Officials decided to shut down the department's computer servers and systems as the Georgia Technology Authority investigates these attacks.

Attacks come at heavy costs even when the ransom is not paid. Atlanta paid $17 million to recover from a 2018 attack and Baltimore has spent about $18 million recovering from an attack this year.

It is critically important that all of us who are entrusted with our citizens' information be aware of the frightening uptick in ransomware. We need to be vigilant at all times. This means continuously updating systems and anti-malware solutions. Information Security Officers (ISOs) should work with their organizations to reinforce the dangers of clicking on sites and attachments without verifying sources and security.

One way to increase your knowledge and personal cyber safety is to attend the Secure Delaware Conference. Information is in the next column and on the event site. I encourage you to join us.

— Solomon Adote, *Chief Security Officer*

REGISTER NOW! SECURE DELAWARE 2019 CONFERENCE

This much anticipated cyber security conference will be held September 24th at the Chase Center on the Riverfront in Wilmington. It is one of the top ***FREE*** Information Security conferences in the region, drawing cyber security thought leaders, technology vendors and services companies to Delaware.

Learn More & Register Today

CAPITAL ONE ANNOUNCES MASSIVE DATA BREACH

The *New York Times* reported that a software engineer in Seattle hacked into a server holding customer information for Capital One, obtaining personal data from over 100 million people, federal prosecutors said on July 29. In one of the largest thefts of data from a bank, tens of millions of credit card applications were stolen. Information was stolen from credit card applications that consumers and small businesses had submitted as early as 2005 and as recently as 2019. Capital One said the bank account numbers were linked to customers with "secured" credit cards. Secured cards require customers to put forth a sum of money — $200 or $250 in exchange for a card.

If you are affected by this breach, Capital One said that everyone affected will receive notification and two years of free credit report monitoring. State data breach laws vary by state. Meanwhile, customers can choose to freeze their credit, which you must do at all three credit bureaus: Equifax, Experian and TransUnion. The freeze prevents lenders from pulling your credit report, which would stop criminals from opening a new account. The process is free, and won't impact your credit score. If you do need to open a new account or complete other activity involving your credit report, you'll need to unfreeze it first.

Keep track of credit card statements in case any fraudulent charges pop up. Also, change your passwords on those accounts. If you've used similar passwords on other accounts, you should change those, too.

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov