https://www.courant.com/opinion/op-ed/hc-op-chaudhary-cyber-attack-0731-20200731-ucbgostn3zecdcsvb7qvmmhuki-story.html

Hartford Courant.
courant.com

State must increase cyber defenses

By ARVIN CHAUDHARY
SPECIAL TO HARTFORD COURANT |
JUL 31, 2020

Hackers broke into the Twitter accounts of world leaders, celebrities and tech moguls in one of the most high-profile security breaches in recent years on Wednesday, July 15, 2020, highlighting a major flaw with the service millions of people have come to rely on as an essential communications tool. (AP Photo/Richard Drew, File) (Richard Drew/AP)

Cyberhackers are in the news again, demonstrating ever-greater sophistication. Both state and private sector employees working from home make the potential for hacking even more serious — and more likely.

The state of Connecticut needs to take action before data and dollars are stolen.

In one recently publicized case, hackers used social engineering, often dubbed "phishing," with Twitter employees to take control of numerous high-profile accounts, including those of Joe Biden, Bill Gates, Elon Musk, Barack Obama, and Apple, Inc. — to perpetuate crypto-currency fraud.

If they could hack into the accounts of such high-profile individuals, it should be fairly easy for these criminals to sneak into computers of state employees staying sequestered from COVID-19.

In a second noteworthy attack, Western intelligence agency officials blamed a prominent hacking group supported by the Russian government for cyber-espionage against organizations involved in the development of coronavirus vaccines and other health-care related work. Yes, they were trying to steal COVID-19 research.

According to one study, 91% of all cyber-attacks begin with phishing emails of unsuspecting victims with about a third of all successful breaches involving the use of ever-more-sophisticated techniques.

Consider all the personal information contained in computers at the state Department of Motor Vehicles, municipal tax departments and the Secretary of the State.

How easy would it be for hackers to erase names off voting lists as a way to cut support for a political enemy? Is it just a matter of time before hackers steal from local or state pension funds?

America is vulnerable. Connecticut is vulnerable. Extremely so.

It is time for the state to create a state-wide cybersecurity task force to determine government vulnerabilities — on the state and local level. Only after such an assessment can we begin to find ways to protect ourselves. You can't prescribe medicine until you know the nature of the disease.

Connecticut should see the nationally publicized hacks as the proverbial canary in the coal mine. Cyber-threats are a significant risk to government and business, especially due to the pandemic, with work-from-home employees creating new and significant security gaps that typically have not been addressed. Hackers will continue to go after these employees even as we start going back to a new normal, however that may come to be defined.

There are steps that Connecticut businesses, hospitals, government entities, and employees can take to begin to protect themselves from cyber-attacks.

A comprehensive "Compliance Assessment and Cyber Risk Assessment" is in order, particularly using a robust cybersecurity framework such as the one provided by the National Institute of Standards and Technology. It will help identify the risks and security gaps and offer a prioritized roadmap for potential cybersecurity investment.

The state must protect against domain spoofing, where a hacker uses the company's own Internet domain name to impersonate the company or one of its employees. Employees, executives and even board members need to be made aware of these techniques and reminded frequently to help minimize these attacks.

Hackers use domain spoofing to divert customers and employees to fake websites to capture user credentials. Protecting against domain spoofing is quick and easy to implement, and relatively inexpensive.

Everyone can take simple steps themselves, such as using password managers, two-factor authentication, strong passwords on home routers and virtual private networks, as well as good antivirus programs on computers and phones.

Working from home clearly will help protect employees from viruses like COVID-19. But working from home without the proper cyber-protection leaves everyone open to a host of other types of very nasty viruses.

Arvin Chaudhary is chief executive officer of the technology services agency Nadicent Technologies Glastonbury.