DigiKnow
CYBER SECURITY DEPENDS ON YOU

SPRINGING INTO SECURITY

April 2021 | Issue 2021:3

CSO's Message

Greetings,

Don't look now, but the "Nigerian" scams of the 1990's have returned. The intent is the same, to steal your money. But the Nigerian Prince might now be the Bank of America or a wealthy Syrian. IT Security leaders worldwide are alarmed.

Nigeria continues to be a cyber crime hotspot. The poorly written emails from foreign "dignitaries" have morphed into sophisticated criminal networks preying on businesses, healthcare and government benefit programs.

AARP provides this advice:

-Do not reply, even out of curiosity, to emails from someone representing himself or herself as a foreign government or business official who needs help transferring a large sum of money.

-Don't provide personal or financial information to anyone making such an appeal.

-Be skeptical of promises of big dollar payoffs for participation in money transfers.

In the coming months we will provide updates on this topic. Awareness and vigilance are the best tools for avoiding these scams.

Solomon Adote
Chief Security Officer

THIRD PARTY COMPROMISES

PROBLEMS CONTINUE TO GROW

Recently there have been a number of breaches of third party providers involved in banking, healthcare, insurance and other industries. You may have received correspondence from your bank or other institution in this matter. Below are parts of an actual notification letter referencing the Accellion breach.

*Accellion, a vendor that ******* uses for its file sharing platform, informed ******* on January 22, 2021 that the platform had a vulnerability that was exploited by an unauthorized party. After Accellion informed us of the incident, we permanently discontinued use of this file sharing platform.*

*Unfortunately, we have learned that the unauthorized party was able to access some of ******** information on the Accellion platform – and that we are one of numerous Accellion clients who were impacted.*

We acted immediately to contain the threat and have engaged a team of third-party forensic experts to investigate and determine the full scope of this incident. We are working expeditiously with our internal and external teams to determine what data may have been accessed.

The security of our customer's information is central to our business values. If we determine your personal information was impacted, we will contact you directly via U.S. Mail and, out of an abundance of caution, provide instructions to sign up for free credit monitoring services.

While as individuals we cannot prevent these type of compromises, we can be aware and act, should our personal data be involved. Look out for emails and regular mail from your mortgage companies, health care providers, insurance companies, etc. You are looking for content that suggests your private information was stolen and what data elements were associated with the breach. Depending on the data elements, you have the right to demand credit monitoring and access to your detailed credit report for a year from all three credit reporting organizations. You also should pay close attention to any credit requests that you did not initiate.

DTI continues to collaborate with IT Security leaders nationwide to protect Delawareans' data. We work with all state government organizations to make certain that networks and systems are patched and updated to limit opportunities for the bad guys to find a way in. Each of us can do our part in securing any data we are responsible for and protecting our personal information.