Worldwide Cyber Tensions Continue

March 2022 | Issue 2022:3

Uptick in Cyber Attacks Continues to be a Real Threat

As we reported in last month's newsletter, the possibility of increased cyber attacks continues as the Russia/Ukraine conflict shows few signs of ending soon.

Economists at Goldman Sachs join a growing chorus of experts and government officials cautioning that cyberattacks are now among the biggest threats to U.S. national security.

While improbable, criminal cyber activity aimed at critical U.S. infrastructure is still technologically possible and could be "extremely destructive," Goldman notes.

Hundreds of thousands of Ukrainian technology workers have taken part in cyberattacks against Russia's government, media and financial institutions in recent days, according to a top Ukrainian cybersecurity official.

We're calling on everyone involved in storing, processing, and safeguarding Delawarean's data to practice extreme diligence. Each of us can do our part by reviewing and implementing cyber hygiene steps.

Secure Your Accounts - Use strong passwords, different for each account. Turn on Two Factor Authentication. Review and increase the security of your social media accounts. Hacked accounts are used to spread disinformation and enable scams.

Software Updates - Update all of your devices now. Don't forget gaming consoles, VR sets, and tablets. Accept updates for your apps, devices and software as soon as they are available.

Solomon Adote
Chief Security Officer

Watch Out for Smishing Texts

"Smishing" might be a funny-sounding word, but Aaron Rouse, the FBI's Special Agent in Charge of its Las Vegas office, says it's a serious problem.

Like "phishing," when scammers try to entice victims to click on an email link, smishing involves receiving Short Message Service (SMS) as a text message on your cell phone. A typical smishing scam message may seem like it's from a bank – maybe your bank – and include a link or phone number to bait you into clicking or calling. If you do, you stand a good chance of being hooked. And that's when the scammers get to work, manipulating your personal information, which they can sell and/or use in another scam.

A few examples of smishing making the rounds – a text claiming to be from AT&T saying your bill has been paid, followed by a link to claim a prize, or a text claiming to be Netflix telling the target they need to click on the attached link if they want to "keep watching." Smishing messages usually include a link to a site that spoofs a popular bank and tries to siphon personal information. But increasingly, phishers are turning to a hybrid form of smishing — blasting out linkless text messages about suspicious bank transfers as a pretext for immediately calling and scamming anyone who responds via text.

According to Checkpoint Security, Smishing botnets use the phone numbers of the existing infected devices, and the phishing domains constantly change. This makes it harder, if not impossible, to block phishing SMS messages on the level of the telecommunications company, or even trace them back to the attackers. Together with the easy adoption of the "botnet as a service" business model, it should come as no surprise that the number of such applications for Android and the number of people selling them is growing. At this time, the only scalable and long-term solution for this problem seems to be raising security awareness among the general public.

Here are some things you can do to avoid being a victim of a smishing attempt:

1) Never click links, reply to text messages or call numbers you don't recognize.
2) Do not respond, even if the message requests that you "text STOP" to end messages.
3) Delete all suspicious texts.
4) Make sure your smart device OS and security apps are updated to the latest version.
5) Consider installing anti-malware software on your device for added security.

CTIA represents the U.S. Wireless industry. Its membership includes carriers and equipment manufacturers as well as mobile app developers and content creators. The organization provides information and resources on all things wireless, including information on how to block and reduce unwanted and harmful texts.

CTIA - Home