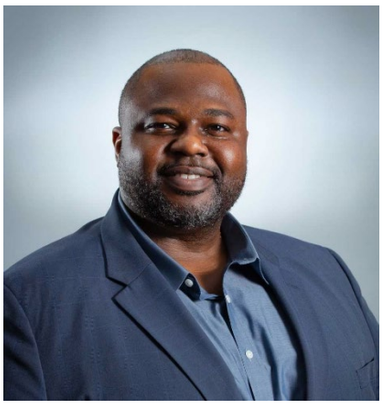
DigiKnow

CYBER SECURITY DEPENDS ON YOU

NEW YEAR - NEW CYBERSECURITY THREATS

January 2023| Issue 2023:1



Building a Security-Aware Culture and a Cyber-Crime Resilient Framework

One of the most important safety steps that any organization can take is fostering a culture of awareness around cybersecurity issues. It's no longer good enough for employers or employees to think of cybersecurity as solely the responsibility of the IT department. In fact, it is an important part of everyone's job to develop a personal awareness of the threats and how to take basic precautions to ensure cyber safety at work and at home too!

The National Institute of Standards and Technology, (NIST) defines cyber resilience as: "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Cyber resiliency is the primary goal of our Security Operations Teams.

It bears repeating that Phishing attacks rely on social engineering methods to trick people into divulging valuable information or installing malware on their devices. No one needs technical skills to educate themselves about these types of attacks and take basic precautions to avoid becoming a victim.

Our monthly cybersecurity training modules help reinforce basic cyber hygiene skills like protecting passwords, safe use of USB drives, and physical building security. Fostering a culture of cybersecurity awareness should be a core element of business strategy at all organizations to

EXPERTS' PREDICTIONS FOR 2023

Statista, a market and consumer data company, estimates that the global cost of cybercrime will reach $10.5 trillion by 2025. According to Forbes, the shift to home and remote working, as well as the spread of the internet of things (IoT) into every area of business and society, means there has never been more opportunity for lax security to cause headaches and expense. Because of this, cybersecurity is top of everyone's agenda in 2023, so here's a look at some of the key trends:

Internet of Things (IoT) and Cloud Security -The more devices we connect together and to our network, the more potential doors and windows exist that attackers can use to get in and access our data. And in 2023, analysts at Gartner predict, there will be 43 billion IoT-connected devices in the world. It's been shown that even when they don't store data themselves, attackers can often find ways to use them as gateways to access other networked devices that might. In 2023, a number of governmental initiatives around the world should come into effect. These are designed to increase security around connected devices, as well as the cloud systems and networks that tie them all together. One initiative is a labeling system for IoT devices set to be rolled out in the U.S. providing consumers with information on possible security threats posed by devices they bring into their homes.

Artificial intelligence (AI) - As the number of attempted cyberattacks has grown rapidly, it has become increasingly difficult for human security experts to react to them all and predict where the most dangerous attacks will take place. This is where **AI** comes into play. Machine learning algorithms can examine the vast amount of data moving across networks in real-time far more effectively than humans and learn to recognize patterns that indicate a threat. Because of the availability of **AI**, hackers and criminals are growing increasingly proficient at using it, too. **AI** algorithms are used to identify systems with weak security or that are likely to contain valuable data among the millions of computers and networks connected to the internet. **AI** can also be used to create large numbers of personalized phishing emails designed to trick receivers into divulging sensitive information and become increasingly good at evading automated email defense systems. **AI** has even been used to artificially "clone" the voice of senior executives and then to fraudulently authorize transactions.

Crypto Scams and Pig Butchering - Using translation programs to communicate with global victims, scammers looking for a payout ,have launched what authorities call "pig butchering" scams. Scammers cold-contact people on SMS (texting) or direct messaging on other social media, dating, and communication platforms. Often, they'll simply say "Hi" or something like "Hey Josh, it was fun catching up last week!" If the recipient responds to say that the attacker has

ensure they build resilience and preparedness to recover in the event of an attack .

Solomon Adote
Chief Security Officer

the wrong number, the scammer seizes the opportunity to strike up a conversation and guide the victim toward feeling like they've hit it off with a new friend. After establishing a rapport, the attacker will introduce the idea that they have been making a lot of money in cryptocurrency investing and suggest the target consider getting involved while they can. The scammers are basically 'fattening the pig' until it's time to "butcher" it, when they take all the money out of the victim's account.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**