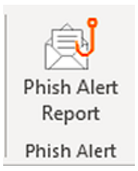
DigiKnow
CYBER SECURITY DEPENDS ON YOU

SUMMER TRAVEL CYBER SAFETY

July 2021 | Issue 2021:6

CSO's Message



SUMMER IS NO TIME FOR PHISHING

Unfortunately, employees are often the first target of hackers trying to breach an organization's defenses. It is easier to attack an organization from the inside. That is why much of our security training is geared to helping you spot phishing and other intrusion tactics. The button you see is one way state and K12 network users can help in the war against cyber fraud. If you receive a suspect phishing email, simply click on the phish alert report button and follow the prompts.

As state and K-12 employees you have a unique opportunity to be on the frontlines in the war against cybercrime. Delaware's annual Security Awareness Assessment/Training kicks off in August for all employees.

This year we will be doing something a little different, everyone will be given the opportunity to “test out” of taking the training. If you get a 70% or above on the assessment you won’t have to take the annual training. The monthly “Netflix’ type trainings will continue to be assigned, as well as any training directed by your agency leadership and based on phish test performance. If you get a 69% or below, you will be assigned the annual training.

More specific information on 2021's Security Awareness Assessment/Training will be arriving in your mailboxes soon. Remember, cyber security depends on all of us.

Solomon Adote
Chief Security Officer

VIRTUALLY PROTECT YOUR INFORMATION

After last summer's restrictions, many of us are eager to travel. Whether it's to visit family, the beach, or the mountains, our devices are coming with us. It's time for a refresher in keeping our information safe as we enjoy public places and spaces.

Public Wi-Fi is so tempting, it's in restaurants, hotels and attractions. Here's the problem with public Wi-Fi, it's inherently insecure, as ZD Net points out. This leaves public Wi-Fi users vulnerable to all sorts of bad actors looking to steal your information.

One solution is to install a Virtual Private Network.(VPN). Each time you access the internet a whole series of communication events take place. The way a VPN works is by encrypting information packets at the originating point, often hiding not only the data but also the information about your originating IP address. The VPN software on your end then sends those packets to the VPN server at some destination point, decrypting that information.

The VPN service gives you an app that you run on your local device. It encrypts your data then it travels in its encrypted form through a tunnel to the VPN service provider's infrastructure.

Two things happen here: First, if you're using an https connection, your data is encrypted by your browser and then by your VPN app. At the VPN data center, your data is decrypted only once, leaving the original encryption provided by the browser intact. That encrypted data then goes on to the destination application, like your bank.

The second thing that happens is that the web application you're talking to does not get to see your IP address. Instead, it sees an IP address owned by the VPN service. This allows you some level of anonymous networking.

There are numerous free VPN services. Most IT experts warn against their use. Malware providers and criminal organizations have set up free VPN services that not only don't protect you but actively harvest personal data and either use it or sell it to the highest bidder. Instead of being protected, you're being plundered.

The Federal Trade Commission (FTC) suggests researching VPN apps before you commit to one. You are trusting a VPN with potentially all of your traffic. Look up outside reviews from sources you respect. You can also look at screenshots, the app’s description, its content rating, and user reviews. The fact that an app promises security or privacy does not necessarily make it trustworthy.

Carefully review the permissions the app requests. Apps will present the permissions they request on their app store page, during installation, or at the time they use the permission. It’s useful information that tells you what types of information the app will access on your device in addition to your internet traffic.

For more information on VPN's:

Best VPN service of 2021 - CNET

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Information & Technology 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/pages/cybersecuritynewsletters.shtml