Say NO to HO HO HOaxes

November 2021 | Issue 2021:10

Does it feel sometimes that you are bombarded with requests to change and update your passwords? Do you resent two factor authentication? Do you still use the same password on nearly every website?

The question we **all** need to be asking is: are we doing enough to protect our identities from cyber criminals? DigiKnow that 47% of Americans have experienced some type of financial identity theft? DigiKnow that 91% of cyber attacks start with a phishing email? The average price for a stolen US credit card: $1 and the price of a stolen healthcare record: $10. Cybercrime proceeds ($105B) outpace illegal drug profits.

These are just a few of the statistics that motivate our security staff to constantly harden our network, explore cutting edge technologies and provide training for all state and K-12 employees.

Recently the value of these efforts was demonstrated on the K-12 side. Unknown perpetrators launched a coordinated phishing attack against this network. Thankfully, a number of alert, well-trained individuals recognized the emails for what they were, a Phishing attempt. These K-12 employees immediately utilized the **PhishAlert** button deployed by DTI. Armed with reports from over 20 employees, DTI staff was able to remove this Phish from the K-12 network before it could wreak havoc. Kudos and thanks to these Cyber Heroes! They truly did save the day!

Solomon Adote
Chief Security Officer

HOLIDAY PHISHING SCAMS

You get an email with an exclusive deal, just for you. Because you've shopped at a certain retailer, the email says, you're eligible to receive a special offer. So you click through to the retailer's landing page, enter your personal information and — poof — you've just been scammed. This could be the beginning and end of your online holiday shopping season if you're not prepared.

The Federal Trade Commission (FTC) is highlighting a rampant rise in Amazon impersonation scams. From July 2020 through June 2021, an estimated one in three people who reported a business impersonator to the FTC said the scammer claimed to be calling from Amazon. Nearly 96,000 people reported being targeted, and nearly 6,000 said they lost money. Reported losses topped more than $27 million. This scam often involves an unexpected message from "Amazon," warning that there's been suspicious activity or unauthorized purchases on the person's Amazon account.

Be on the alert for these holiday scams as reported by AARP:

• Delivery scams: As holiday packages crisscross the country, scammers send out phishing emails disguised as UPS, FedEx or U.S. Postal Service notifications of incoming or missed deliveries. Links lead to phony sign-in pages asking for personal information, or to websites infested with malware.
• Travel scams: Despite the pandemic, 46 percent of U.S. adults plan to travel during the holidays in 2021, a SurveyMonkey poll found. Spoofed booking sites and email offers proliferate, with travel deals that look too good to be true probably are.
• Letter from Santa scams: A custom letter from the jolly old elf makes a holiday treat for the little ones on your list, and many legitimate businesses offer them. But so do many scammers looking to scavenge personal information about you or, worse, your kids or grandkids, who may not learn until many years later that their identity was stolen and their credit compromised.

Locally, a fraternal organization in Newark warned about a scammer on their Facebook page. A person falsely representing the organization's craft show staff was phishing for potential vendors' registration fees.

Warning Signs
• Huge discounts on hot gift items, especially when touted on social media posts or unfamiliar websites.
• Spelling errors or shoddy grammar on a shopping website or in an email.
• A shopping or travel site does not list a phone number or street address for the business and offers only an email address or a fill-in contact form.
• A website does not have a privacy policy.
• An unsolicited email asks you to click on a link or download an app to access a deal or arrange a delivery.

This year, be a cyber-savvy shopper and think before you click.