DigiKnow
CYBER SECURITY DEPENDS ON YOU

HO TO THE NO - WATCH OUT FOR SEASONAL SCAMS

November/December 2024 Issue 2024:10

HOLIDAY SEASON BRINGS OUT THE BAD GUYS

As we enter the season of shopping, eating, and giving, most of our thoughts center on family and festivities. Sadly, the opposite is true for cyber criminals. They look at this time of year as hunting season for scams and theft, of both money and personal information.

One of the most devious scams takes advantage of peoples' good will. Charitable contribution fraud is prevalent at year's end. Here are some scams to watch out for:

Impersonating Real Charities: Scammers often use names that sound like well-known charities to trick donors.

Emotional Appeals: They create heart-wrenching stories or capitalize on current events and disasters to evoke an emotional response.

Fake Websites and Social Media: Crooks set up fake websites or social media profiles that mimic legitimate charities.

Phishing Emails: Scammers send emails that appear to be from reputable charities, asking for donations.

Unsolicited Phone Calls:/Texts: You receive an urgent unsolicited call or text

HOLIDAY HEARTBREAK ONLINE SHOPPING SCAMS

Three out of four Americans ages 18 to 85 told a 2023 Michigan State University survey they had bought a fake product in the previous year. Americans buy $2 trillion in counterfeit products annually, according to the National Crime Prevention Council. These include knockoffs of brand name clothing and shoes, household goods, electronics, cosmetics, and more.

American Business magazine, Forbes, reports on scams to avoid during the 2024 holidays:

The Gift Card Peek Scam
Scammers will take gift cards off the rack, scratch off the silver coating that protects the PIN code, record the code, then carefully apply a new coating in a way that leaves buyers none the wiser.

The perpetrator waits a day or two for the card to be purchased and activated, and the card number and PIN are ready for the scammer to use.

Solution: Carefully examine any gift cards you purchase. Better yet, send e-gift cards directly to recipients from a reputable site.

Counterfeit Goods Scams
An estimated 57% of shoppers will make their purchases online this holiday season, according to research from the accounting giant PwC. You can be sure scammers will be ready, advertising hot deals on well-known brands via social media.

Their websites will look genuine and may even feature the brand’s name in the URL for legitimacy. You or your recipient will probably even receive the goods, but they’ll clearly be cheap knockoffs.

Solution: Buy from reputable sites you trust. If you’re suspicious, do a Google search of the site’s name plus the word “scam” to see what comes up.

Mail Theft
Surprisingly, sending cash through the mail is still popular. But handwritten addresses and colorful envelopes make it easy for thieves to distinguish personal cards from the sea of junk mail and

from a supposed charity representative. They stress an immediate need and suggest that they can take your credit card information over the phone to expedite your donation.

TIPS TO AVOID CHARITABLE FRAUD

Check the Validity of the Charity - Use websites like Charity Navigator or the Better Business Bureau's Wise Giving Alliances to verify validity.

Donate Directly to a Charity - Go directly to a charity's website instead of using a third-party link.

Do Not Provide Any Personal Information - Legitimate charities will never ask for your social security number or other personal data.

Do your research, stay vigilant, and you will be able to avoid falling victim to charitable fraud.

Solomon Adote
Chief Security Officer

bills. They'll steam a card open to look for cash, reseal the envelope and put it back in your mailbox.

Mail theft also happens on a larger scale. There are universal keys that can open any blue post office mailbox as well as keys that unlock entire racks of mailboxes at apartment and condo complexes.

There's been a rash of these thefts recently because the keys are easy to obtain. Once thieves gain access to the boxes, they not only steal cash, but they can also find credit cards and valuable tidbits of information perfect for identity theft.

Solution: Don't send cash. Order a cool gift online or send an e-gift card.

Delivery Notification Scams: Fake emails or texts claiming you missed a delivery leads you to malicious websites.

Solution: Always check the sender's information and avoid clicking on suspicious links.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & 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**