12 SCAMS OF CHRISTMAS TO AVOID THIS YEAR

Tis the season for holiday scams. Holiday preparation and celebrations may keep you busy and distracted, and that's exactly when scammers and identity thieves strike. Keep your holidays bright this year. Learn about "The Twelve Scams of Christmas" and some tips to help protect you and your family.

ON THE TWELFTH DAY OF CHRISTMAS, FRAUDSTERS GAVE TO ME:

12 MALICIOUS HOLIDAY E-CARDS

Holiday e-cards are increasingly popular but may be fraudulent or have potential to deliver malware to your device.

Tip: Delete, don't open, an e-card from an unknown party. If received from a known party, confirm with the sender that they indeed sent it before you open.

11 SEASONAL JOB SCAMS

Retailers hire thousands of temporary workers during the holidays. Before agreeing to work for anyone, watch out for job scams designed to collect your personal information, including Social Security numbers and bank account information.

Tip: Research the company name, address, phone number and website. Call the human resources department to verify that the company is hiring. Ask about the correct application process. Be skeptical if asked to pay any upfront fees.

10 HACKED CHARGING STATIONS

Traveling for the holidays? Charging stations in public places, like airports and hospitals, may look appealing for a quick charge of your mobile device. But cyber criminals have been known to hack these stations to steal sensitive data on your device or to install malware on your device the moment you plug in (called "juice jacking").

Tip: Don't let convenience outweigh security. Avoid public charging stations, except for an emergency.

09 FAKE SHIPPING/DELIVERY NOTIFICATION EMAILS

Were you expecting a delivery? Fake notification emails are often phishing scams designed to trick you into sharing personal or financial information by asking you to verify a purchase. Stop before calling the phone number or responding to the email.

Tip: Keep a list of your online purchases; check off each item as it arrives. Use the vendor's official website to check the status of your purchases. Do not send additional payment to receive your package; payment is typically made at the time of your purchase.

08 BOGUS WEBSITES

Don't trust a website or an online vendor that you don't know; check them out before purchasing, even if the website offers that hard-to-find gift at an unbelievable price.

Tip: Verify that there's a padlock next to the website URL in your internet search engine and that it begins with "https" on the checkout page. Google the URL/address and the company's name followed by the word "complaints" or "scam."

07 PAY WITH GIFT CARD SCAMS

In the rush of holiday shopping online, hit the pause button if you are asked to pay with an Amazon or iTunes gift card or to wire money. This could be a sign that the website you are on is a fake. Scammers prefer to take your cash this way because it's nearly impossible for you to get it back.

Tip: Use a retailer's gift card on the retailer's website for purchases. Otherwise, do not pay for online purchases via general gift cards or by wiring funds.

06 TOO-GOOD-TO-BE-TRUE POP-UP ADS

Be wary of pop-up windows or banner ads that promise unrealistic prices, special coupons or additional discounts before you complete an online transaction. The pop-up may not be associated with the vendor whose website you are visiting.

Tip: Contact the retailer to verify the too-good-to-be-true offer before proceeding.

PNC BANK

05 PICKPOCKETS LURKING

Be aware of your physical security among holiday crowds. Your wallet appeals to criminals for the money and credit cards, but identity thieves also value all of the sensitive data it contains. Your wallet, purse and packages can be quickly pilfered without you noticing.

Tip: Leave nonessential identifying information and spare credit cards at home. Make frequent trips to your car to lock packages out of sight. Park in well-lit areas close to walkways and other people. Be aware of your surroundings — not talking on a phone — when exiting buildings.

04 FRAUDULENT BUY-ONLINE/PICK-UP-IN-STORE OR CURBSIDE PURCHASES

This scam involves fraudsters making online purchases using stolen credit cards. Unfortunately, due to the coronavirus, requirements that the customer produce identification or their credit card when picking up in a store or curbside purchase have become lax to prevent spreading the virus.

Tip: Enable phone alerts for all credit card purchases to detect unauthorized purchases. Scrutinize your credit card statement every month and question any unfamiliar charges, no matter how small. Report any unauthorized transactions immediately to your card issuer.

03 CARD READER SKIMMERS

Thieves can install small electronic devices, called skimmers, over the slot where you insert or swipe a credit or debit card. The device is used to steal details attached to the card, such as your account number and personal information.

Tip: Select ATMs, gas pumps or other devices for which you use a card that are located in public, well-lit areas and free of shrubbery or other obstructions. Look for loose parts or signs of tampering. Give a good tug on the card reader before inserting your card. If the machine appears damaged (scratches, dents, evidence of glue or tape) do no use the machine and report it immediately.

02 GIFT CARD SCAMS

In one scam, the value of gift cards selected from do-it-yourself racks may be compromised by thieves before you even purchase the card, leaving your card value at $0. For those gift cards received that you will never use, there are legitimate marketplaces with buyers willing to take them off your hands for a reduced price. In a second type of scam, fraudsters seek to relieve you of that card by tricking you and stealing the value of the card to make a purchase before you realize you've been victimized.

Tip: Purchase gift cards stored behind counters or from the retailer directly; save your receipt to prove the card's value and purchase date. Use known gift card marketplaces, which have customer-service contacts and are tracked by the Better Business Bureau. Avoid posts in social media offering to pay 100% of the value of your unwanted card.

AND A FAKE OFFER FOR A LETTER FROM SANTA TO A CHILD

Parents and grandparents receive offers to have a personalized letter sent from Santa to a child. Some offers may be legitimate, but many scammers use this as a ruse; a letter never arrives, but you've shared sensitive personal information (name and address) and payment information.

Tip: Opt for the "Letter from Santa" campaign offered by the U.S. Postal Service.

CON PDF 0720 0161

PNC BANK