FDIC

November 19, 2018

FEDERAL DEPOSIT INSURANCE CORPORATION

consumer news

Shopping Online During the Holidays?

Protect Your Money From Scams

During the holiday season, we tend to make a lot more purchases online for travel and gifts, so it's especially important to be vigilant about protecting your money. Here are some of the most common scams to watch for:

Fake Websites and Apps. Scammers often create fake websites that are so similar to the sites of popular retailers, it easily tricks consumers into providing payment information. The scammers take your information and your money, but you never receive the products. Scammers have also developed fake apps that contain malware. When you download the app, the malware steals personal information from your device or locks it, holding it for ransom until you pay the scammers. Other types of fraudulent apps ask you to login using your social media or email accounts that could expose your personal information for the scammers to steal.

Be careful of apps or websites that ask for suspicious permissions, such as granting access to your contacts, text messages, stored passwords, or credit card information. Also, poor grammar or misspelled words in an apps' description or on a website is a red flag that it is not legitimate.

Email Links. Avoid clicking on links in unsolicited emails or emails from unfamiliar sources. The links may lead to an illegitimate website attempting to get you to enter your credit card or other personal information. Some links may download malware (malicious software, such as computer viruses) to your computer when you click on them that can steal your banking information, including login identification, passwords, and credit or debit card numbers. These emails typically look very similar to ones sent by well-known retailers, banks, and other entities.

Be on the lookout for emails that have typos or other obvious mistakes. In addition, be skeptical of email attachments described as coupons, rebates, or payment forms – they could include malware. And avoid email offers that seem "too good to be true." If an email promises popular items for free or a surprisingly low price, it is probably a scam.

Making Payments on Unsecure Sites. Before paying for a purchase online, make sure the website you're on has "https" at the beginning of its URL with a lock symbol:

This means the site has a protected network connection. Websites with

"http" at the beginning of the URL with no "s" are more vulnerable to attacks by scammers who steal credit card information by monitoring network traffic. Also be aware of pop-up windows that appear while you are on a website asking for your credit card information to receive coupons or to win free items. Legitimate companies do not ask for your personal information for those purposes.

Using Public Wi-Fi to Shop or Access Sensitive Information. Wireless connectivity, also known as Wi-Fi, allows your laptop, PC, or mobile device to connect to the internet without a physical wire connection. Many restaurants, hotels, libraries, and other places offer free public Wi-Fi, which is convenient when you're on the go. However, these networks may not be secure (since they either do not require a password or provide the same generic password to all customers for access) and may expose your personal and banking information to scammers looking to steal names, social security numbers, and bank account numbers.

Avoid using public Wi-Fi to make purchases online, login to your financial accounts, or access other sites that have sensitive information about you. It's also a good idea to stick with websites that have "https" encryption (discussed above) when in public places.

Package Delivery Confirmation Scams. This scam is especially popular during the holidays when people receive gifts through the mail that they may not be expecting. The scammers call or email claiming to be from the U.S. Postal Service or a major shipping company and state that you have a package waiting for delivery. To ensure the package is meant for you, you are asked to provide personal information, which the scammers steal to use to open credit accounts in your name. In response to this scam, the U.S. Postal Service explained it does not call or email people and ask for personal information if there is a problem with a delivery. Visit https://postalinspectors.uspis.gov/radDocs/consumer/CrimeAlert-DoNotTaketheBait.pdf for more information.

Don't let these scams dampen your holiday spirits. Instead, here are precautions you can take to protect your money while shopping online:

- In general, always use difficult-to-guess, unique passwords on every account.
- If you're using shopping apps, focus only on official retailer apps found on the retailer's website or a reputable app marketplace, which offer stronger security.
- Never provide your credit card information unless you are on a secure site, showing "https" at the beginning of the URL and the lock symbol.
- Think about implementing two factor authentication on your accounts. Two factor authentication requires you to provide two pieces of evidence when logging into an account. It presents an extra layer of security to make it more difficult for someone who isn't you to log into your account. For more information, visit https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication
- Monitor credit card bills and bank statements as well as app and other online transactions for unauthorized purchases or withdrawals. Immediately contact your bank if you see anything suspicious. In addition, you may want to consider signing up for alert services. Many credit card issuers, banks, and mobile app providers offer services that notify you about certain account activities, such as recent logins from unrecognized devices.

For more help or information, go to **www.fdic.gov** or call the FDIC toll-free at **1-877-ASK-FDIC (1-877-275-3342)**. Please send your story ideas or comments to Consumer Affairs at **consumeraffairsmailbox@fdic.gov**

FDIC