DATCU
CREDIT UNION

Common Holiday Scams

We love the holidays and all the festivities that accompany this wonderful time of the year.

However, it is also a favorite season for cyber criminals and scam artists intent upon taking advantage of those celebrating the joys of the holiday season.

Below are a few important tips that can help reduce your chances of becoming a victim. Please read them carefully.

1. DATCU will NEVER contact you, or any member, requesting your personal information. We have seen instances of fraudsters pretending to be DATCU employees calling from a spoofed/fake DATCU phone number. They request information such as your one time PIN number. NEVER share your personal information with anyone for any reason.

2. Online shoppers are a high-value target for scammers. Many fake /spoofed internet websites or social media ads (Facebook, Instagram etc.) promote great deals from a "legitimate retailer". These are often "fake websites". In these cases, consumers buy holiday products and gifts but never receive the purchased merchandise. How can you know for sure if it is a reputable seller or website?

- Read reviews to see if it is a valid site.

- If the deal seems too good to be true, it probably isn't a legitimate retailer.

- Confirm that it is a secure site. Look for HTTPS (vs. HTTP) and a green padlock symbol next to the URL address.

- Look carefully at the URL. Is the retailer name spelled correctly and does it correlate to the website. Misspellings (even one character) or poor grammar frequently indicate a fake website.

- With so many deliveries during the holidays, beware of delivery service emails that claim you have a pending or missed delivery. They look like they are from UPS, FedEx, USPS etc. and request that you "click a link" and enter personal information. Do not fall for it!

Simply put, NEVER enter your personal information into a website that you are not 100% confident is a legitimate and secure website.

3. An unexpected or unsolicited email with a directive to "click a link" or download an app to verify an online order that you have made, or initiate a special coupon offer, etc. is a cause for concern. Do NOT click these links. They often have malware (viruses) that can compromise your identity and even access your personal information.

4. You may want to avoid using debit cards or other payment sources that link directly to your credit union or bank account. If there is a data security breach of a retailer, scammers and cyber criminals may gain access to your accounts and empty them. Using a credit card might be a better alternative. DATCU offers a Cash Back Rewards Credit Card where you will earn money back on every purchase. Frequently, credit cards offer fraud protection and put no liability on you as a consumer.

5. One of the top gift items year after year is gift cards. Gift cards scams are a big deal. In 2018, it was reported that one of the most common gift card scams centered around eBay/Craigslist card selling scams and Police/IRS impersonation scams. If someone calls you and says you owe money and that you must purchase gift cards or you will go to jail, it is a scam!

6. One of the most prolific areas of theft is the identity of our children. Why? It can take many years before we realize that our kids or grandkids identity has been stolen. During the holidays, there are many fake companies claiming that they can send a letter from Santa himself to your child or grandchild. It is another nefarious action to gain personal information on kids.

7. Always be vigilant in reviewing your accounts and statements. Take a few minutes each day to go online and check your accounts for fraud or even duplicate charges. If you see something that is not correct, contact DATCU or your financial institution. It can save you a lot of hassle.

The above is only a brief summary of common cyber and holiday scams. These are good tips to remember all year long. At the end, there are several links to other great tips and sources on security scams.

Finally, Cyber Monday and Cyber Week 2019 was the largest online shopping events ever. Millions of Americans will be having packages delivered.

Ways to Prevent Porch Theft

• If allowed, have your purchases mailed to your workplace. If not, send to a friend or trustworthy neighbor. If you know that you will not be home, do not have the packages delivered to your home but somewhere else or have someone you trust pick them up and hold them for you.

• If the item is expensive, require that a signature be required for delivery.

• Thieves do not like inconvenience. Think about anti-theft products like lockable delivery bags and drop boxes. You can also install Wi-Fi-enabled security cameras and motion sensitive lights.

• Rent a delivery box or locker. There are major retailers that offer delivery hubs with secure lockers.

Other sources:
https://www.consumerfraudreporting.org/current_top_10_scam_list.php
https://aarp.org/money/scams
https://blog.knowbe4.com