PENNSYLVANIA STATE POLICE
COMMUNITY AWARENESS BULLETIN
CAB 006-19 December 9, 2019

BEWARE OF HOLIDAY SCAMS

The Pennsylvania State Police (PSP) reminds commonwealth residents to remain aware and protect themselves from holiday scams. Criminals capitalize on an increase in spending, online shopping, and charitable giving during the holiday season. Scammers target and exploit victims in several ways. The PSP is providing the following information regarding some of the most common holiday scams residents should be aware of, such as fake shipping notifications, money transfer scams, holiday travel scams, copycat websites, fake charity scams, and package theft.

Fake shipping notifications are a type of scam designed to trick the victim into clicking a fraudulent/malicious link in order to see the shipping status of their package. If the victim clicks the fake link, software could be downloaded onto the victim's computer or cell phone, compromising it. This email scam may be sent after someone makes a legitimate online purchase or at random.

Money transfer scams promise victims extra, unearned cash if they use a money transfer service to wire money back to the scammer. A fraudulent check, over payment, or secret shopper offer are several ways scammers trick victims into wiring them money. The scammer provides the victim with a counterfeit bank check and requests that the victim send a portion of the money back to the scammer. By the time the counterfeit check is discovered, the wired money is gone and nearly impossible to recover.

Holiday travel scams offer significantly discounted prices for airline tickets and hotel rooms. Fake email offers include links to fraudulent websites that collect bank account information and other personally identifiable information during the checkout process.

Copycat websites target internet users who incorrectly type in a website address into their browser or click on a link that looks like it is from a legitimate website. The fake websites mirror real company websites and collect users' log in credentials and passwords.

Fake charity scams are established by criminals to collect donations that appear to be for other well-known charities or for vague causes such as "California Wildfires" or "Gifts for the needy." Fake charity scams may be over the phone, through email, or in person. The scammer uses a victim's sympathy and often requests a donation quickly.

Package theft is an increasing problem with the uptick in online shopping. There are many packages sitting unprotected outside of their intended destinations. This provides thieves with easy access to steal holiday gifts from victims' doorsteps.

Recommendations

- Use a credit card to make the purchase or ask your bank about single-use credit cards for holiday purchases.
- Use secure websites, which can be identified by the lock symbol in the address bar.
- Log directly into a business website by carefully typing in the official address.
- Purchase airline tickets and hotel reservations through official websites.
- Be skeptical of cashback rewards and research offers before signing up.
- Be skeptical of "cold calls" and unsolicited emails from charities.
- Do not click unknown links in emails.
- Do not accept personal or commercial checks from unknown individuals.
- Do not transfer money via gift cards, prepaid debit cards, or other untraceable forms of payment.
- Do not log into websites using linked social media usernames and passwords.
- Do not provide personal information, addresses, or bank account numbers to anyone you are not certain is legitimate.

The PSP reminds residents, if you fall victim to a scam, call your bank and local police department. Additionally, victims can make a complaint with the FBI Internet Crime Complaint Center (IC3) at https://www.ic3.gov/complaint/default.aspx.