Be Aware of These 6 Holiday Ho Ho Hoaxes

From Black Friday to New Year's Eve, take steps to help reduce the risk of fraud this season by learning about these common holiday scams and tips to protect yourself

PITTSBURGH, Dec. 6, 2017 – Attention shoppers: a Monday Christmas holiday may mean an extra-long weekend for you to shop 'til you drop, but fraudsters see it as more opportunity to trick innocent holiday revelers with holiday-related scams.

In fact, ACI Worldwide reports that from 2015 to 2016, global fraud attempts grew by 31 percent between Thanksgiving to New Year's Eve. Generally fraud losses are 20 percent higher during the holiday season, according to the Association of Certified Fraud Examiners.

"With fraud efforts spiking around holiday shipping deadlines and December 25, consumers should take time to educate themselves on popular fraud attempts and how to protect themselves," said Trevor Buxton, a fraud awareness and communications manager and Certified Fraud Examiner with PNC Bank.

"Taking the extra time now will help you guard against starting out the New Year on the wrong foot."

Buxton offers information on this season's most common scams and tips on how to guard against them:

Gift Card Fraud

- Gift cards – both electronic and plastic – are a popular option for gift-givers. For the eleventh year in a row, 61 percent of consumers want gift cards as a holiday present, according to the National Retail Federation.
- But gift cards also are highly prone to fraud. Because they do not contain customer information, they are not traceable and scammers can get money fast.

Copycat Websites & Mobile Apps

- Some say imitation is the sincerest form of flattery, but not when it comes to websites or apps. Fraudsters like to be copycats and engage in cybersquatting, where they profit by imitating someone else's trademark.
- They take well-known brands, create a website with a few extra words in the URL, market goods using words such as "hot-selling" or "discount" and voila – they are in business. You hand over your credit card number, but the fraudsters have no actual merchandise to sell.
- To guard against these copycat websites, search online yourself for the real company's website. Double check information such as a company's street address or phone number when you enter their website. As an added precaution, use Whois.net, which allows you to check domain names and registration of websites.
- Use caution when downloading mobile apps. Always download and install apps from well-known stores, such as Apple® Store, Google Play Store, Amazon Store and Windows® Store. Some applications can house malware capable of stealing your data as you use your phone or charge money to your app-linked accounts without your knowledge.

Fake Shipping Notifications

- Did you get an email saying a shipper is trying to deliver a package or a package is undeliverable, but you don't remember providing your email address? It could be a scam.

- Attachments or links in these emails could be a phishing attack and pollute your device with malware in an attempt to steal passwords, personal information or worst case – your identity. PNC offers tips to help you learn how to identify a phishing attempt.
- Always visit the shipping services' valid website to call and verify. Fraudsters may also place a "missed delivery" postcard on your door that could contain false numbers. Some lead to a fraudulent company overseas, which is one expensive call to make.

Phony E-Greeting Cards

- If you receive an e-card in your inbox and can't make out the sender's name, chances are it's not a secret admirer, but a fraudster. Always delete an e-card from someone that you don't know. Legitimate companies also will never make you share personal information to open a card.

Help Wanted: Seasonal Job Solicitations

- You or your teenager may be looking to earn some extra cash to spend over the holidays, and seasonal jobs are a popular option. During your job search, go to the company's main website to apply or apply in person. Never pay or share personal information to get a job lead.

Travel Scams

- See a travel deal around the holidays that seems too good to be true? Chances are it is. Fraudsters reel you in with fake travel websites and vacation rentals, and stop responding once you enter your credit card number.
- Guard against these scams by dealing with a reputable travel agency or directly with a property owner. In addition, follow these tips to help secure your finances during holiday travel.

Think you're a Victim?

- Regardless of the scam or amount you think was compromised, contact your financial institution, law enforcement and then file a complaint with the FBI's Internet Crime Complaint Center.
- You also can report a scam to the Better Business Bureau's Scam Tracker.
- PNC offers security tips to help keep yourself safe during holiday shopping.

# # #

CONTACT:
Amy Vargo
(412) 762-1535
amy.vargo@pnc.com

Additional assets available online: Photos (6)

https://pnc.mediaroom.com/2017-11-21-Be-Aware-of-These-6-Holiday-Ho-Ho-Hoaxes