Title: Beware of These 6 Fraud Scams Hitting Businesses this Thanksgiving

Description: Don't let holidays distract you from fraudsters trying to gobble up your business payments this Thanksgiving.

The holidays are just around the corner. Thanksgiving is a special time for gathering with friends and family, but fraudsters are set to make sure you have much less to be thankful for this holiday season.

In 2021, holiday shoppers dropped a record-breaking $9 billion on Black Friday and Cyber Monday shopping[1]. While you may awake from your turkey-induced coma refreshed and ready to embrace the madness of the two biggest shopping days of the year, you must remember these popular days bring with them an increased risk of a fraudulent attack. Fraudsters will target consumers to steal credit card numbers, bank account numbers, social media accounts, and email addresses.

Some data hints that consumers know the potential threats they face while shopping for Holiday presents. According to TransUnion's (NYSE: TRU) 2022 Consumer Holiday Shopping report, most consumers (54%) are concerned with being victimized by fraud this holiday season, a 17% increase from the last year[2]. Additionally, consumers are more concerned with fraud this year than in previous years. Though you may be aware of an increased risk of fraud this Thanksgiving, spotting a scam or scheme can be challenging as fraud schemes get increasingly more sophisticated each year.

Here are six fraud schemes you should be aware of and how to prevent them:

1. **Phishing**

Phishing occurs when fraudsters send a fake message designed to trick a human victim into revealing sensitive information so that the attacker can expose the victim's device to malicious software to get their credit card information and passwords.

To prevent a phishing attack, you should be aware of the following:

- Poor spelling or grammar
- Requests for sensitive or personal information, or to update profile or payment information
- Requests to send or move money
- A sense of urgency

2. **Fake Order Attack**

Like a phishing attack, a fake order attack urges consumers to click on a text or email that notifies them of a problem with an order even though the user has not purchased anything[3]. These messages appear to be from a legitimate sender and encourage the receiver to input information to see the issue.

To prevent a fake order attack, do not click on a link if you know you have not purchased something. If you suspect a problem with your order, check the original confirmation you received upon purchasing an item.

3. **Fake Website Scam**

The internet has opened the door for more complex fraud schemes, with fake website scams growing in popularity. Scam artists create phony websites and fake online businesses, add fake “positive” reviews, throw in a fake street address (or sometimes use the actual location of an unsuspecting business), and wait for payments. Unsuspecting customers who fall for the scheme submit online payments or wire transfers for a transaction[4]. Sadly, because the company does not exist, you can't track scam artists and recover the funds.

Checking to see if a website is legitimate is a simple way to prevent this type of fraud. To do so:

- Carefully look at the address bar and URL
- Double-check the domain name – scammers will spoof domain names to make them look like legitimate websites, such as Yahoo (Yah00). Always check your address bar to ensure you will be redirected to a legitimate site before clicking on a link.
- Look out for poor spelling and grammar

4. **Fraudulent Gift Card Scam**

Like fake website scams, gift card scams are on the rise. According to the Federal Trade Commission, nearly 40,0000 consumers reported losing $148 million in gift card scams in the first nine months of 2021[5]. One example is when a fraudster calls and pretends to be part of a government agency, like the Social Security Administration. They will demand funds from a gift card to fix a "problem" with your account and threaten to freeze it if you don't act on their request.

To avoid this scam, always remember that no legitimate government or other agency will ask you to pay with gift cards.

5. **Credit Card Skimmers**

Thanksgiving and Christmas are two of the biggest travel days of the year, with more than 112 million Americans expected to travel this Thanksgiving holiday based on survey reports[6]. Before swiping your credit or debit card at an ATM, gas station, restaurant, or shopping mall, be aware of the following scam: credit card skimmer fraud.

A skimmer is a device installed on card readers that collects card numbers. Once a card has been swiped, thieves will recover and use the information to make fraudulent purchases[7]. To prevent this, banks and law enforcement officials recommend using either a credit card at the pump that does not require a pin or paying inside. Fraudsters can watch consumers with a tiny camera and see them enter their pin number. Once that pin number is entered, the fraudsters have your card number and pin number. They then create fake cards and go to the ATM to drain your account.

If you must use a credit card at the pump that requires a pin, check for a skimmer beforehand by looking for alignment issues between the card reader and the panel underneath it. Often, skimmers are put on top of the actual card reader and jut out an odd angle or cover the directional arrows found on the original panel. If you cannot determine whether a skimmer has been applied, compare the card reader to a neighboring ATM or gas pump to spot any differences.

6. **Fake Charity Scams**

Fake charity scams run rampant around the holidays as people are in the spirit of giving. According to the FBI, charity fraud schemes seek donations for organizations that do little or no work—instead, the money goes to the fake charity's creator[8]. This scam can come in many forms, including emails, social media posts, crowdfunding platforms, cold, calls, and more.

Follow these tips from the FBI to prevent this type of scam:

- Give to established charities or groups whose work you know and trust.
- Be aware of organizations with copycat names or names like reputable organizations.
- Do your research. Use the Federal Trade Commission's resources to examine the track record of a charity.
- Give using a check or credit card. If a charity or organization asks you to donate through cash, gift card, virtual currency, or wire transfer, it's probably a scam.
- Practice good cyber hygiene:
    - Don't click links or open email attachments from someone you don't know.
    - Manually type out links instead of clicking on them.
    - Don't provide any personal information in response to an email, robocall, or robotext.
    - Check the website's address—most legitimate charity organization websites use .org, not .com.

<u>You become a victim of fraud. Now what?</u>

If you took all the steps to prevent a fraudulent attack or holiday scam and it still happened, don't worry. You aren't alone. Acting quickly against fraudsters is the first step to stopping them. Here are ways you can recover after an attack[9]:

- Think locally and report the scam to your local law enforcement
- Match the agency to the crime: Find the correct government agency to help you handle your case
- Focus on emotional healing

The holidays are hectic, but it's important to remember to stay vigilant against fraud. Following these tips and learning how to spot fraud schemes and other common scams can ensure you can relax with your friends and family for the rest of the year without dealing with the stress or worry of a fraudulent attack.

Sources:

[1]Aura: The Worst Black Friday & Cyber Monday Scams (2022 Update)
[2]TransUnion's (NYSE: TRU) 2022 Consumer Holiday Shopping Report
[3]Aura
[4]North Dakota: Fake Website Scams
[5]Federal Trade Commission: Consumer Protection Data Spotlight
[6]The Vacationer
[7]Forbes: How to Spot a Credit Card Skimmer
[8]FBI Common Scams and Crimes: Charity and Disaster Fraud
[9]Consumer Reports: What to Do If You've Been a Victim of Scams or Fraud