

PUBLIC ADVISORY: Holiday Shopping Scams: *Deals, Deals and More Scams!*

As the holiday season and shopping begins, fraudsters will look to take advantage, below are several common holiday scams.

Online Shopping Scams: The Better Business Bureau (BBB) warns shoppers of an increase in fake websites or personal sellers offering discounts this holiday season. Fake ads posted on social media sites show expensive or in high demand products at unbelievable low prices luring in potential victims. Scammers create bogus sites stealing photos and logos from legitimate businesses to obtain PII, credit card information or send shoppers a cheap counterfeit product.

Puppy Scams: Adding a furry friend is a common occurrence during the holiday season. The internet has become the go to place to find those new friends, unfortunately 80% of sponsored pet advertisements online may be fake according to the BBB. **Before purchasing a furry friend, individuals should conduct a reverse image search for other ads. Do research on a fair price for the breed and never purchase a pet before seeing them in person. Avoid wiring, using cash app or gift cards.**²



Congrats! You've been selected to participate in our monthly **\$1000 Costco Gift Card Promotion!**



Phishing Attempts: Likely phishing emails are nothing new to your inbox, however you are likely to see an increase in these attempts over the holiday season. Scammers will send emails impersonating legitimate companies (Amazon, Apple) offering “giveaways” or warning accounts (company, bank) are being comprised.³ “Free Gift Cards” in exchange for information is another tactic.⁴ **Treat these emails with caution. Do not click any strange links or websites as they can contain malware. Look for clues that the emails are fake: spelling mistakes, grammar, formatting errors.**⁵

Gift Card Scams: These come in several forms. Scammers will instruct victims to purchase cards then send them the serial number and PIN on the back. Scammers will also scratch the film strip off the back to get the PIN; cover it with a replacement sticker; then, wait for a victim to load it. Scammers can also steal the value remotely by using malicious software. **It is recommended when purchasing gift cards to avoid the kiosks and purchase one from behind a counter or online from a legitimate store (i.e. Target Gift Card from target.com).**⁶

Text Message Scams

Delivery Scams: Fraudsters will send phishing texts warning customers that a delivery could not be completed and to follow a link or to call a phone number.

Non-Payment or Overpayment Scams: Fraudsters will send phishing texts claiming that your account has been locked due to non-payment and provide a link to update payment information. Scammers may also send an “overpayment” message with a link to receive a refund.⁷

Like phishing emails, these text messages should be treated with caution. No links should be clicked. Delivery companies (FedEx, UPS, USPS, Amazon) will never ask for social security numbers or credit card numbers for delivery purposes.⁸

DO NOT click on any provided link and contact the company directly, if you have any concerns about payment.

You've missed our delivery, for the redelivery of your parcel please visit: <https://myparcel-ups.com> and confirm the settlement of (1.45).

¹ <https://www.seattletimes.com/nation-world/as-youre-shopping-this-season-beware-of-these-holiday-scams/>

² <https://www.bbb.org/all/holiday-hq/scams/12-scams-of-christmas>

³ <https://www.trufcu.com/learn/financial-wellness/blog/blog/2024/11/14/scams-to-watch-out-for-this-holiday-season>

⁴ <https://www.bbb.org/all/holiday-hq/scams/12-scams-of-christmas>

⁵ <https://www.trufcu.com/learn/financial-wellness/blog/blog/2024/11/14/scams-to-watch-out-for-this-holiday-season>

⁶ <https://www.aarp.org/money/scams-fraud/info-2019/gift-card.html>

⁷ <https://www.firstbank.com/resources/learning-center/10-text-message-scams-you-didnt-know-about-until-now/>

⁸ <https://www.trufcu.com/learn/financial-wellness/blog/blog/2024/11/14/scams-to-watch-out-for-this-holiday-season>

Grandparent Scams: Uncorroborated information suggests that grandparent scams increase during the holiday season. Scammers will text, email, or call elders impersonating a family member in trouble or claiming to represent said family member in trouble (i.e. lawyer). These scammers will then demand money, via gift cards, wire transfers, cryptocurrency or gold bars. Scammers instruct victims not to tell anyone and try to create a sense of urgency and fear. **Victims are advised to hang up immediately and reach out to family members before taking any other action to verify information being provided.**⁹¹⁰

Temporary Holiday Jobs: The BBB warns “the number one riskiest scam for people ages 18-44 in 2023,” was temporary holiday jobs. Scammers will advertise online temporary positions for holiday work by impersonating legitimate companies. **Employers will never ask for payment for supplies, applications or training fees. Job seekers should be caution of big money for these positions and are advised to never work for a company before being hired.**¹¹¹²

Charity Scams: Scammers will use familiar sounding names or impersonate reputable charities. **Those looking to donate to charities this season should first verify the organization by using: Better Business Bureau’s Wise Giving Alliance, Charity Navigator, Charity Watch or Guide Star. Individuals can also utilize the Smart Donor Checklist to ask questions about the charity in question.**¹³

Example of a Family Emergency Scam Call

Hi Grandpa, it's me.

Sebastian? Is that you?

Yes, it's me, Sebastian. Grandpa, I'm in trouble, and I need money for bail.

What happened?

Please don't tell Mom or Dad, I'll get in so much trouble. Please help me!



Search the charity name online. Do people say it's a scam?



Watch for names that only look like well-known charities.



Look up a charity's report and ratings:

- give.org
- charitywatch.org
- candid.org
- charitvnaviaator.org

Resources & Reporting

If you have paid scammers, there are some actions you can take to protect yourself from further issues and potentially get money back. Follow the QR Code for “What to Do if You were Scammed” for steps to take.

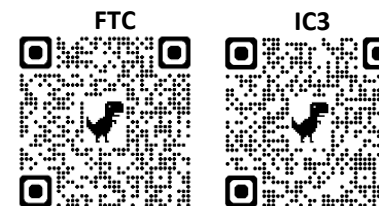
Victims are encouraged to file a police report with their local area station. Please follow the QR Code below to find your local Boston area station.



If the scammers obtained your Social Security number, go to IdentityTheft.gov with the below QR Code.



For additional reporting victims can also file with the **Federal Trade Commission (FTC)** or with the **FBI’s Internet Crime Complaint Center (IC3)**, by following the below QR codes.



What to Do if You Were Scammed



⁹ <https://www.trufcu.com/learn/financial-wellness/blog/blog/2024/11/14/scams-to-watch-out-for-this-holiday-season>

¹⁰ <https://ncdoj.gov/protecting-consumers/holiday-scams/>

¹¹ <https://www.bbb.org/all/holiday-hq/scams/12-scams-of-christmas>

¹² <https://www.bbb.org/article/news-releases/14438-bbb-tips-for-avoiding-job-scams-this-holiday-season>

¹³ <https://ncdoj.gov/protecting-consumers/holiday-scams/>