Keep Your Holidays Happy

It's the most wonderful time of the year...
...for scammers

Office of Information Technology
Division of Information Security
DECEMBER 2022

According to a new report by the American Association of Retired Persons (AARP), three-quarters of U.S. consumers have experienced or been targeted by at least one form of fraud that can be tied to the holidays. Most of these scams are variations on everyday fraud, ramped up to match seasonal spikes in spending and web traffic. Note that if you are the victim of a scam, you should report it to the Federal Trade Commission (FTC).

- **Non-payment scam:** These scams contact targets claiming that they are in default of a payment from a corporation, utility, or government agency and demand immediate payment. If you receive such a demand, verify the claim by contacting the creditor directly using their official contact information.

- **Non-delivery scam:** A buyer pays for goods or services they find online, but never receive the items they've ordered. If you receive a call, email, or text claiming that a package couldn't be delivered, go to the vendor's web site directly or call their published help line. Never click on a link to respond to these messages and don't use the information in the message to contact the sender.

- **Package delivery scam:** Similar to non-delivery scams, package delivery scams occur when scammers send phishing emails and texts disguised as notifications about missed deliveries or undeliverable packages for items you never ordered. These emails claim to be from legitimate shipping entities like UPS, FedEx, or the U.S. Postal Service; however, links lead to phony sign-in pages asking for personal information, or to sites infested with malware. Like any other email or text, never click on a link unless you are absolutely sure where it leads. Hover over it without clicking to see where it goes. As with the scams mentioned above, your best bet is to contact the shipping company directly using their official contact information.

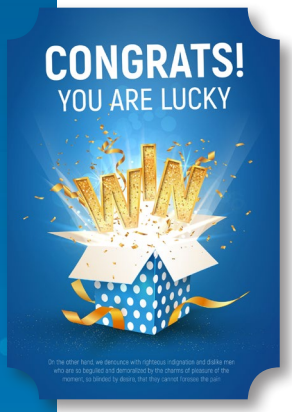
- **Gift card scam:** There are actually two types of these scams. The most prevalent is entities claiming to be a government agency or legitimate business using threats to try to get you to pay fake charges using gift cards. They will usually indicate what type of card they want you to use (for example Amazon or eBay). Many will ask you to purchase these while they are still on the line. Remember that a legitimate business or government agency will never ask you to pay for anything using gift cards. Anyone who does is likely to be a fraud. The second type of gift card scam is selling "discounted" gift cards that actually have no value loaded or have their codes and pins recorded so that scammers can drain the cards upon activation. The FTC has additional information on various gift card scams and how to avoid them, buy gift cards only from the companies they are for, preferably directly from those companies. If buying a gift card from a brick-and-mortar retailer, be sure that it is sealed in a tamper-proof package.

- **Gift exchange scam:** Prevalent on social media sites, these scams claim to be "Secret Santa" style gift exchanges. They may include schemes that promise if you send presents or money to an address, you'll get money from multiple people in return. These are not only fake, but if they weren't, they'd be illegal pyramid schemes. Your safest course of action is to never participate in a gift exchange with people you don't know personally.

- **Social media shopping scam:** These may appear as contests or deeply-discounted goods, including gift cards and vouchers, and may appear to have been shared by friends or family. In reality, these offers generally offer cheap knock-offs of the goods in photos they've stolen from legitimate sources or provide no goods at all, just serving as a means to collect your credit card or bank information. You can always search online for company reviews and scam reports. Remember, if a deal sounds too good to be true, it probably is. You'll save more money in the long run by limiting yourself to legitimate companies.

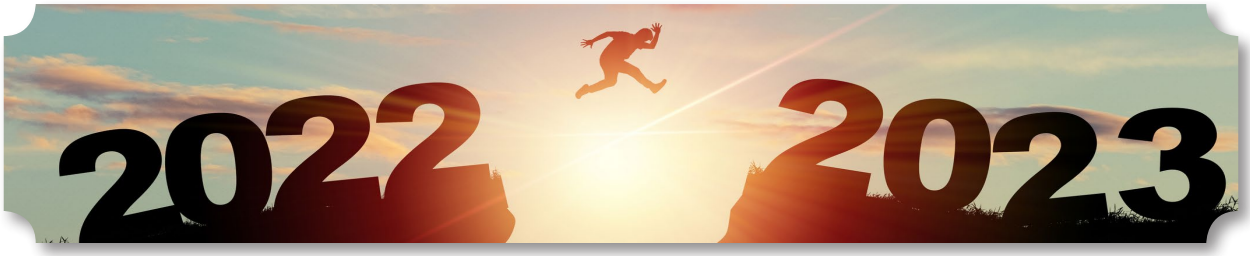
- **Charity scam:** Frequently increasing at holiday times, in hopes of exploiting people's holiday goodwill, charity scams may include phone calls, texts, or emails soliciting donations to fake charities, fake sites spoofing real charities, or even personal appeals from malicious actors posing as trusted religious leaders. If you receive an email that appears to be from a charity or from your spiritual leader, verify that the purported sender actually sent the request before providing any money or information.

- **Job opportunity scam:** Malicious actors may advertise jobs using the same methods any legitimate business would; however, the jobs being offered may be either non-existent or illegal. Any job that asks you to provide personal information, especially bank information or your social security number, pay to be hired, or pay for materials or special certifications before you start is likely to be fraudulent. Any job that sends you a check and asks you to cash it then forward part of the money is definitely not legitimate. If you do as they ask, you may be liable for the entire amount of the fake check. The FTC provides examples of common job opportunity scams and how to avoid them.



- **Travel scam:** Some criminals send scam emails and texts offering promotions such as free travel or greatly discounted vacation packages. These scams frequently use spoofed web sites pretending to be legitimate hotels, airlines, home-rental sites, and other travel-related businesses to get you to hand over your credit card or bank account information or to click on links that download malware. Some of these web sites will let you book vacations, including flights and lodging, only for you to arrive and find that the legitimate vendor has no record of your purchase.

Don't think that you're safe once the new year starts. Malicious actors just change their bait. Typical scams target annual resolutions like weight loss products and financial counseling. Use caution when responding to emails and texts and when making online purchases.



The IHS OIT Division of Information Security wishes you a happy, healthy, and safe holiday season and a joyous 2023. If you have any questions about this newsletter, please email Cybersecurity@ihs.gov.