



Safety Tips

From the Mountlake Terrace Community Policing Advisory Board

Top 5 Holiday Season Scams

As the Holiday shopping season shifts into high gear, take time to think carefully before making charitable donations and purchases. Although scammers are always prowling for victims with scams, consumers are especially vulnerable during the holidays. With so much to do, many otherwise cautious people let their guard down. Con artists are ready to exploit busy, distracted shoppers -- some desperate to buy popular gift items. They're also ready to "ramp up" their emotional appeals when posing as representatives of real (or real-sounding) charities.

We believe the following **5 Holiday Scams will dominate the 2011 Holiday season**. However, if you use common sense and take our advice, the Grinch won't have a chance of stealing YOUR Holiday.

Fly-By-Night Web Merchants. Each holiday season features THE gift -- an item so "hot" that many store shelves are quickly emptied, causing people to literally lose their minds in an effort to buy it. To exploit scarcity, scammers set up websites offering this product, as do dishonest online auction sellers. After raking in the money, the scammers shut down their "stores" and disappear. If you're "lucky," you are simply left with no gift item. If you're unlucky, you are further victimized by a credit card fraud. **Safety Tip:** Protect yourself by buying from reputable merchants -- and read the next scam.

Phishing Scam, run by someone who will use your credit card information to charge more products and services to your account and/or sell the information to identity thieves. In most cases, however, phishing scammers launch websites that look nearly identical to those of larger, reputable merchants -- not unknown companies. Typically, you're contacted by email with a tempting offer or dire warning, and then directed to click on a link, which takes you to a fake website. Once there, you're told to enter personal and financial information wanted by the thieves.

Safety Tips: To avoid falling prey to either Christmas scam #1 or #2: Shop only with reputable merchants, preferably ones you've used before and confirm that the website actually BELONGS to that merchant. Don't click on links in unsolicited emails. Type in the website yourself. Use a credit card, not your debit card. Even if you never get the merchandise, credit cards aren't directly linked to your bank account, and you're also not responsible for more than \$50 in fraudulent charges. If possible, use one-time use credit card numbers, called "controlled payment numbers" or "virtual account numbers," for your online purchases.

Charity Scams. Scammers may pose as representatives of charitable organizations that are real (or merely sound real). At this time of year, their emotionally-charged appeals are more likely to strike "pay dirt" with normally savvy people. The scams may involve nationally recognized charities aiding well-known causes, or local groups handling problems closer to home.

Safety Tips: Whether you're approached by email, telephone or in person, be VERY wary of high-pressure, donate NOW pitches. Avoid "charities" whose representatives won't answer reasonable questions, such as how the money will be spent. And NEVER give cash or supply credit card information via email or phone. Don't write checks payable to an individual solicitor. If you've never heard of an organization, confirm for yourself that it's real.

Gift Card Scams. Nearly every major retailer offers gift cards, many of which hang on racks at checkout counters. Today, most cards are protected by scratch-off security codes and protective packaging to prevent information theft. If cards are not protected, however, scammers can write down the numbers while the cards are on display, and then call an 800 number to learn when the cards have been activated. After that, stealing is as simple as rushing to the merchant and making purchases before the REAL cardholder gets there.

Safety Tips: Purchase gift cards online, if possible. Or, only buy the cards from retailers when they're kept behind registers or available upon request.

Holiday E-Card Scams. You may receive an email from an unnamed "relative," "neighbor," or "friend" who has supposedly sent you an e-card that can be viewed by clicking on a link. Clicking on that link, however, may unleash anything from spyware and pop-up ads to viruses and "Trojan Horses" In some cases, nothing bad happens until you first download software from the e-card website. (The software is supposedly needed to "run" your e-card.) Sometimes, unwanted or malicious software is downloaded to your computer with your permission -- after you agree to certain "fine-print" terms and conditions, usually without reading them.

Safety Tips: If there's any doubt about an e-card's authenticity, don't click on any links inside. Delete e-cards from people you don't know without opening or reading them, and never click to accept terms from any company without actually reading the fine print. Most important, install antivirus and anti-spyware software and keep it up to date.

When it comes to any type of scam -- at any time of year -- we suggest you **trust your instincts**. If something doesn't feel right, do more homework or buy from another vendor. Here's hoping you have a happy and scam-free Holiday season!

Safety Tips is an ongoing, public safety and awareness program presented by the Mountlake Terrace Community Policing Advisory Board and the city of Mountlake Terrace.