YORKVILLE POLICE DEPARTMENT
NEIGHBORHOOD WATCH NEWSLETTER
December 2010

Sweepstakes & Lotteries Scams

"Congratulations, it's your lucky day! You've just won $5,000!"

If you get a phone call or a letter with a message like this, be skeptical. Scam artists often use the promise of a valuable prize or award to entice consumers to send money, buy overpriced products or services, or contribute to bogus charities. People who fall for their ploys may end up paying more and more for the products — if they ever get them at all.

How to Avoid Prize and Sweepstakes Fraud

The next time you get a "personal" telephone call or letter telling you "it's your lucky day," remember:

- Don't pay to collect sweepstakes winnings. If you have to pay to collect your winnings, you're not winning — you're buying. Legitimate sweepstakes don't require you to pay "insurance," "taxes", or "shipping and handling charges" to collect your prize.
- Hold on to your money. Scammers pressure people to wire money through commercial money transfer companies because wiring money is the same as sending cash. When the money's gone, there's very little chance of recovery. Likewise, resist any push to send a check or money order by overnight delivery or courier. Con artists recommend these services so they can get to your money before you realize you've been cheated.
- Phone numbers can deceive. Some con artists use Internet technology to call you. It allows them to disguise their area code: although it may look like they're calling from your local area, they could be calling from anywhere in the world.

How to Recognize a Reloader

- Their offer requires a "recovery fee." Legitimate organizations, like national, state, and local consumer enforcement agencies and non-profit organizations, do not charge or guarantee results for their services to help you get your money back from a telemarketing fraud.
- Their offer requires you to wire money or send it by a courier. They contact you several times to urge you to buy more merchandise to increase your chances of winning so-called valuable prizes.

Fake Check Scams

"It's your lucky day! You just won a foreign lottery! The caller says so. And they are sending a cashier's check to cover the taxes and fees. All you have to do to get your winnings is deposit the check and wire the money to the sender to pay the taxes and fees. You're guaranteed that when they get your payment, you'll get your prize."

There's just one catch: this is a scam. The check is no good, even though it appears to be a legitimate cashier's check. The lottery angle is a trick to get you to wire money to someone you don't know. If you were to deposit the check and wire the money, your bank would soon learn that the check was a fake. And you would be out the money: The money you wired can't be recovered, and you're responsible for the checks you deposit - even though you don't know they're fake.

International Lottery Scams

"Congratulations! You may receive a certified check for up to $400,000 U.S. CASH! Tax free! Your odds to WIN are 1-6." "Hundreds of U.S. citizens win every week using our secret system! You can win as much as you want!"

Sound great? It's a fraud. Scam operators — often based in Canada — are using the telephone to entice U.S. consumers to buy chances in high-stakes foreign lotteries from as far away as Australia and Europe. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

(Courtesy of www.ftc.gov)

Top 5 Christmas Season Scams

1) 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.

2) Phishing Scam

These are 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.
- Confirm that the website actually BELONGS to that merchant. Don't click on links in unsolicited emails. Type in the URL 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.

3) 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. We recently reported a new email phishing scam that's soliciting donations to help victims of the California wildfires. You can be sure that other scams will soon be asking for donations to this cause and many others. 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 (specifically) 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.

4) 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.

5) 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 Trojans. 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 Christmas season!

(Courtesy of www.scambusters.org)