Tips for Avoiding Common Holiday Cyberscams

For many of us, the holiday season is a wonderful time of year. Unfortunately, it can be especially profitable for cybercriminals. Because of the prevalence of online shopping, we almost always see a significant increase in cyberscams during November and December. To help you avoid becoming a victim of holiday cybercrime, here are some of the top scams to watch out for—and tips for avoiding them.

Shady Shipping Notices
During the holiday season, it's very likely that you will ship at least a couple of packages directly to your loved ones or have online purchases sent to your home. This makes the shipping notice scam a popular one for cyberscrooges. Here's how it works: The scammer crafts an email, purportedly coming from UPS or FedEx, notifying you of a problem delivering your package. To resolve the issue, you need only click on a link in the email message or open an attached invoice. Of course, doing so will install malware or ransomware on your computer or device.

Don't fall for it. Be particularly wary of emails claiming to come from any courier service. If you do receive a message like the one described above—whether you believe it to be legitimate or not—go to the website of the company you may have ordered from. You should be able to track your package from the retailer's site. Use the tracking number for the courier service that the retailer provides. You can also go directly to UPS.com or FedEx.com and obtain the delivery status there. Whatever you do, don't click on any links or download any attachments in the original message.

Eyebrow-Raising Refunds

This phishing scam is designed to steal your personal and financial information. Typically, an email claiming to be from an e-commerce company like Amazon, eBay, or Overstock will say that something has gone wrong with your recent order. You will be prompted to click on a link in the message to obtain your refund. Unfortunately, if you do, you will be taken to a dummy website set up to look like a legitimate sender. There, you will be asked to fill out a form with your financial information to let the sender know where it can issue your refund.

Don’t fall for it. Again, to check the status of any order you may have placed, go to the company’s website directly (e.g., Amazon.com, eBay.com). If the company doesn’t offer the ability to check an order’s status, verify the transaction by calling the firm at a phone number that you know is legitimate.

Giveaways Galore

The gift card scam is seen year-round but more often during the holidays. These bogus offers are most commonly delivered by cybercriminals through social media, usually through a friend’s hacked account or a fake company page set up to look as if it’s legitimate. Appearing to originate from an entity like Best Buy, Ikea, or Whole Foods, the offer claims that the company is giving away hundreds or thousands of dollars in gift cards. But if you follow the instructions provided to obtain your gift card, you will likely be led to a phishing form that asks for your personal information.

Don’t fall for it. Remember, if something seems too good to be true, it probably is! If the post appears to come from a friend, call or text him or her to ask if it’s legitimate. In addition, be wary if the “official company page” looks a little off. Check how many followers the website has. The retailer’s authentic website may have hundreds of thousands or millions of followers. Further, a huge promotion such as the one described in the offer

you received would also be listed on the retailer's website, so check there directly or call the company's customer service number.

Website Vendors That Don't Deliver

Many popular and novelty items may be sold out and on backorder until after the holidays. Or they may be hard to find from mainstream merchants altogether. So it's not uncommon for consumers to search online for a less well-known vendor that may have the items. But beware! Another favorite holiday scam is staged through sketchy websites claiming to have hard-to-find items in stock. These sites trick you into paying for the items with no intention of delivering them. Often, these entities are based overseas.

Don't fall for it. Search the Better Business Bureau website for customer reviews and the accreditations of merchants that are unfamiliar to you. In addition, because not all businesses are listed with the BBB, you might want to hunt elsewhere on the web for reviews posted by other consumers. If you can't find much information on the vendor, stay away!

Still nervous? Below are additional tips to protect yourself from holiday scams:

• If possible, use credit cards for online transactions. If you fall for one of these scams and unknowingly hand over your debit card information, it's easy for the cybercriminal to drain your bank account quickly. Purchases made with credit cards typically offer more consumer protections.
• If you're uncertain about the legitimacy of a website, check its safety rating on Scamadviser.com or URLVoid.com.
• If searching for an item on a lesser-known merchant's website, check for spelling and grammatical errors. If found, these mistakes are a red flag that the site is most likely based

overseas—indicating a possible scam.
• Avoid online shopping or conducting any financial transactions over an unsecure Wi-Fi network.

'Tis the Season
With all the merriment and shopping during the holidays, the risk of inadvertently exposing your credit card or bank account details is very real. It's important to take a step back and pay attention to the emails you're receiving and the websites you're using. By following the suggestions discussed here, you can help protect yourself against cyberscams so you can fully enjoy the holiday season.

Karen Reed Earns CPIA Designation

Karen Reed,
CRIS, CPIA

Karen Reed, a member of our business insurance team, recently earned the designation of Certified Professional Insurance Agent (CPIA), a professional designation conferred by the American Insurance Marketing and Sales Society (the AIMS Society).
The CPIA designation, received after completion of three in-depth seminars, stands for professionalism, commitment to sales training and results, and technical knowledge. The designation requires a bi-annual continuing education update.
Reed, of Appleton, has been with Allen Insurance and Financial

for 25 years and specializes in insurance for contractors and large businesses. She is also certified as a Construction Risk and Insurance Specialist (CRIS), and is a member of the Maine Association of Building Efficiency Professionals.

The AIMS Society is the only insurance organization dedicated solely to recognizing training and service quality among property and casualty insurance personnel. The mission of the AIMS Society is to improve the selling skills and insurance knowledge of its members by upgrading professionalism through information and education, which will result in providing better service to the insurance-buying public.