Better Business Bureau®
Start With Trust℠
in Wisconsin

The Consumer Newsletter

December 2010

'Tis the Season for Holiday Scams

The holidays are a happy time for food, family, and friendship, but they are also a time for fraud.

Consumers can fall into any number of traps over the holidays and become victim to identity thieves, hackers and deceptive merchants online. The Better Business Bureau is warning holiday shoppers and donors to look out for five common scams this season.

Scam shopping sites online

We're all looking for a great deal online, but some sites offer electronics or luxury goods at prices that are too good to be true. Every holiday season, BBB hears from holiday shoppers who paid for a supposedly great deal online, but received nothing in return.

BBB advice: Always look for the BBB seal when shopping online and click on the seal to confirm it is legitimate. When shopping on sites that aren't household names, check the business out with the BBB before you buy.

Finding the season's hottest toys and gadgets online

Every year, holiday shoppers fight over the "must have" toy or gadget of the season. When the item is sold out in stores, you can often find it online through sites like Craigslist or eBay—for a much steeper price. The problem is that some sellers will take your money and run.

BBB advice: Shop locally on Craigslist and conduct the transaction in person—never wire money as payment. When purchasing items on auctions like eBay, research the seller extensively and always listen to your doubts if the deal doesn't sound legit.

Identity theft at the mall

While you're struggling at the mall with bags of presents, identity thieves see an opportunity to steal your wallet and debit or credit card numbers.

BBB advice: Don't let yourself get bogged down in purchases and lose track of your wallet. Know where your credit and debit cards are at all times and cover the keypad when entering your pin number while purchasing items or getting money from the ATM.

Bogus charitable pleas

The holidays are a time of giving, which creates a great opportunity for scammers to solicit donations to line their own pockets. Also beware of solicitations from charities that don't necessarily deliver on their promises or are ill-equipped to carry through on their plans.

BBB advice: Always research a charity with the BBB Wise Giving Alliance before you give to see if the charity meets the 20 Standards for Charity Accountability.

Phishing e-mails

Phishing e-mails are a common way for hackers to get at your personal information or break into your computer. Common phishing e-mails around the holidays include e-cards and messages pretending to be from companies like UPS or Fedex with links to package tracking information.

BBB advice: Don't click on any links or open any attachments to e-mails until you have confirmed that they are not malicious. E-mail addresses that don't match up, typos and grammatical mistakes are common red flags of a malicious phishing e-mail. Also beware of unsolicited e-mails from companies with which you have no association. Make sure you have current antivirus software and that all security patches have been installed on the computer.

Traveling over the holidays? Beware of "Free Wi-Fi" scams, especially at airports

Many airports and other public spaces offer free wireless, or Wi-Fi, connections for the public to log onto the Internet from their laptop computers. However, hackers are taking advantage of those who want to stay connected by setting up fake Wi-Fi connections designed to steal your personal information.

Here's how it works:

When searching for connections, consumers may see a network connection available that could be simply named "Free Wi-Fi." Unfortunately, the network may actually be an ad-hoc network, or a peer-to-peer connection. The user will be able to surf the Internet, but they are doing it through the hacker's computer. While the user is online, the hacker is stealing information like passwords, credit card and bank account numbers, and social security numbers from the user's laptop computers. Airports across the nation continue to report Wi-Fi security issues.

The BBB offers the following advice for travelers using Wi-Fi Hot Spots:

- **Connect securely.** Never connect to an unfamiliar wireless network—even if the name sounds genuine. A hacker can change the name of his network to anything he wants, including the name of the legitimate Internet connection offered by the airport.
- **Disable automatic connections.** Make sure that your computer is not set up to automatically connect to any wireless networks within your range. Otherwise, your computer could automatically connect to the hacker's network without your knowledge.
- **Turn off file sharing** when you are on the road to prevent hackers from stealing sensitive data from your computer.
- **Create a Virtual Private Network (VPN).** A VPN establishes a private network across the public network which prevents a hacker from intercepting your data.

Beware of Rose Bowl ticket scams

If tickets to see the Wisconsin Badgers in the Rose Bowl are on your holiday wish list, the Wisconsin BBB wants you to be careful when purchasing tickets or travel packages.

Scams are common, especially in the form of counterfeit tickets, either from online sites like Craigslist and eBay, or from ticket scalpers and online agencies that do not deliver.

Rose Bowl ticket scammers have a history with Wisconsin games. In 1994, nearly 10,000 Badger fans made the long journey to California after purchasing a ticket package, only to discover that they had been scammed and did not have legitimate tickets to the game. Before boarding the plane, the BBB recommends having your ticket for the game in hand to prevent a similar situation.

The BBB offers these tips to make sure you do not get scammed:

- Always use a credit card or PayPal for online purchases, so that charges can be disputed. Ask for a picture of the ticket, verify it using the venue's seating chart, and get a receipt.
- Never leave the website to finish a transaction; you will lose protection a website like eBay provides.
- Try to buy from someone who is local and has a good history of satisfying customers. Check other consumers' feedback before purchasing tickets from the seller.
- Get the seller's real name and contact information.
- Never go alone to pick up tickets purchased from someone online, and always meet in a public place. The "seller" knows when and where you're going to be, and that you're carrying a lot of cash. He/she may be setting you up to get robbed.
- Only buy from people or ticket brokers that you trust. Look for a BBB logo to select a ticket broker that is accredited by the BBB, or find one at www.bbb.org.

Protect yourself from “electronic pickpocketing” using Radio Frequency Identification (RFID) technology

Until now, you thought that if your credit card was safely tucked into your wallet, it was safe from identity thieves. Unfortunately, new technology - which was developed to make credit card and other transactions quicker -- is being misused by scammers to swipe the data from your card without ever touching you.

It’s dubbed “electronic pickpocketing”, and the theft occurs when the scammer has an RFID (radio frequency identification) scanner, a device available on the internet. He simply needs to pass by you for the scanner to read your credit card number, passport information or smart card data.

RFID is commonly used as anti-shoplifting technology, security entrance cards, to allow automatic checkout at libraries and scanning of passports. Large RFID scanners can be found surrounding exits of stores and libraries.

The Wisconsin Better Business Bureau says consumers can easily protect their information from RFID scanners by purchasing a special wallet or with a simple do-it-yourself method:

- Cut two pieces of cardboard the size of a credit card, and wrap each dummy card with foil. Place one of the foil cards on each side of the wallet to shield credit cards from RFID scanning.
- RFID scanners also can penetrate a wallet head-on. Keep all cards with smart chips next to each other between the foil cards to make them more difficult to read.
- As privacy advocates express concern about growing use of RFID and its vulnerabilities, manufacturers are working on ways to limit their transmission range.

Whether giving or receiving, you’ll want to check out this BBB advice on returning

Although we all know it’s the thought that counts, sometimes a gift is either the wrong size, wrong color...or just wrong, period. You think you can automatically exchange it, right? Think again!

Actually, no Wisconsin law regulates returns or refunds. So, unless the item is defective or misrepresented, it’s up to the individual retailer to set its own return/refund policy. To ensure a pleasant experience at the return counter for you or the recipient of your gift, heed this advice from the Wisconsin BBB:

- Before buying, ask: Is the sale final? May I exchange it? How long after the purchase can I return it? Can I return for money or in-store credit? Can I have a gift receipt? Is there a restocking fee?
- Before buying, always inspect merchandise closely at the store.
- Keep all of the following: Original packaging, receipt and a copy of the store’s return policy.
- When receiving a refund, check to see that the return price matches the paid price.
- Don’t assume the regular return policy applies to sale or clearance items. Some merchants consider clearance items to be final, so ask.
- When shopping online, look for - and print - a return policy BEFORE you check out.

Find the Wisconsin BBB online: www.wisconsin.bbb.org

www.twitter.com/WisconsinBBB

www.facebook.com/WisconsinBBB

www.youtube.com/WisconsinBBB