



Chester Academy Technology Newsletter

Winter 2009-2010

Ah, the holidays—that most wonderful time of year when the Web is aflutter with e-mailed season's greetings, online shopping offers...and cyber criminals. The scams run the gamut, from fraudulent e-mails purporting to be alerts about online transactions to scam gift card offers.

Cybercriminals know it's easier to get people to fall for scams related to online shopping when they have shopping on the brain. People are particularly vulnerable this time of year because they are looking for bargains. It also doesn't hurt that the legitimate act of online shopping often involves visits to comparison-shopping sites and strange discount sites. So it's little surprise that some of those destinations turn out to be fake.

The rising popularity of online shopping makes for a target-rich environment. According to the *Better Business Bureau, Last year consumers spent about \$25 billion online by Dec. 1st. That's a 19% increase from the year before.

*(www.bbb.org)

So what can consumers do to protect themselves from unwittingly buying someone else's holiday gifts this season? For starters, they can keep an eye out for the following common holiday scams:

Cybercriminals prey on online shoppers over the holidays. Here are the most common scams and how you can avoid them

Tis the Season for...

1. *Fraudulent e-Mails*
2. *Charity Scams*
3. *Gift Card Scams*
4. *Job Scams*
5. *Gifts for Geeks*



1. *Fraudulent (phishing) e-mails or links*

www.microsoft.com/protect/fraud/phishing/symptoms.aspx

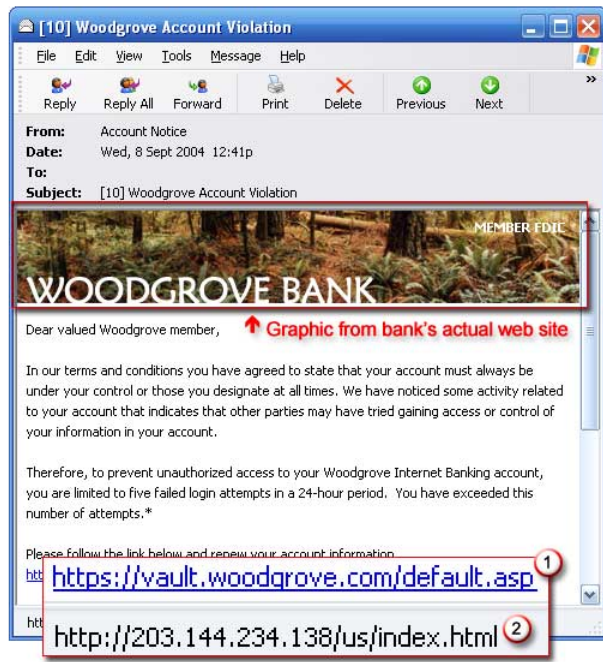
Phishing e-mail messages are designed to steal your identity. They ask for personal data, or direct you to Web sites or phone numbers to call where they ask you to provide personal data.

Phishing e-mail messages take a number of forms:

- They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking site.
- They might appear to be from someone you know. *Spear phishing* is a targeted form of phishing in which an e-mail message might look like it comes from your employer, or from a colleague who might send an e-mail message to everyone in the company, such as the head of human resources or IT.
- They might ask you to make a phone call. *Phone phishing* scams direct you to call a customer support phone number. A person or an audio response unit waits to take your account number, personal identification number, password, or other valuable personal data. The phone phisher might claim that your account will be closed or other problems could occur if you don't respond.
- They might include official-looking logos and other identifying information taken directly from legitimate Web sites, and they might include convincing details about your personal information that scammers found on your social networking pages.

They might include links to spoofed Web sites where you are asked to enter personal information.

Here is an example of what a phishing scam in an e-mail message might look like.



Example of a phishing e-mail message, which includes a deceptive Web address that links to a scam Web site.

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site.

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

"Verify your account."

Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.

"You have won the lottery."

The lottery scam is a common phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work on your part. The lottery scam often includes references to big companies, such as Microsoft. There is no Microsoft lottery.

"If you don't respond within 48 hours, your account will be closed."

These messages convey a sense of urgency so that you'll respond immediately without thinking. A phishing e-mail message might even claim that your response is required because your account might have been compromised.

What does a phishing link look like?

Sometimes phishing e-mails direct you to spoofed web sites. Here's an example of the kind of phrase you might see in an e-mail message that directs you to a phishing Web site:

"Click the link below to gain access to your account."

HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site.

Phishing links that you are urged to click in e-mail messages, on Web sites, or even in instant messages may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate Web site.

Notice in the following example that resting (but not clicking) the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.



Example of a masked Web address

Con artists also use Web addresses that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the address "**www.microsoft.com**" could appear instead as:

www.micosoft.com

www.mircosoft.com

www.verify-microsoft.com

This is called "typo-squatting" or "cybersquatting."



2. Charity Scams

www.irs.gov, www.fbi.gov, www.bbb.org, www.ftc.gov

You'd think that con artists would be least likely to strike following a major tragedy. Not so. And they're more likely to con you at this time of year, when they know you're in a giving mood -- and perhaps thinking of year-end tax deductions. The holidays are a time for giving, but not for giving unwisely.

Shortly after Hurricane Katrina slammed into the Gulf Coast, a website sprang up asking for donations for an ex-Air Force pilot who said he'd evacuated local political figures before the storm made landfall and was now airlifting medical supplies and rescuing critical patients with his own money.

It was all a scam. The man wasn't a pilot, and he never delivered any supplies. He was simply pocketing the money collected through his website. Following an FBI investigation, he's now in jail for fraud.

We've seen them (con artists) prey on the rising tide of goodwill and generosity in disaster after disaster—from Hurricane Katrina...to the Asian tsunami, from the Sago mine tragedy...to the London terrorist bombings.

And they're MORE LIKELY to con you at this time of year, when they know you're in a giving mood—and perhaps thinking of year-end tax deductions.

Don't let it happen to you. The holidays are a time for giving, but not for giving unwisely. Jack Liao, a supervisory special agent at FBI Headquarters who specializes in fraud investigations, has some advice to reduce your chances of getting scammed:

- "Our basic rule of thumb is: when in doubt, check it out," says Liao. "Ask a lot of questions and get information in writing if you're not sure about a charity. If you get fuzzy or unsatisfying answers about the charity, its fundraising activities, and the tax-deductibility of donations, think about taking your money elsewhere."
- "Make sure you get the actual name, address, and phone number of the charity before giving. Then check it out by going to the IRS website at www.irs.gov, which has an updated list of legitimate charities and non-profit groups, or by calling the IRS toll-free at (877) 829-5500. Another useful website is www.give.org, part of the Better Business Bureau's Wise Giving Alliance."
- "Don't ever, ever give out personal or financial information to anyone who has contacted you out of the blue. That's just leaving yourself wide open to the theft of your money and your identity."
- "Don't be intimidated into giving. You have the right to say no. If you're really unsure who you're talking with, just tell them you want to do some checking first and ask for a way to contact them later if you decide to give."

Should you exercise due diligence even if there are no major charity drives this holiday season? “Absolutely,” says Liao. “There is more giving during the holidays overall and just about any cause can be exploited. So be crime smart—don’t give unless you’re really sure about who you’re giving to.”

And what if you do get scammed? “Contact the Federal Trade Commission toll-free at (877) FTC-HELP. Also report the fake charity to the state attorney general where you live and/or where the charity is located. By stepping forward, you can help put these scam artists out of business.” *And that’s a holiday gift that keeps on giving.*

3. Gift Card Scams



Gift Card Scams That Pose a Threat This Holiday Season – www.scambusters.org/giftcard.html

With gift card sales estimates at \$24.81 billion this holiday season (up from \$18.48 billion last year according to the NRF), it is not surprising that there are bigger gift card scams going on right now, even if the one on the news is overstated.

According to experts, there are three common types of gift card scams:

1. Used, counterfeit and fraudulent gift cards are being sold on auction websites.
2. Sellers often overstate the value of real gift cards they are selling on auction websites, so buyers don't get what they think they are purchasing.
3. Scammers are using stolen credit cards to buy gift cards and then selling these gift cards for cash, either at online auction sites or elsewhere.

Here are two other current gift card scams:

- Crooks swap blank gift cards that they stole on previous trips to a store for cards activated by clerks when they purchase them. Since the clerks don't realize that the returned cards are blank rather than the ones just purchased, the scammers are able to steal fully charged cards.
- Thieves also carefully open the packaging of new gift cards and replace them with used, worthless cards. When the card is sold, the gift card the scammer has in his possession gets activated, rather than the worthless used card that the real buyer has. (This will only work on some types of cards.)

8 Tips for Protecting Yourself from a Gift Card Scam:

There are plenty of things that you can do to protect yourself from gift card scams. And the best part is that none of these things will take more than a few minutes.

Just follow these eight simple tips to make shopping for gift cards safer:

1. **Don't buy gift cards from online auction sites.** Since this is a large source of gift card fraud, these cheap gift cards may well be worthless to you. Sure, some of these cards are real, but many are stolen, counterfeit or used. It's not worth the risk.
2. **Only buy gift cards directly from the store issuing the gift card or from a secure retailer's website** -- no matter how much cheaper they may be somewhere else. If you do buy a gift card online, make sure you buy it from the place that you plan to use it.
3. **Don't buy gift cards off of publicly displayed racks in retail stores.** In addition, don't assume that because gift cards are inaccessible to the public, they are safe. After all, store employees can participate in gift card scams too.
4. **Always carefully examine both the front and back of a gift card before you buy it.** If you can see a PIN number, put the card back and get a different one. If a gift card looks like it could have been tampered with, don't buy that gift card.

5. **Always ask the store cashier to scan the gift card in front of you.** This will guarantee that your card is valid when you buy it and that it reflects the balance you just charged it with. This will also protect you from crooks who exchange worthless cards for the cards you think you are buying.
6. **Always keep your receipt as a proof of purchase as long as there is money stored on the gift card.** Since many retailers can track where the gift card was purchased, activated and used, if the card is stolen, some retailers will replace the card for you if you have your receipt.
7. **If possible, register your gift card at the store's website.** Although not all stores offer this option, you can uncover any misuse of your gift card sooner and report it more quickly.
8. **Finally, never, ever give your Social Security number, date of birth or any other unneeded private information** when you purchase a gift card. No reputable company will ask for this info.



4. Job Scams

Article on www.ConsumerAffairs.com

College and high school graduations have produced thousands of new people in the labor force, seeking that first job. With a recession and rising unemployment, Pennsylvania Attorney General Tom Corbett is advising new graduates, along with other consumers seeking work, to be wary of Internet job scams.

"It is important for all consumers to be watchful for online job scams, especially young people looking for part-time or summer work," Corbett said. "Falling for these schemes will not only leave you unemployed, but victims can also lose thousands of dollars and find themselves targeted by identity thieves."

Corbett says con artists typically use Internet postings or websites like Craigslist to publish ads that offer high pay for part-time employment, including work as personal assistants, 'mystery shoppers' and check processors.

The exact wording of these scams can vary greatly, but all of the offers have common themes:

- They offer "easy money" for little work.
- Consumers work from home, rather than an office.
- It is difficult to meet your "employer" in-person, often because they travel frequently or are based overseas.
- Consumers need to respond quickly.

Corbett said the most important element in all of these scams is that consumers will eventually be asked to wire-transfer money to another person:

- Personal assistants may be asked to pay bills for the 'employer'.
- Check processors may think they are handling payments for an overseas business.
- 'Mystery Shoppers' may believe they are evaluating stores that deal with wire transfers.

"In reality, victims are depositing counterfeit checks or money orders into their bank accounts and then wire-transferring that money to scam artists overseas," Corbett said. "Eventually, these bogus checks will be returned and banks will require consumers to repay any funds they withdrew."

Corbett said that consumers should always be wary of online job offers that seem "too good to be true," especially any situation where you are being asked to wire-transfer money to someone you do not know.

5. For the Geek who has everything

If you have a resident geek on your shopping list and the usual gifts at Radio Shack, Brookstone, or Best Buy just won't cut it, then try one of the following sites.

Check out the following sites for Geek shopping

www.thinkgeek.com

www.x-tremegeek.com

www.kleargear.com

www.geeks.com

THE CHESTER ACADEMY TECHNOLOGY DEPARTMENT
BILL CAVANAUGH, SHAWN POWER, SUSAN KESSLER,
JOANNE FLANAGAN, AND SUSAN WARNKE

WOULD LIKE TO WISH YOU ALL A

Happy Holiday and Safe New Year

Chester Academy
Technology Department
22 Murphy Dr
Chester, NH. 03036
603-887-8228
WWW.ChesterAcademy.org

