

Happy Holidays!

Burgoyne is dedicated to being *smarter, swifter, and more responsive*. That means you too! We value your business.

We want you to have a better experience in using the internet. As a way of making you *smarter*, Burgoyne is excited to present to you, our valued internet customer, the first in an ongoing series of computer/internet lessons. Lessons can be expensive—just check out a few computer training schools, and you'll see what we mean. But for you, as a Burgoyne customer, they're **absolutely free!** These lessons will come to you monthly, and are specifically designed to be timely, user friendly, and practical, at any level of computer expertise. They will help you to optimize your internet experience. So enjoy and learn!



Christmas Phishing Phrenzy

According to Microsoft, “[p]hishing is the fastest rising online crime method used for stealing personal finances and perpetrating identity theft.” Yet, you may not be aware of what phishing is. This lesson will teach you how to prevent its encroachment into your privacy, especially during this holiday season, when you may be considering online purchases that must be delivered before December 25.

What is Phishing?

Phishing gets its name because highly technical scam artists design emails and web links designed to bait unsuspecting internet users to divulge personal financial information. Since the “phishers” create official-looking emails by using the exact logos, graphics, colors and fonts as the well-known and trusted brand name company, organization, or charity they are trying to duplicate, it can be difficult to detect that the email you are receiving is fake. After this lesson, you’ll be better equipped to prevent being phished.

Red Flag Warning Signs

In most cases, these emails carry a spirit of great *urgency*, and that something bad will happen if you don’t comply. An example is an email from eBay informing you that you need to update your profile, and that if you don’t do it right now, your package will *not* arrive by Christmas. The email will then try to lure you into a link to “update” your credit card or some other vital account information. The phishers desire, of course, is to use such records to embezzle your money and to perform other identity-theft tasks. Millions of people have already fallen prey to phishing.

What Phishers Most Often Want

Online criminals are most likely to desire your:

- Name and username
- Address and phone number
- Password or PIN
- Bank account number
- ATM/debit or credit card number
- Credit card validation code (CVC—this is the three-digit code on the back of your credit card.)
- Social security number (SSN)

(Source: *Microsoft.com*)

How to Avoid being Phished

There are things to look for in order to keep your vital information safe:

- Most reputable companies have policies against asking for vital information through an email. Therefore, you must *never* supply such information if requested by email.
- Most upstanding companies personalize emails to customers; most phishing messages are generic, beginning with phrases such as “Dear Valued Customer.”
- Legitimate URLs should never have the @ sign. Browsers ignore anything before the @. Something as *http://www.amazon.com@nl.tv/protected_verification.aspx* is likely to be unsafe.
- Phishers will often deftly misspell a company’s name. An example would be *http://www.burgoye.com*, instead of *www.burgoyne.com*. Be sure to read carefully.
- According to eWeek.com’s David Coursey, “Nobody needs to verify your password. Ever.” (The whole *eWeek* article is referenced below.)

What to do if You Suspect “Phishy” Activity

The best way to confirm that someone has attempted to lure you into a phishing scam is to contact the company directly, either by phone, or email. (Of course, do *not* use the link on the suspected phishing message to contact the company.) You can ask them if indeed, they need to update your information. If they don’t (and as explained earlier in this lesson, they likely would use another means to contact you if they needed any vital information), then you can report the problem directly to the company.

What to do if You Have Been Phished and Have Suffered Online Identity Theft

If you have indeed been phished and your financial information has been compromised, you need to take the following steps:

- Contact the company that has been “copied.”
- Contact any other online sites that have vital financial information on you.
- Contact your bank(s) and close all compromised accounts.
- File a police report—be persistent in following up.
- Contact the FTC Identity Theft site: (*www.consumer.gov/idtheft/index.html*) and follow all steps as indicated.
- Contact all three major credit bureaus and request a fraud alert be placed on your file.

In Summary

Scam artists are becoming more sophisticated and technologically adept. In short, never give any vital information that is requested through email *for any reason*.

Sites for Further Study

- <http://www.eweek.com/article2/0,1895,1813657,00.asp>
- www.antiphishing.org/
- <http://www.dcfcu.org/phishing/phishingprevention.htm>
- <http://www.bbbonline.org/idtheft/phishing.asp>
- www.privacyrights.org.htm
- <http://www.msnbc.msn.com/id/6679100/>
- <http://msnbc.msn.com/id/6560652/>