My Bowling Diary

Strike out with information… don't spare the details!

June 2005

This newsletter is a first in a series of articles relating to the Internet and internet security. This is prompted by the increase in virus attacks as well as malicious email. If there is a subject that you would like to see covered, please send an email to info@mybowlingdiary.com and put your suggestion in the subject line.

Going fishing is fine. Just don't be "phishing" bait!

(By Timothy A. Sawyer, CISSP)

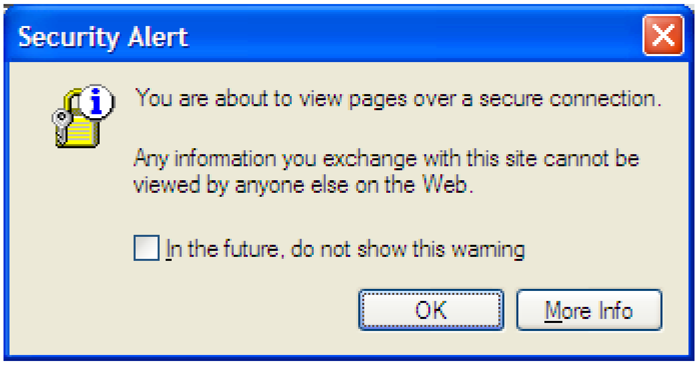
This is a first in a series of articles with regard to safety on the Internet. The articles are designed to give you some advice and tips on how to be safe on the Internet while allowing you to have fun and to conduct your business with a reasonable sense of security. Should you have any questions with regard to the content of the articles, please contact me at tsawyer@mybowlingdiary.com.

Before the explosion of the Internet, we would generally purchase goods and services by going to the business, choosing what we need and then paying a cashier with a check, cash or credit card. You saw the person who took your money, probably exchanged a few words with them and you could be reasonably certain that if you wrote a check or used a credit card that your information was not going to be given away or shared with someone else. I remember that the biggest concern was the customer getting the "carbons" of the credit card slip. You were also certain that you received the goods and/or services that you purchased. But since the explosion of the Internet, we are generally enticed by the "instant gratification" that the Internet provides us, therefore giving traditional storefront operations another avenue to sell products and increase revenue. The Internet is a wonderful tool for transacting business, but there is danger involved. What I want to do is leave you with some advice and tips for protecting yourself and your personal information online in hopes that you don't fall victim to some of the schemes that are out there.

RSA Security, Inc. (www.rsasecurity.com) recently conducted a survey with regard to online shopping... "**One-fourth of online shoppers have reduced their purchases in the past year as concerns over identity theft have risen…"** [http://news.zdnet.com/2100-1009_22-5575569.html?tag=sas.email, 2/14/2005]. Identity theft occurs when someone steals your personal information (i.e. credit card numbers, Social Security numbers, driver's license numbers) and use your identity to perform bogus transactions in your name and basically stick you with the bill, or much worse. Some companies are now coming out with software that will allow you to protect yourself against identity theft. I have not personally seen any of this software so I cannot say one way or the other if any one package works. However, there are steps that you can take TODAY to start protecting yourself, and these steps will not require additional software or money:

1) If you do transact business over the Internet, make sure that when you send personal information that it is transmitted securely. A secure transaction generally means that the information, when sent over the Internet, is encrypted. This will prevent people from reading your information because all they will see is a bunch of gibberish. Since most Internet transactions are done via web browsers (I will use Internet Explorer as an example), here are some tips to see if your transaction is in fact, secure.

   a. First, if you are being redirected to a secure website then you may see the following message:



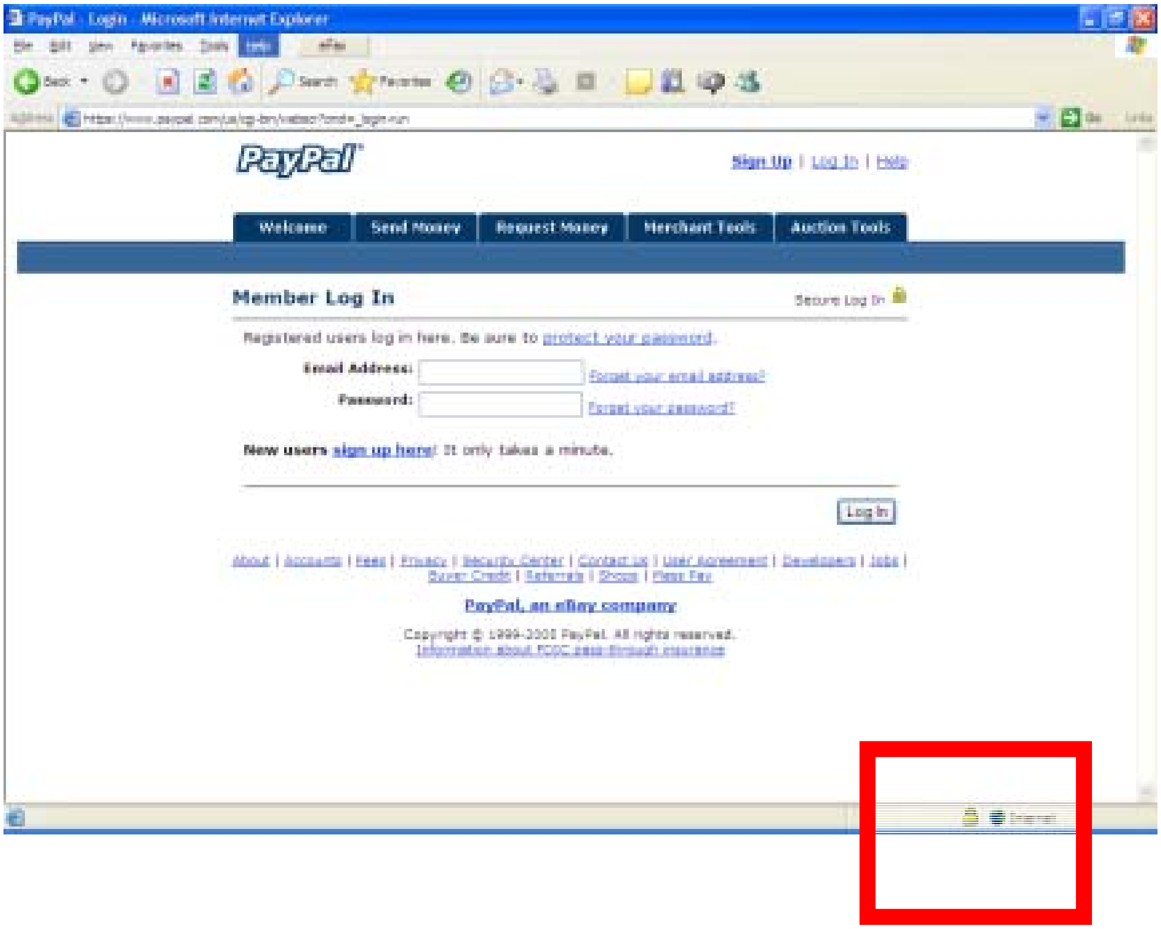
Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

☐ In the future, do not show this warning

b) What this means is that you are about to go to a website that is secure. After you click "OK" then you are redirected to the page:



PayPal - Login - Microsoft Internet Explorer

Member Log In

Registered users log in here. Be sure to protect your password.

Email Address:

Password:

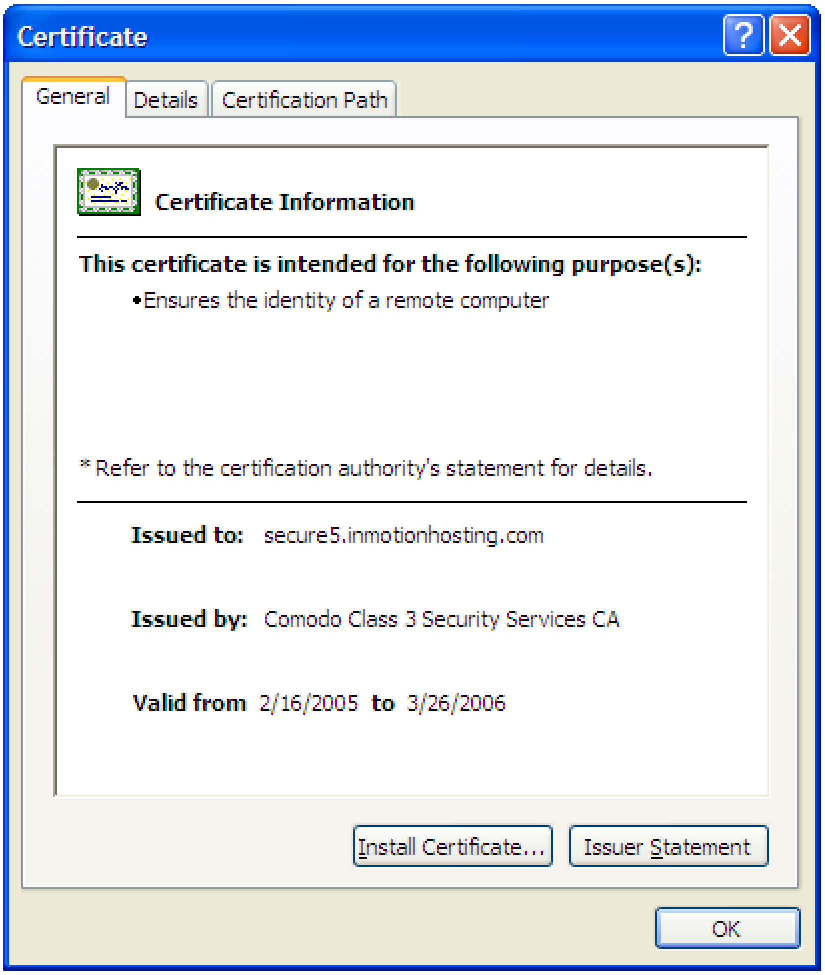
New users sign up here! It only takes a minute.

PayPal, an eBay company

Copyright © 1999-[illegible] PayPal. All rights reserved.

Look in the bottom right corner of your browser. If you see the lock there (outlined in red) this means that anything sent from this page is sent in an encrypted fashion. Now beware! Not all encryption is created equal. What does this mean? I'll try to explain without going into a lot of techno-talk.

When you go to a secure server, that server sends your browser a “digital certificate”. A “digital certificate” is like a server's ‘proof of identity’. The server is letting your browser know that it is actually the site to where you wanted to go to. So how can you be reasonably certain that this certificate is valid? Simply double click on the lock. When you do you will see the following:



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

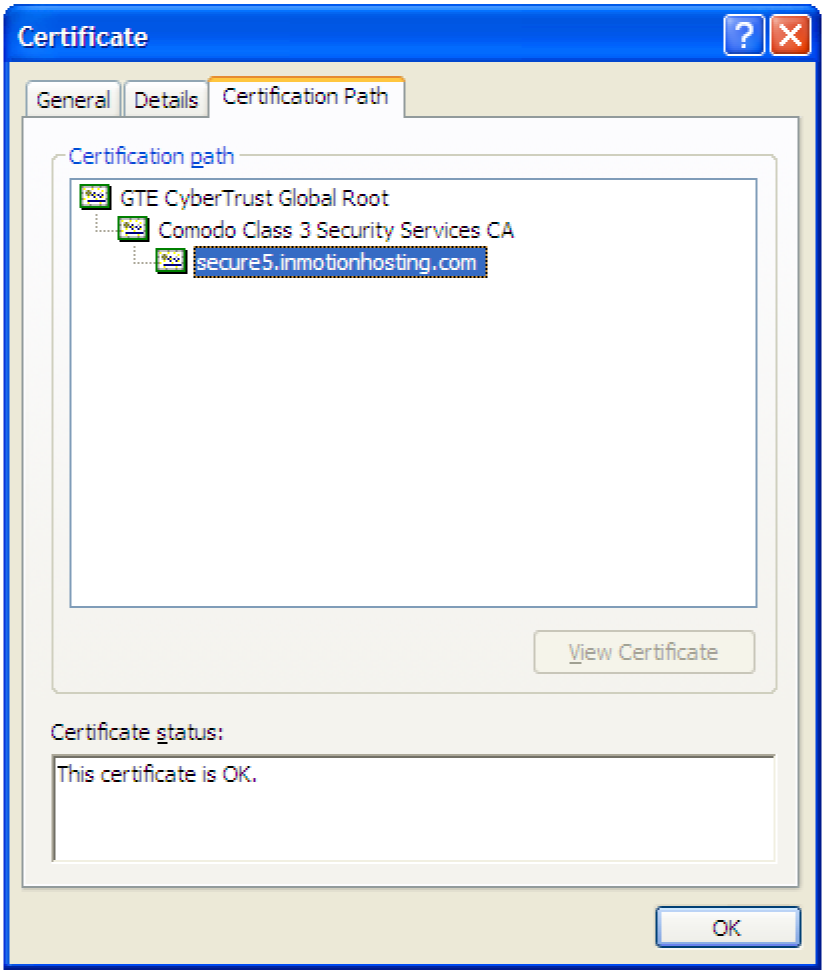
* Refer to the certification authority's statement for details.

Issued to: secure5.inmotionhosting.com

Issued by: Comodo Class 3 Security Services CA

Valid from 2/16/2005 **to** 3/26/2006

Now this screen tells you the identity of the server, and who the “issuer” is of the identity – otherwise known as a “Certification Authority”, or CA for short. In the screen above, this is from the mailing list registration page at http://www.mybowlingdiary.com/. The certificate was issued to the hosting web server from “Comodo Class 3 Security Services CA”. But then the question is “Who trusts the issuer”? Can you be reasonably certain that the certificate was issued from a reputable source? Click on the “Certification Path” tab –



Certification path

GTE CyberTrust Global Root
Comodo Class 3 Security Services CA
secure5.inmotionhosting.com

Certificate status:

This certificate is OK.

This is known as a “Certificate Chain”. This allows you to see who issued the certificate and make a decision as to whether or not to trust the site. Note that the “Comodo Class 3 Security Services CA” has an issuer as well. Since this was issued by “GTE CyberTrust Global Root” (this is also known as the “Root CA”) I can rest assured that this certificate is valid because I know about GTE CyberTrust.

Before issuing certificates to the general public, an issuing CA must be “signed” or validated by a “Root” certification authority. Some of the more popular “Root CA” are VeriSign, Thawte, ValiCert and GTE. When signing or validating an intermediate issuer, these “issuers” must pass a stringent audit of their facility to include physical and computer security. Reputable companies have their certificates signed by one of these root authorities, and you can be reasonably certain that your data is safe.

OK, enough brain overload. Let me give you some more tips

- This may not be computer related, but if you have papers with personal information (i.e. bank statements, pay stubs, etc) that you are discarding, shred these papers before putting them in the trash. You can purchase personal shredders for a reasonable price at most office supply stores. Believe it or not, when you put something in the trash and take the trash out of your home it becomes part of the “public domain” which means that people can actually “dumpster dive” legally

- If you go to websites where you must sign in, (banking, purchasing sites and the like) these sites usually ask for a username and password. Choose a password that is easy for you to remember and hard for someone to guess. Don't use your spouse's name, kids' names or the name of your dog. Use numbers, and upper / lower case letters. Example:
    - If your child's name is Cheryl, don't use "Cheryl" as the password. What you might do is something like "ch3ry1" or "Ch3Ryl"

  Above all, **don't write your passwords down - especially on "post it" notes - and leave them under your keyboard.** You're just asking for trouble.

- Before you decide to do business with a company, review their privacy policy, especially with regard to email addresses. Any reputable company should, on request, provide you with their complete privacy policy. Be wary of emails that look like they are coming from a reputable company with web links. These could be "phishing" attack, or an attempt by someone to gain access to your personal information. In this type of attack, a hacker will put a URL (web link) into an email where it will look legitimate, but actually the URL directs you to another site where the attacker can get your username and password. If you suspect that an email is a "phishing" email, contact the company and ask if they sent this email. Most reputable companies have a policy that they DO NOT solicit your password.