
Dealing with
Online Security
Threats

A presentation
on

Dealing with Online Security Threats

given to the
Illawarra Computer Enthusiasts Club

by Rolf Schreiber, 23 June 2012

Overview

- Safe Use of the Internet
- Protecting Your Computer Network from Cyber Intruders
- Computer Security (Malware and Spam)
- Protecting Your Online Privacy
- Avoiding Online Identity Theft
- Protecting Your Online Financial Transactions

Safe Use of the Internet

ADSL, the ‘Always On’ Internet Connection

- If you have an **ADSL** Internet connection, your home network is ‘live’ on the Internet as soon as you switch on your computer, even if your browser isn’t running.
- The connection is **bi-directional**, so while ever you are connected to the Internet, the **Internet is connected to your computer network**.

Use the Internet Responsibly

You have a responsibility to use the Internet in a safe manner, in order to **protect**:

- **yourself** from ‘cyber intrusions’
- **any children** using your computer network from unsuitable content / online predators
- **other Internet users** from potential damage **if your computer were to be hijacked** (become part of a ‘botnet’) and used for illegal purposes

Practice Safe Internet Use

- Avoid accessing web sites with questionable content, since this often results in spyware or malware infecting your computer.
- Don’t download unknown or unsolicited programs.
- Don’t open, forward or reply to suspicious or unsolicited emails.
- Don’t open email attachments or click on web site addresses in the email.

Be Diligent with Computer Security Updates

- Having computer security software installed on your computer **is not enough**!
- The malware ‘definitions’ need to be **constantly updated**, if the installed security software is to provide an effective defence against the constant stream of new cyber threats.

Keep Your Operating System & Browser Up-to-Date

Download all the Microsoft software patches and security updates for WinXP, Vista, Win7 **and** the browser (especially Internet Explorer)

Protecting Your Home Network from Cyber Intruders

Use a Firewall

- A firewall is usually software that creates a protective barrier between your computer network and potentially damaging content on the Internet.
- The firewall helps to guard your computer network against online attacks (‘cyber intrusions’).
- The firewall should also monitor **outgoing** traffic, to ensure that no **unauthorised** information is being sent.

Zone Alarm Free Firewall

Take Precautions When You Go Wireless

- Many homes now have a wireless network, which allows mobile devices such as laptops, netbooks, iPads and Tablets to share an Internet connection
- While convenient, a wireless network can be a security risk, **if the network is not secured** with a password

Securing the Wireless Network

To secure your wireless network:

- change the default SSID
- don’t hide the Access Point
- use WPA2 encryption with a strong password

Online Computer Security when Dealing with Malware and Spam

How Does an Unprotected Computer Become Infected?

Without a connection to the Internet:

- running infected media (floppy disk, CD/DVD ROM) on your computer
- opening an infected email attachment offline
- running an infected downloaded file

How Does an Unprotected Computer Become Infected? (cont.)

While connected to the Internet:

- any “online” (Internet based) activity can potentially cause an infection
- just ‘viewing’ a malicious web page, without even clicking on any links

Physical Symptoms of Infection

The usual visual symptoms that a computer is infected with some type of malware may include:

- the computer runs more slowly than usual
- the computer may frequently lock up or reboot
- certain programs (eg antivirus software) may stop working properly
- Internet connectivity may be lost, or the browser becomes very slow at accessing websites, or can’t access them at all

Malware Overview

- "malware" is a contraction of mal<u>icious soft</u>ware, and includes:
  - computer viruses ('viruses')
  - computer worms ('worms')
  - trojan horses ('trojans') and
  - rootkits
- some overlap with spyware:
  - all spyware is malware, but
  - <u>not</u> all malware is spyware

Computer Virus

- self-replicating computer code
- designed to avoid detection
- spreads by ‘infecting’ executable files
- an infected file must be ‘run’ for the virus to become ‘active’ in the computer’s memory
- carries a ‘payload’ designed to cause damage
- cannot survive “in the wild”

Computer Worm

- self-contained, self-replicating computer program
  - can survive “in the wild”
- usually spread by opening an infected email attachment
- designed to:
  - delete files on a host system
  - send documents (‘spam’) via email
  - carry other ‘executables’ as a payload

Trojan Horse

- malicious program disguised as legitimate software
- cannot replicate itself
- allows unauthorized remote control of a compromised computer while online
- can be used to set up massive ($>10^6$) networks of zombie computers ('botnets') to carry out illegal activities on a massive scale

Rootkit

- collection of malware tools (programs) enabling unauthorized administrator-level access to a computer
- may consist of spyware and other malware
- creates a ‘backdoor’ into the system for the hacker’s own malicious or illegal use
- **cannot** be detected by normal antivirus software

Spyware

- software that is designed to steal personal information and then send it ‘back to base’
- may be present in a spam email, **or**
- may be embedded in a web page that you have been ‘tricked’ into visiting, eg, taking advantage of a person’s accidental mis-spelling of the real web page

Use Up-to-date Computer Security Software

Free Anti-Malware Software:

- **Anti Virus:** AVG Antivirus Free, or Avast Antivirus Free
- **Anti Spyware:** SpyBot & Ad-Aware
- **Anti Rootkit:** RootkitRevealer (from www.sysinternals.com)
- **Firewall:** ZoneAlarm Free

Spam Overview

- the term ‘spam’ is generally used when referring to unsolicited emails
- the use of ‘spamming’ techniques can be applied to other forms of electronic communications

Spam – The Details

All types of ‘spam’ have one or more of the following characteristics:

- unsolicited
- sent in bulk (usually >10^6 email addresses)
- have a monetary motive (ie, trying to sell you something, or get you to send them money)
- may contain spyware or malware
- may use ‘phishing’ techniques to try to obtain personal information

Protecting Yourself from Spam

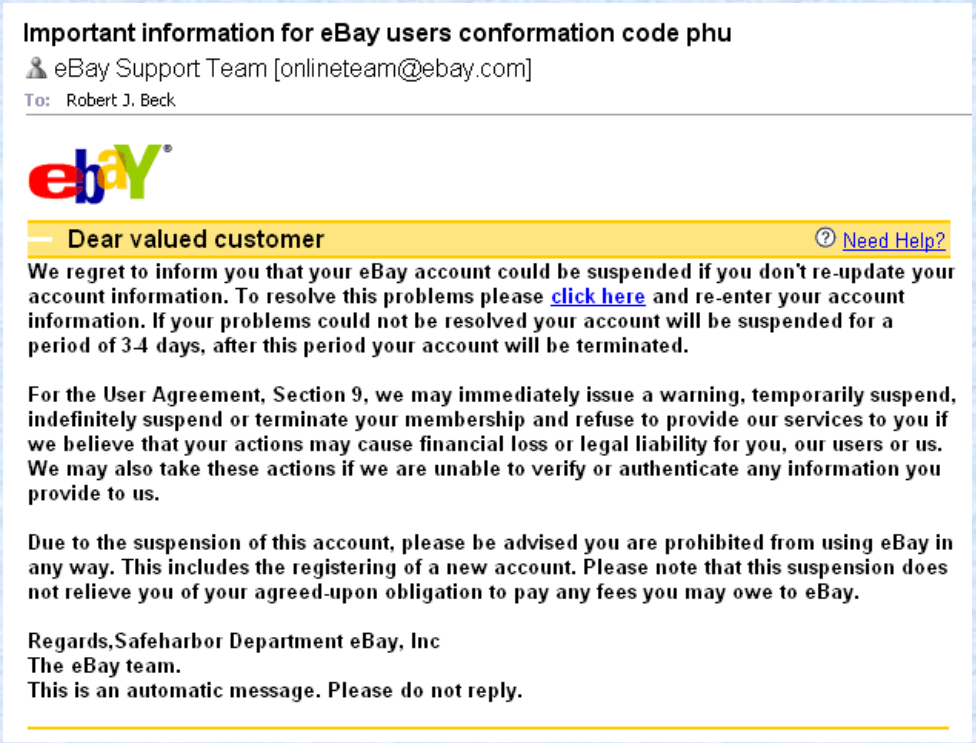
- install and use an email spam filter (eg Mail-washer Free) to assist in the detection and filtering out of unsolicited emails
- while it may be possible to minimize spam in your email inbox, it can never be completely eliminated
- the only safe way to protect yourself from spam emails is **to do nothing** except delete them

‘Phishing’

- a type of deception (‘scam’) designed to steal your **personal** information).
- use false pretences to try to get you to disclose valuable personal data
  - credit card numbers
  - passwords
  - bank account data, or
  - other financial information

Phishing Scams

- most are delivered online through spam emails or pop-up windows



Important information for eBay users conformation code phu

eBay Support Team [onlineteam@ebay.com]

To: Robert J. Beck

ebay

Dear valued customer — Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 3-4 days, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.

How to Protect Your Online Privacy

Your Online Privacy

There are laws in Australia about online privacy protection. If you want to know the details, go and research the topic for yourself.

The most effective way for you to protect your online privacy is to be very particular who you give personal information to – it should be on a strictly need-to-know basis.

Social Networking Sites can be a Privacy Problem

Think twice before you sign up for a social networking account such as ‘Facebook’, et al

All these social networking sites rely on sharing access to personal information between friends.

This can become a trap for allowing one’s personal information to escape into the public domain, where it may be readily stolen.

Remember: Once anything is on the Internet, it can never be completely removed/recalled.

How to Avoid Online Identity Theft

What Is Online Identity Theft?

- fraudulent practice of using another person's name and other personal information online, usually for financial gain

What Personal Information Do Identity Thieves Look For?

Personal information that can be used to steal a person's identity can include their:

- address
- date of birth
- mother's maiden name
- driver's licence details
- medicare details
- credit card details
- passwords to bank accounts, etc.

Protecting Your Online Identity

Avoid giving personal information to anyone who doesn't have a legitimate reason to ask for it.

Organisations with a legitimate right to know your personal details would include:

- government departments
- financial institutions
- health funds, etc

Be wary of divulging personal information to anyone else.

How to Protect Your Online Financial Transactions

Don’t Use Public Computers for Financial Transactions

Never use a public computer for carrying out any financial transactions. You might be at risk of having your login name and password stolen, if the computer has keystroke logging software installed.

Protecting Your Online Financial Transactions

- Choose strong passwords for your financial logins (ie, for banking, eBay transactions and buying online)
- Change your passwords regularly
- Don’t share your passwords with anyone
- If possible, use a credit card (for fraud protection) and avoid using direct transfers (much harder to get your money back!)

Protecting Your Online Financial Transactions (cont.)

- Setup and use a **Paypal** account for online purchases
- It is possible to use a security key with your Paypal account, which makes logins significantly more secure

PayPal®

Any Questions?