

## **Internet safety –**

**READ what you are clicking on!!** Some EULA's state they will install software on your machine for data gathering purposes.

**RENAME the administrator account** - Because the Administrator account is created by default it gives a hacker 50% of the information they need to access your computer. All they have to do then is crack the password. To make things more difficult, it is good practice to rename the Administrator account. You can call it anything you like.

Assign the **guest account** a password, and disable the guest account when not in use.

1. **Install and maintain anti-virus software.** This software checks for known viruses by scanning your computer periodically. Most will also check for viruses on incoming email. It is important to update the software as well though.

New viruses are discovered almost daily. Configure the AV for automatic updates at a minimum of daily.

2. **Do not open unknown or suspicious email.** Many viruses and worms use what is called "social engineering". That is, they attempt to trick you into becoming a participant in the process. The latest viruses can "spoof" the sending email address so that it looks like it is coming from someone other than the computer that infected it.

If an email is not from someone you know, it is usually best to simply delete it without looking at it. If the email appears to be from someone you know, you should read the message carefully before opening any attached files. Viruses and worms often have bad English and poor grammar. Consider whether the person you know would really have written that message or forwarded you the attached file. If in doubt, contact that person you know to confirm they truly sent it before opening the attachment.

3. **Keep your computer patched against known vulnerabilities.** Almost as often as new viruses are discovered, new vulnerabilities are discovered as well. Many times they are in the operating system (like Windows), but vulnerabilities are also found in tools like your web browser, email software and other 3rd party tools. If left unpatched, these vulnerabilities can be exploited by hackers to obtain access and control of your computer.

Staying up to date can be difficult. Some vendors, such as Microsoft, have automated utilities that check for updates and notify you. Other vendors may have an email mailing list you can join so they can notify you of any new updates. If your vendor doesn't offer one of these solutions, you may just need to periodically visit their support web site to check for any new patches or updates.

#### 4. **Peer-To-Peer (P2P) - Don't Use P2P On a Corporate Network:**

At least, don't **ever** install a P2P client or use P2P network file sharing on a corporate network without explicit permission- preferably in writing. Having other P2P users downloading files from your computer can clog the company's network bandwidth. That is the best-case scenario. You may also inadvertently share company files of a sensitive or confidential nature. All of the other concerns listed below are also a factor.

#### **Beware The Client Software:**

There are two reasons to be cautious of the P2P network software that you must install in order to participate on the file-sharing network. First, the software is often under fairly continuous development and may be buggy. Installing the software might cause system crashes or problems with your computer in general. Another factor is that the client software is typically hosted from every participating user's machine and could potentially be replaced with a malicious version that may install a [virus](#) or Trojan on your computer. The P2P providers do have security safeguards in place which would make such a malicious replacement exceptionally difficult though.

#### 5. **Don't Share Everything:**

When you install P2P client software and join a P2P network like BitTorrent, there is generally a default folder for sharing designated during the installation. The designated folder should contain only files that you want others on the P2P network to be able to view and download. Many users unknowingly designate the root "C:" drive as their shared files folder which enables everyone on the P2P network to see and access virtually every file and folder on the entire hard drive, including critical operating system files.

#### 6. **Scan Everything**

You should treat all downloaded files with the utmost suspicion. As mentioned earlier, you have virtually no way of ensuring that what you downloaded is what you think it is or that it doesn't also contain some sort of Trojan or virus. You should also scan your computer periodically with a tool such as [Ad-Aware](#) to ensure you haven't unwittingly installed spyware on your system. You should perform a virus scan using updated antivirus software on any file you download before you execute or open it. It may still be possible that it could contain malicious code that your antivirus vendor is unaware of or does not detect, but scanning it before opening it will help you prevent most attacks.

## **Phishing –**

<http://www.microsoft.com/athome/security/email/phishing/video1.mspix>

[http://www.mailfrontier.com/forms/msft\\_ig\\_test.html](http://www.mailfrontier.com/forms/msft_ig_test.html)

<http://www.sonicwall.com/phishing/>

1. **Be Skeptical:** It is better to err on the side of caution. Unless you are 100% sure that a particular message is legitimate, assume it is not. You should never supply your username, password, account number or any other personal or confidential information via email and you should not reply directly to the email in question. If the user really suspects that an e-mail is legit, they should:
  - Close their e-mail client
  - Close ALL browser windows
  - Open a brand new browser,
  - Surf to the e-commerce company's site as they normally would. If there's anything wrong with their account, there will be a message at the site when they log in. We need people to close their mail readers and browsers first, just in case an attacker sent a malicious script or tried to direct the user to a different site.
2. **Initiate contact to the organization:** An even safer means of verifying if an email regarding your account is legitimate or not is to simply delete the email and pick up the phone. Rather than risking that you may somehow be emailing the attacker or mis-directed to the attacker's replica web site, just call customer service and explain what the email stated to verify if there is truly a problem with your account or if this is simply a phishing scam.
3. **Review statements:** When your bank statements or account details arrive, whether in print or through electronic means, analyze them closely. Make sure there are no transactions that you can't account for and that all of the decimals are in the right spots. If you find any problems contact the company or financial institution in question immediately to notify them.
4. **Use secure browsers:** The latest generation web browsers, such as [Internet Explorer 7](#) and [Firefox 2.0](#) come with built in phishing protection. These browsers will analyze web sites and compare them against known or suspected phishing sites and warn you if the site you are visiting may be malicious or illegitimate.
5. **The safest practice** is to open a new browser window and navigate to the page yourself. Use the e-mail in question to provide you with the source of your questions.

## **Identity Theft –**

**Shred everything.** One of the ways that would-be identity thieves acquire information is through “dumpster-diving”, aka trash-picking. If you are throwing out bills and credit card statements, old credit card or ATM receipts, medical statements or even junk-mail solicitations for credit cards and mortgages, you may be leaving too much information laying about. Buy a personal shredder and shred all papers with PII on them before disposing of them.

**Destroy digital data.** When you sell, trade or otherwise dispose of a computer system, or a hard drive, or even a recordable CD, DVD or backup tape, you need to take extra steps to ensure the data is completely, utterly and irrevocably destroyed. Simply deleting the data or reformatting the hard drive is nowhere near enough. Anyone with a little tech skill can undelete files or recover data from a formatted drive. For CD, DVD or tape media you should physically destroy it by breaking or shattering it before disposing of it. There are shredders designed specifically to shred CD / DVD media.

**Limit revealing your SSN to organizations unless absolutely necessary, and NEVER send your SSN through e-mail or other unencrypted mediums.**

## **Wireless “Hot Spots”**

**Make sure your firewall is activated.** A firewall helps protect your mobile PC by preventing unauthorized users from gaining access to your computer through the Internet or a network. It acts as a barrier that checks all incoming information, and then either blocks the information or allows it to come through. All Microsoft Windows operating systems come with a firewall, and you can make sure it's turned on.

**Disable file and printer sharing:** File and printer sharing is a feature that enables other computers on a network to access resources on your computer. When using your mobile PC in a hotspot, it's best to disable file and printer sharing because when enabled, it leaves your computer vulnerable to hackers. Remember, though, to turn this feature back on when you return to the office.

In Windows XP –

1. Click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **Security Center**.
3. In the **Security Center** window, click **Windows Firewall**.
4. In the **Windows Firewall** dialog box, click the **Exceptions** tab.
5. On the **Exceptions** tab, under **Programs and Services**, clear the **File and**

**Printer Sharing** check box and then click **OK**.

In Windows Vista –

1. Click **Start** and then click **Control Panel**.
2. In **Control Panel**, select **Network and Sharing Center**.
3. Under **Sharing and Discovery**, turn **File Sharing** and **Printer Sharing** to off.

**Make your folders private.** When the folders on your mobile PC are private, it's more difficult for hackers to access your files.

In XP –

1. Click **Start**, and then click **My Computer**.
2. In the **My Computer** window, double click the drive where Windows is installed, and then double click **Documents and Settings**.
3. Double click your user folder, right-click the folder that you want to make private, and then click **Properties**.
4. In the **Properties** dialog box, on the **Sharing** tab, click **Do not share this folder**, and then click **OK**. Repeat the steps above for each folder that you want to make private.

In Vista –

Windows Vista not only makes folders private by default, but it also requires passwords for shared folders. As a result, you're already covered! But if you want to double check, simply right click on the folder in question, and select **Properties**. On the **Security** tab, you can review the set permissions.