



“Stay safe whilst using the Internet”

A paper showing guidelines on how to protect yourself, your computer and your family whilst using the Internet.

Table of Contents

Abstract	3
Introduction	3
Modern dangers of the Internet.....	3
Software to avoid these dangers	4
Ways for children to stay safe online	5
Ways for adults to stay safe online	7
How to secure logins	7
Real world examples	7
Conclusion	8

Abstract

In this paper, I set forth guidelines for staying safe while using the Internet. I propose several security enhancements to daily Internet use with the intension of keeping your computers, and your private data safe. The author of this paper does however remind the reader that these are only guidelines, and cannot 100% guarantee your safety whilst using the Internet. My employers and I therefore accept no liability for any computer infections or data losses readers may encounter before or after reading this paper.

Introduction

The Internet started in the 1960s as a project commissioned by the United States Department of Defense. Their plan was to create a network of computers – which at the time was called the ARPANET – with redundant paths to allow researchers to share data. The network had to be redundant so as to allow multiple paths of communication in case one path was to fail. The need for this network can be seen from both an academic perspective, and also from a military one, as at this time the United States found themselves in the middle of the Cold War.

Along with the Department of Defence, a select number of higher education establishments were also granted access to use the ARPANET. Throughout the next 30 years, many more establishments were also granted access. In the early 1990s the ARPANET became available for public use and its name officially changed to the Internet.

The modern day Internet is a collection of computers that are connected together to allow users to share data. Home users are able to connect to the Internet via a paid subscription to an Internet Service Provider (ISP). These currently include, but are not limited to BT, TalkTalk, and Virgin Media.

Modern dangers of the Internet

Simply stated, the Internet can be a very dangerous place and allows for anonymous communications between users from any part of the world. Some of the most common dangers on the Internet are:

- **Malware:** Malware is a term used to describe any software that is designed to access a user's computer without their consent. Malware is short for malicious software. Malware includes the following:
 - **Viruses** – A virus is a piece of malicious software that can copy itself and infect a computer. A virus can copy itself in many ways such as when being sent over a network (possibly via email without the sender's knowledge) or when automatically transferred onto a USB drive.
 - **Worm** – A worm is another piece of malicious software that can copy itself and infect a computer. Unlike a virus, worms are capable of self replicating. This means that it needs no user intervention to travel from one computer to another.

- **Trojan Horse** – A Trojan Horse is a piece of malicious software which masquerades as a legitimate piece of software. A Trojan Horse can be “bundled” in with a piece of software downloaded from the Internet. The “bundled” software is normally a virus or worm.
- **Spyware** – Spyware is a form of malicious software that once installed on a computer will start collecting information about the user, and will send it back to a third party. This information is then normally sold to a buyer.
- **Adware** – Adware is a form of software that automatically displays, or downloads advertisements onto your computer. Adware creators can purchase information from Spyware creators about your computer usage, and then display adverts on your computer which are tailored to your browsing habits. They can also change settings on your computer to redirect you to their websites (i.e. it is very common for Adware to change your web browser homepage to a site under their control without your consent).
- **Phishing Websites:** Phishing Websites are websites that masquerade as a trustworthy identity in the hope of acquiring usernames, passwords, and other sensitive information from users. Users are normally sent a SPAM email which appears to be from a trustworthy identity (i.e. your bank) and asks that you visit a website which will ask for private information.

Software to avoid these dangers

The following list of software should be installed on your computer to protect users:

Anti-Virus

Anti-Virus software is software that is used to prevent, detect and remove malicious software include Viruses, Worms and Trojan Horses. They normally do not remove Spyware or Adware. Commonly used Anti-Virus products can be purchased or downloaded for free from the following companies:

- AVG – <http://free.avg.com> or <http://www.avg.com>
- Avast – <http://www.avast.com>
- Kaspersky – <http://www.kaspersky.co.uk>
- Symantec/Norton – <http://www.symantec.com>
- McAfee – <http://www.mcafee.com>
- Sophos – <http://www.sophos.com>

All of the previously mentioned Anti-Virus products are comparable. The important thing to do with any Anti-Virus product is to **make sure the program has up-to-date anti-virus definitions**. The software should be set to auto-update. Please note that newly purchased laptops/computers usually come with a trial version of anti-virus software installed. To best protect yourself and your family this software should not be allowed to expire.

Anti-Spyware

Anti-Spyware software is software that is used to remove or block spyware from entering your computer. The two most popular Anti-Spyware products are:

- “Spybot – Search & Destroy” – <http://www.safer-networking.org>
- Microsoft Windows Defender – <http://www.microsoft.com/windows/products/winfamily/defender/default.mspx>

Anti-Adware

Anti-Adware software is software that is designed to remove or block adware from entering your computer. The most popular Ad-Ware removal program is Ad-Ware from Lavasoft:

- Ad-Ware – <http://www.lavasoft.com/>

Firewall

A Firewall is part of a computer system that blocks unauthorised access to a network or computer, while still allowing authorised communications. The most popular firewall products are:

- **Windows Firewall** – This program is installed on all Microsoft operating systems from Windows XP onwards. You can check the status of this firewall (i.e. it should be turn on unless you are using a third party firewall) by following this path:
 - Start > Control Panel > Windows Firewall
- **Zone Alarm** – <http://www.zonealarm.com/>

Operating System and Applications

The final pieces of software to check are the Operating System, and the Applications you use on your computer (especially the web browser). You must keep all these products up to date with the latest security patches. You can do this by using Windows Update, and making sure it is set to allow automatic updates. You can access Windows Update via:

- Start > All Programs > Windows Update

Ways for children to stay safe online¹

- Don't share your password with anyone else – **ever!**
- Before you share any information about yourself on the Internet, get your parents' permission.
- Double-check the URL (the address of the Web site) before hitting the Enter key or before clicking a link. Make sure the spelling is right. This will help ensure you go to the site you want, and not some other place. (See Appendix 1).
- Check with your parents or another adult you trust before going into a chat room. Different chat rooms have different rules and different types of people going to them. You and your parents want to make sure it is an appropriate place for you before you enter.

¹ 30 Ways to Stay Safe on the Internet; <http://www.chaminade.org/MIS/WebSafety/30ways.htm>

- If something you see or read online makes you uncomfortable, leave the site. Tell a parent or a teacher right away.
- Never send a picture of yourself (or anything else) to someone in e-mail unless your parents say it is okay.
- If you receive unwanted, offensive, mean, threatening, or harassing e-mail, do not respond to it. Tell your parents or another adult right away.
- Remember: not everything you read on the Internet is true!
- Don't give out your age without checking with your parents first.
- Never give out your full name (first and last). Don't give out your first name without checking with your parents or another adult first.
- Never give out your home address over the Internet.
- Ask your parents or an adult before signing up for anything online.
- Don't purchase anything with your credit card (or anyone else's) without permission from a parent.
- Remember, when you are online, what you do is up to you. Don't do anything you don't want to do.
- Don't open files or e-mail from someone you don't know. You don't know what might be inside – the files could contain a computer virus or offensive material. Always scan downloads with Anti-Virus software before opening them.
- Only download software from trusted sources. Never run downloaded software without scanning it with your Anti-Virus software.
- Keep the computer in a common space, like the family room, den, or living room.
- Never agree to meet someone you met on the Internet in person without your parents' permission. You should never meet someone you met online alone. If you do set up a meeting with an online friend, meet in a public place and go with your parent or guardian.
- Remember that any information you share about yourself can be seen by anyone who is online.
- Don't give out your phone number.
- Talk to your parents (or your teacher or another adult) about the kinds of places you go and things you do and see when you are online.
- Pick a name – different from your real name – to use online.
- If someone online asks you too many personal questions, be suspicious. Stop talking with them and report this to your parents or an adult you trust.
- Don't give out the name of your school.
- Always remember that people online may not be who they say they are. It is very easy for people to pretend to be someone they are not.
- Don't do things online that you wouldn't do in real life.
- Keep social networking profiles private. Do not accept invites from people you do not know and trust.
- Be careful when someone offers you something for free, like gifts or money. You don't know what their motives are. Decline the offer and tell your parents.
- Treat other people as you'd like to be treated. Never use bad language or send mean messages online.
- The "off" button is always there. Use it if you need to. You don't have to stay online if you don't want to.

Ways for adults to stay safe online

The above information can also keep adults safe online, however there are some other concerns that are specific to adults. They include:

- Never purchase anything on the Internet from an un-trusted source. Always check the URL starts with “https” before sending credit card or debit card information across the Internet.
- Be aware of what your children are doing online. Have them show you their social networking profiles at random intervals.
- If you must use Internet Banking, make sure your computer is fully protected. Also run an Anti-Virus scan with up to date definitions before you start.
- Run Anti-Virus scans on a regular basis. This would preferably be done everyday when the computer is not in use.

How to secure logins

Usernames and passwords are the most common way to prove your identity on the Internet. It is therefore extremely important that these details are kept private. Follow the guidelines below to stay secure:

- Do not ever use the same password on multiple sites.
- Change your passwords on a regular basis.
- If you must write down passwords, store the hard copy list in a secure location away from prying eyes.

Real world examples

As the first example, consider the following:

I send you an email (such as this file) which you download to your computer. Once downloaded you open it, read it, and follow one or two of the guidelines in it. You then go about your life thinking that you are keeping your private information safe. You should have followed all the guidelines...

What actually happens is this:

You download the file and open it. Once opened, the file launches a piece of software that was bundled with it – without you ever knowing. This software allows me to monitor your habits online, and also keeps track of all the keystrokes you type. In real time this information is sent to an email address that I control. I can then log into your email account with the information I have captured. Once in your email account I can send an email to your entire address book telling them to click a link to a website (i.e. a bargain holiday you came across, or a site that you have created to keep in touch with people, or whatever it is that you and your friends have in common). When they click the link (why wouldn't they? They trust you!), they are taken to a website that looks genuine, but actually installs the exact same software on their computer that was

originally installed on yours when you opened the attachment. I would then do the exact same thing to the computers that I had just infected.

With all the information gathered, I could also start stealing identities. I could do any of the following:

- Open new credit card accounts in your name. I of course will never pay the bill – but you will have to!
- Change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account.
- Open a bank account in your name and write bad checks.
- I could also give your personal information to police during a stoppage. When I don't show up for my court date, a warrant for an arrest will be issued in your name.

Computers that are taken over by Viruses, Worms or Trojan Horses allow cyber criminals to do a lot of different things with your computer. Three very common examples are:

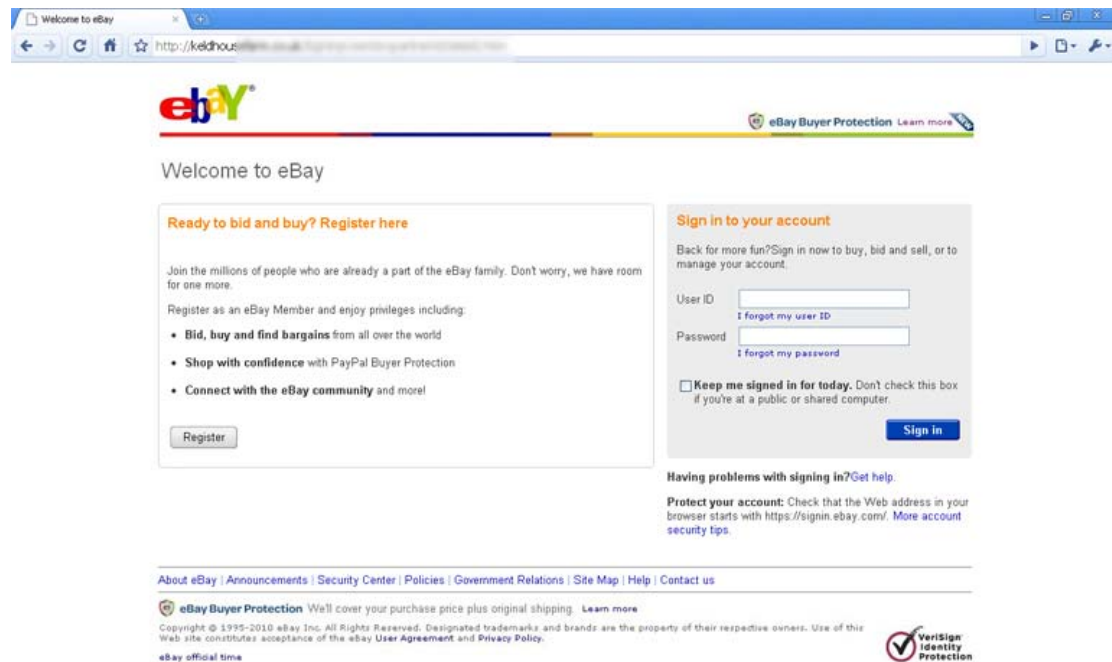
- **Send spam** – Spam is the sending of unsolicited bulk messages indiscriminately. An attacker may use your compromised computer to send millions of SPAM emails daily. This will slow your computer to a crawl, and also blacklist your computer with many websites on the Internet.
- **Host websites on your computer** – A common use of infected computers is to host websites without the owner's knowledge. Cyber criminals may use your computer to host illegal websites such as those containing child pornography. When people type in "http://www.very-bad-website.com" they are actually viewing content that is hosted on your computer. Sooner or later you will get a knock at your door from the police under the orders of Interpol.
- **Participate in DDoS** – A Distributed Denial of Service (DDoS) is an attack that is used to make a website unreachable. Your infected computer will become part of a botnet (along with all the other computers a hacker has infected), and at the same time, all these computers will request a website for a defined period of time. By doing this, all the websites resources are taken up by the botnet, and genuine users are unable to reach the website. Once again, if this happens, your computer will be blacklisted from many websites on the Internet.

Conclusion

Staying safe while online is not difficult. It is simply a matter of staying alert, questioning everything, and keeping your protective software up to date. If all the guidelines in this document are adhered to, you should be able to limit the risk of someone successfully attacking you, your computer, and more importantly, your family.

Appendix 1

At first glance the site below is the eBay logon page.



A closer look however shows that the URL for this site is actually (I have removed some of the letters so as to protect anyone who thinks it is a good idea to go to this website):

`http://keldh*****.co.uk/SignInUserId*****nerId2siteid2.htm`

This is an example of a phishing site. The user will input their username and password and then try to sign in to eBay. What actually happens is that the site steals your username and password, and then redirects you to the actual eBay page which tells you your username or password are incorrect. The user simply thinks they have typed the information wrong, retypes it, and successfully logs into eBay. They are completely unaware that their eBay login details have just been stolen!

Appendix 2

If you would like to contact me regarding any of the information in this document (or for any other reason), I can be contacted via email at:

Email: dduffield934@c2kni.net