INTERNET SECURITY

The Threats

When information like emails or web pages is sent over the *Internet* it passes through many different computers to reach its destination. Unless you take suitable precautions, your information could fall into the wrong hands. Additionally, you may open your computer systems to unauthorised access simply by being connected to the Internet.
You should take these threats seriously, but don't panic! Basic precautions will minimise the risks.

Email

Email is a fast and efficient way of communicating, but sending information by email is not secure unless you take extra measures. A good rule of thumb is "If you wouldn't be happy writing it on a postcard then don't send it by email". You can protect sensitive information such as personal details by encrypting emails before you send them. Even if an encrypted email is intercepted, the information in it cannot be read.

One of the best known encryption programs is PGP (Pretty Good Privacy). PGP is free for personal and non-commercial use and can be downloaded from the International PGP home page. The intended recipient of your email will also need PGP installed on their computer. Another way of encrypting emails is to buy a digital certificate that works in conjunction with your email program. Digital certificates can be bought from companies such

as Verisign and Thawte. Free certificates that don't include your name are also available from Thawte and CACert and it is possible to add your name through their verification schemes. As well as encrypting your emails, Personal Email Certificates can digitally "sign" your e-mail so that people know it came from you.
The potential threats posed by email are not limited to email being intercepted and read. Emails are also used to distribute viruses (see under viruses below), hoaxes, and various scams to try and part you from your cash.

Beware of any offers you receive by email that seem too good to be true, they probably are! The "From" address in an email can be forged relatively easily to make it appear to have come from a legitimate source, as can the date and time. This is known as "spoofing".

Web links in emails can also be forged. *Phishing* is a now common method of stealing personal information such as passwords, bank details, credit card details etc. Emails are sent out en masse, purporting to be from well known companies such as banks, auction sites etc. The sender tries to trick recipients into giving out personal information, for example by asking them to click on a Web link in the email and reconfirm their details by entering information into a form on a website. Clicking on the link in such emails takes the user to what very convincingly appears to be a legitimate website. In reality the user is taken to a fake site that uses the details entered in the form to access their bank account for example, and steal their cash.
Treat such emails with a great deal of caution and never click on the links in the email. Type web addresses into your *web browser* yourself. Banks will never send you an email asking you to confirm details. If in doubt, 'phone your bank.
For more on spoofing and phishing see the IT Safe website.

Viruses

A computer virus is software written for the sole purpose of infecting a computer. The effects range from irritating but harmless, such as humorous text being displayed on your monitor, to malicious - for example destruction of all the files on your hard disk. E-mail is now the most common way of spreading viruses. Before email, viruses were spread on *floppy disks*, and they can still spread this way.
A virus is usually sent as an attachment to an email. The damage is done when the attachment is opened. Often the message is designed to intrigue you, so that you will open the attachment. The most famous example of this was the "I Love You" virus which caused worldwide disruption. When its attachment was opened it scanned your contacts and sent all of them an e-mail which looked as though you had sent it. Many viruses created since then have used similar methods.

It is ***vital*** that you install *antivirus software* on all your computers and that you update the software regularly.
Most antivirus software makes this process simple and the main vendors release updates on their website every week or fortnight. The software can be set up to check for updates automatically on a regular basis, provided the computer is switched on and connected to the Internet at the scheduled times.

There is a time lag between the first appearance of a virus and the development of a "cure", so use vigilance and common sense.

Be cautious about opening email you are not expecting, or which comes from people you don't know.

Don't open unsolicited emails.

Even if you receive an attachment that you are expecting, save it to your hard drive or another disk before you open it. Microsoft Word documents and others can contain viruses.

Make sure your Antivirus software is up to date and that it scans the attachment***before*** you open it. Don't open the attachment if your software detects anything untoward.

Active code

Malicious material can be included in the code used to write web pages. An increasing amount of email is also written in *HTML*, the code used for web pages. This allows you to send and receive attractive messages which can include pictures. However, HTML email can also include malicious content. To avoid this problem, set up your email program to send only plain text messages, and convert messages you receive to plain text. Malicious code means that you can now get a virus simply by opening an email message, even without an attachment.
If you use Microsoft Outlook or Outlook Express with the preview pane open, some viruses can infect your computer even if you don't open the infected message. Deal with this problem by ensuring your antivirus software is up to date. Microsoft has since released a software fix for this problem - check that you have updated your Microsoft software using Windows Update.

Trojans

A trojan is a program with a secret purpose - usually malicious. Trojans enter your computer disguised as an email or free program you have downloaded from the Internet. Once installed a trojan attempts to broadcast information to its author each time you connect to the Internet. The author can then attempt to take over your PC as though they were sitting at your keyboard. The trojan can log keystrokes even when you're not online and then attempt to send them to the author next time you connect. By recording your keystrokes information such as passwords, credit card numbers - anything you've typed can be revealed.

Most antivirus programs detect and remove trojans. Prevention is better than cure however. Using a good *firewall* and setting it up correctly can block trojans from your computer.
A firewall is a system designed to prevent unauthorised access to a computer or computer *network*. Firewalls use *hardware*, software or a combination of both.
For more information see the knowledgebase article on Firewalls.

Port scanning

If your network is not connected to the Internet it will normally be safe from everyone except its users. However, once you connect to the Internet you are part of a world network used by millions of people. This may allow uninvited people to access your computer for malicious

purposes such as stealing or damaging your data. They do this by using special software to scan computers connected to the Internet for security weaknesses.

People do this for many reasons, including:

- To use your computer to commit crimes. For example, people may make malicious attempts to take over hundreds or even thousands of computers at once. They then get all the computers to access the same website, so making it unavailable.
- To send out spam (unsolicited email) which looks as though it has come from you. This potentially risks your organisation's reputation, and may get your Internet connection suspended by your Internet Service Provider (ISP) - most ISPs have rules against people using their accounts to send spam. For more on spam see the knowledgebase article Dealing With Spam.
- To wipe files from your computer, steal data or obstruct your Internet connection because they dislike you or your organisation - for example because they don't agree with its values or politics
- To try to get sensitive information such as credit card numbers and personal information

The risk is greater if you have an *ADSL* ("*broadband* - always on") Internet connection, and less if you have an ordinary dial up modem. Every computer connected to the Internet is identified by a number called its "*IP address*" - just as you use a person's phone number to call them, other computers use your machine's IP address to communicate with it. If you use a *modem*, you will only be connected for short periods, and your IP address will be different every time you connect. However, if you have ADSL your IP address may never change, and will certainly stay the same for long periods.
If you use ADSL it is essential to have a firewall. This may be included as part of your ADSL modem, but in some cases (BT for example) it isn't. In such cases be sure to install a software firewall such as Zone Alarm on you computers**before** connecting to the internet. Without a firewall, infection can occur within*seconds* of connecting to the internet.

Spyware

Spyware is any software that gathers information through a user's Internet connection without their knowledge. This is usually for market research purposes, but can be more malicious. Spyware is usually a hidden component of free programs that can be downloaded from the Internet. Once installed, the spyware monitors the user's Internet activity (for example information about websites visited). This information is then covertly sent to someone else. Spyware can also be used to gather information about e-mail addresses and even passwords and credit card numbers. Spyware is similar to a Trojans in that users unwittingly install the product when they install something else.

Spyware can be the cause of many problems with internet connected PCs. For more on spyware see the knowledgebase article Removing Spyware, Viruses and Other Malware from Windows.

Summary

There is much media hype about the dangers of the Internet. The hype is often inaccurate or oversimplified. Although there are some real security threats out there, much can be done to minimise the risks. Here's a summary of precautions you can take to help you stay safe online:

- Never send sensitive information by email (unless you encrypt it first)
- Never open email attachments from an unknown source, scan any attachments from trusted sources for viruses before opening them - even a trusted source could be inadvertently sending you a virus
- Set up your email program to send and receive plain text messages
- Install and use Antivirus software from a reputable manufacturer and keep the software up to date
- Regularly check for security updates for your browser, email program and operating system. Windows users should check for and download critical updates at Microsoft's Windows Update site. It's also worth checking the home page of your Antivirus software manufacturer and the Microsoft Security page
- Be careful what you download and run on your computer
- Even if the program is known and respected make sure you get it from the author's website or a reputable download site rather than someone else's home page
- Block unauthorised access to your computer by installing and using firewall software or hardware to prevent Trojans. If you are using a standalone computer there are a few good personal firewalls that can help including ZoneAlarm which is free to individual and non-profit users. If you are using your computer on a network seek advice from your network support provider on suitable options.

Source :http://www.ictknowledgebase.org.uk/internetsecurity