

## Getting Started

### Computer Security

This section looks at Internet/computer security and gives some basic, practical advice on how to use the Internet safely.

#### **Saving Your Information**

Once you begin to use a computer to store information there is a risk, (only a small one) that the information could be lost due to a malfunction. With modern hardware, such instances are rare, but it is prudent to take some simple steps to protect the information and save you a lot of work.

- Regularly copy your files to a CD or to a USB memory key.
- Sign up for an online back-up service such as Backblaze [www.backblaze.com](http://www.backblaze.com). Some anti-virus software also offer a backup service e.g. Norton.

Just think how handy it would be if you had a copy somewhere of every document in your handbag or briefcase in case your bag was lost or destroyed! Imagine the computer is your handbag or briefcase so if anything happens to the original files on your computer you just retrieve the copies and carry on as normal.

### The Internet

When you use the Internet it can be like strolling down the street with your handbag or briefcase wide open. Anyone on the Internet can 'see' you and, if they connect to your computer, they can rummage through your files and information. For protection it's best to have a Firewall and anti-virus software on your computer.

#### **Firewall**

A 'Firewall' stops people from connecting to your computer without your permission. Fortunately a firewall is included free with Microsoft Windows and is turned on by default and will update automatically.

#### **Anti-Virus**

Some strange people get pleasure from destroying other people's computers by putting malicious viruses on the Internet which can enter your computer and damage or destroy your files.

Viruses can also get into your computer from discs or USB memory sticks that you use to transfer files. Only use files from people you can trust.

Anti-virus software will help to protect you from these threats. Anti-virus software packages often offer both a free version and a version that you pay for. In most cases, these 'free' products are scaled-back versions of commercial products to

which the software manufacturer hopes you will buy one day. Several companies offer free downloadable trial versions of their software that range from 3 to 12 months. Some of the most popular programmes are Avast! [www.avast.com](http://www.avast.com) AVG [www.avg.com](http://www.avg.com) Norton [www.norton.com](http://www.norton.com) and MacAfee [www.mcafee.com](http://www.mcafee.com) Once the software is installed it should automatically update each time you are online.

### **Spyware**

Spyware is like a virus and is unwanted software that infects your computer. It might make it run slow or display annoying pop-up messages. In some cases it might scan your files for personal information or give outsiders control over your computers. Most anti-virus software packages also offer anti-spyware protection.

## **Email**

Remember you must “log out” of your email account when you finish using it. If you just close down the Internet page, and someone else comes along to use the computer you were at, they may inadvertently open your email account if you have not properly signed out. Most email accounts will have a “log out”/”sign out” button that you click to sign out of your account.

### **Phishing**

Phishing occurs when criminals (phishers) pretend to be legitimate organisations, like banks and credit card companies in order to trick you into giving them your personal details such as bank account numbers or PIN numbers. Phishers usually send you an email in which they may ask you to ‘verify’ or ‘re-submit’ personal information by return. They could ask you to complete an online form and may offer you something attractive like money or a holiday if you do so. Be alert for anyone requesting your bank account details, credit card numbers, passwords, PIN numbers or PPS number. Phishers can use this information to impersonate you and make unauthorised withdrawals from your bank account or use it to pay for online purchases. They can even sell on this valuable information to third parties.

Remember, no reputable company will ever ask you to give out personal details by email. Never give out personal details by email, fax or in response to a pop up advertisement or unexpected website address. Trust your instincts. If an email looks suspicious, delete it immediately or if it offers something that looks too good to be true, it probably is. If it appears to come from your bank or credit card company, inform their customer service Department.

Keep a look out also for fake emails that tell you that you have won the lottery or ask for your assistance to smuggle money out of a country and again if it offers something that looks too good to be true, it probably is.

## Safe Shopping Online

### Credit Cards

Many people have concerns about using a credit card online and it's always wise to be careful with your credit card in any situation. However, there is no reason why shopping on the Internet is any less secure, as long as you follow some basic guidelines.

- Ensure the site you are buying from is a secure site. There are a number of ways to identify a secure site:
  - When you get to the payment section of the website, check the web address in the browser starts with [https](https://) (rather than [http](http://)) – this means they're using some sort of security when handing your money.
  - Look for the security icon (a locked padlock or unbroken key symbol) in the bottom right-hand corner of the screen
- If a website doesn't display a full postal address or contact landline number and doesn't display a returns policy or procedure on what to do if there's a problem and you need to return goods, it's in breach of the Distance Selling Regulations, so don't use it! These details are usually displayed on the bottom of the home page.
- Anyone can create a web page, so there's no immediate way for a shopper to tell whether an online shop is genuine at first sight. Try to purchase items from trusted, well-established retailers, or ones recommended by friends.

### Pay Pal

Some website allow you to pay for goods and services using Pay Pal. This service that allows you to make secure payments and money transfers through the Internet. Once you sign up for a Pay Pal account, you can then purchase items and send money without ever sharing your financial information with the retailer.

[www.paypal.com](http://www.paypal.com)

### Alternatives to using a Credit Card

If you do not have a credit card or do not want to use your credit/debit card online, you can still shop online using 3V vouchers. 3V vouchers are disposable pre-paid VISA numbers that can be used to shop online, via mail order or over the telephone just like using a standard credit card. You don't need a bank account to purchase a 3V voucher and they are not linked to any of your financial details. You can purchase a 3V voucher in many local shops, petrol stations etc. Go to [www.3v.ie](http://www.3v.ie) for information on what they are and where you can get them locally.

For more information on using your credit card safely online go to Safe Card at [www.safecard.ie](http://www.safecard.ie)

## Using Public Computers

Sometimes you may use someone else's computer (e.g. an Internet café) to browse the Internet. If you have entered any private information during the session, you should delete it to prevent the next user finding that information.

If the browser is **Internet Explorer** then choose:  
Tools>delete browsing history>delete

If the browser is **Mozilla Firefox** then choose:  
History> Clear Recent History> Select the time range > Clear Now

If the browser is **SAFARI** then choose:  
Settings>History>clear history

## Top Tips

- Have up-to-date anti-virus software and a firewall installed on your computer.
- Don't open email attachments if you are suspicious of them.
- Install the latest security software updates to protect your computer.
- Don't share your password with anyone.
- Do make sure your Internet connection is secure when giving out personal details – look for the padlock icon or the https (rather than http).
- Do make back-up copies of your files and store them in a safe place.
- Don't give out personal banking and credit card details by email.
- Mark your profile private on social networking sites.

So, with some basic precautions you can enjoy all the benefits of your computer without any concern for the security and confidentiality of your information. The Internet is a goldmine of useful information so enjoy and Happy Surfing!

For more information on Internet security see [www.makeitsecure.org](http://www.makeitsecure.org) and [www.getsafeonline.org](http://www.getsafeonline.org)