Maximize your online security by following these tips

## Microsoft Security Essentials

Download Microsoft Security Essentials For Free Anti-Virus Protection. Microsoft Security Essentials helps provide real-time protection for your home PC that guards against viruses and other malicious software. It is simple to install, easy to use and always kept up to date. It's free to anyone with a genuine copy of Microsoft Windows. It offers comprehensive malware protection with automatic updates and it comes from one of the world's largest IT companies

## Browsers

Modern up-to-date browser software helps protect you against online problems Just like any other software, it makes sense to use the latest, most secure web browser. The latest browsers have security features that block fake websites and protect against some viruses (but you still need anti-virus for advanced protection).

If you have updated your computer regularly or bought it in the last couple of years, it is likely that you are already using an up-to-date browser such as Microsoft Internet Explorer 8 (on Windows PCs) or Safari 5 (on Macs) or higher versions. You can check by clicking on 'About' on the browser menu. If this is not the case, you may want to get the new browser software immediately and update it regularly for maximum protection.

## Anti-virus

Anti-virus software protects you, your privacy and your money. Viruses are not good for the computers and they steal personal information, take over your PC, pop up unwanted adverts and can even use your computer to attack other people's computers. You may also hear them called Malware, Trojans, Spyware or Adware. Anti-virus software protects you against all of them. Anti-virus software has to download and updated regularly over the internet.

You can download Microsoft Security Essentials (free for personal use) or antivirus software such as McAfee.

## Do not share private information online

Double-check privacy settings on social networking sites.

What's your mother's maiden name? What's the name of the first school you went to? What was your favorite subject at school? What's your address? Birthday? Phone number?

All this information is useful to people who want to steal your identity or break into your personal internet banking. You wouldn't give this information away to a stranger in the street but if you use social networking sites, such as Facebook, twitter or Myspace, you could be oversharing personal data.

You may want to think carefully about the information you put into your profiles on sites like this. It is also a good idea that you check the privacy settings on each site that you use to make sure you only share personal information with people you trust.

## Look after your Documents

Fraudsters use personal information from different sources to steal people's identities. Viruses are one way to do it but they also use paper documents of your accounts containing personal details, such as receipts and bank statements.

## Understand how criminals use the internet

There are many ways for them to make money online by:

- Stealing your passwords and bank details with viruses, fake emails and fake websites
- Asking you to provide security details
- Using viruses to display unwanted adverts on your pc

take your personal internet security and privacy very seriously. Protecting yourself and your money takes a bit of know-how and the right software.

## Avoid online fraud

If it's too good to be true, it probably is. When it comes to protecting yourself and your money on the internet be wary of ridiculous deals. Criminals may contact you by email, through websites you use, via SMS or even by phone.

If an attachments looks suspicious don't open them. Don't install software unless it comes from a website you trust.

## Protect your mobile phone

Your phone may hold lots of personal data you may even use it for internet banking and online shopping so you should think about:

- Setting and using a security PIN code
- Adjusting the phone settings so that it locks automatically if you don't use it for five or ten minutes
- Not storing passwords or other sensitive information on your phone in a way that can be understood by someone else
- Not storing your home phone number and address under 'home' in the contact list
- Be wary of voicemail and text message scams

If you lose your phone report it to your mobile phone provider immediately. Make a note of your phone's IMEI number (dial *#06# to get it). This could make it easier for your phone company to disable a stolen phone.