

# Checklist to Secure Your PC

## Make sure you have all the latest updates installed for Windows

Download and install all the updates for Microsoft Windows XP. If you have Automatic Updates enabled on your computer this should take place automatically. To check visit: <http://windowsupdate.microsoft.com> and follow the onscreen instructions to update Windows. At the top right of the screen will be the status of your automatic updates and a button to 'Turn on Automatic Updates' if it is currently off.

## Check that you have an Up-to-Date Internet Security Package Installed

An internet Security Package comprises mainly of an Anti-Virus and Firewall program to both scan for and remove computer viruses and prevent hackers gaining access to you PC and data. Some packages may come with Spam-Filters, Spy-Ware and Ad-Ware scanners and parental controls, but these are not essential for securing your PC. If you do not have an active Internet Security Package it is strongly advised you get one as soon as possible. Internet Security packages cost around £50 and can be obtained from most computer stores.

## Run a full Virus Scan on your PC

Check through the entire computer to make sure there are no Viruses, or other malicious programs/files on the computer.

## Secure Wireless Networks

If you have a wireless internet connection, make sure it is secure by enabling a WEP (Wired Equivalent Privacy) Key. The WEP blocks any computer that does not have the WEP key saved on it from being able to access the wireless signal, thus making it the security equivalent of a wired network.

## Watch Out For Phishing Emails

If you receive an email that looks very official and is asking for you to reply to it or click on a button or link contained within the email DON'T. All responsible Banks, Building Societies and large organizations such as Microsoft will always ask you to visit their website address as published on their printed literature. If you are in any doubt delete the email straight away.

## Look out for Secure Websites

When entering a website that is asking for account details or card numbers etc. for either banking purposes or for purchasing items from an online retailer look for the site being secure. Do not pay any attention to pictures of padlocks and logos saying the site is safe on the actual website as these can easily be faked. First look at the address bar at the top of the screen where it will usually say **http://www** if you are on a secure site it should change to **https://www** the 'S' indicating it is secure

This should become this

Also look for a small padlock to appear at the bottom right of the internet browsers window which should look

like this: Providing you have these two items the site should be perfectly safe to use.

## Useful Websites and Links

Microsoft  
[www.microsoft.com](http://www.microsoft.com)

Get Safe Online  
[www.getsafeonline.org](http://www.getsafeonline.org)

PC Care  
[www.pccareuk.com/advice](http://www.pccareuk.com/advice)

Produced by **PC Care** for **John Lewis Ltd.** Sheffield

**PC Care**

Repairs, Upgrades, Tuition & Advice

01246 410829

PCCISOS16.06.06

# Checklist to Secure Your PC

## Make sure you have all the latest updates installed for Windows

Download and install all the updates for Microsoft Windows XP. If you have Automatic Updates enabled on your computer this should take place automatically. To check visit: <http://windowsupdate.microsoft.com> and follow the onscreen instructions to update Windows. At the top right of the screen will be the status of your automatic updates and a button to 'Turn on Automatic Updates' if it is currently off.

## Check that you have an Up-to-Date Internet Security Package Installed

An internet Security Package comprises mainly of an Anti-Virus and Firewall program to both scan for and remove computer viruses and prevent hackers gaining access to you PC and data. Some packages may come with Spam-Filters, Spy-Ware and Ad-Ware scanners and parental controls, but these are not essential for securing your PC. If you do not have an active Internet Security Package it is strongly advised you get one as soon as possible. Internet Security packages cost around £50 and can be obtained from most computer stores.

## Run a full Virus Scan on your PC

Check through the entire computer to make sure there are no Viruses, or other malicious programs/files on the computer.

## Secure Wireless Networks

If you have a wireless internet connection, make sure it is secure by enabling a WEP (Wired Equivalent Privacy) Key. The WEP blocks any computer that does not have the WEP key saved on it from being able to access the wireless signal, thus making it the security equivalent of a wired network.

## Watch Out For Phishing Emails

If you receive an email that looks very official and is asking for you to reply to it or click on a button or link contained within the email DON'T. All responsible Banks, Building Societies and large organizations such as Microsoft will always ask you to visit their website address as published on their printed literature. If you are in any doubt delete the email straight away.

## Look out for Secure Websites

When entering a website that is asking for account details or card numbers etc. for either banking purposes or for purchasing items from an online retailer look for the site being secure. Do not pay any attention to pictures of padlocks and logos saying the site is safe on the actual website as these can easily be faked. First look at the address bar at the top of the screen where it will usually say **http://www** if you are on a secure site it should change to **https://www** the 'S' indicating it is secure

This should become this

Also look for a small padlock to appear at the bottom right of the internet browsers window which should look

like this: Providing you have these two items the site should be perfectly safe to use.

## Useful Websites and Links

Microsoft  
[www.microsoft.com](http://www.microsoft.com)

Get Safe Online  
[www.getsafeonline.org](http://www.getsafeonline.org)

PC Care  
[www.pccareuk.com/advice](http://www.pccareuk.com/advice)

Produced by **PC Care** for **John Lewis Ltd.** Sheffield

**PC Care**

Repairs, Upgrades, Tuition & Advice

01246 410829

PCCISOS16.06.06

# Internet Security & Online Safety

## The hazards and the solutions

Internet Security & Online Safety are becoming much talked about subjects by the government, banks, and businesses. Identity Theft and Online Fraud are becoming the fastest growing crimes in the UK and cost the UK economy over £23 Million in 2005. This figure is estimated to rise by 17% in 2006 to nearly £27 Million. Across Europe Online Fraud is estimated to be around €1 Billion (£688 Million) per year. Online fraudsters are not targeting big businesses for large sums anymore; the vast majority of these figures come from the general public. A recent survey conducted by the Internet Service Provider AOL found that as many as 1 in 20 internet users in the UK had fallen foul of some form of Internet related fraud. Fraudsters are taking small sums of money usually less than £100 from 1000's of accounts and as such can often go undetected.

So you are now aware that the problem is big, and ever growing but just how do these people steal your account details and commit fraud?

## Know Your Enemy

There are many ways fraudsters can obtain your personal details, account information and passwords, enabling them to commit fraud. Below are a few examples of how they do so.



### Trojans

Trojans are files that disguise themselves as legitimate programs (usually games, antivirus software, or computer updates). Once run, the Trojan infects the computer and can create an opening to the internet that goes unchecked by your computer's firewall. This opening can then be exploited by fraudsters to access files on your computer or place further programs on your system to assist them in their illegal activities.

Trojans can also steal passwords by either pretending to be a legitimate site asking for your password or scanning through your system for a stored passwords list.



### Key-loggers

Online banking and internet shopping are completely safe from anyone stealing your details whilst the information is being transmitted across the internet. All banks, building societies and reputable online retailers will encrypt any data before it is transmitted over the internet so that it is safe from hackers. To get around this security mechanism, a program called a key-logger infects your computer system and logs every keystroke you make on your keyboard, saving the information to a file hidden on your computer. This file can later be accessed through a vulnerability in your computer's security (usually created by a Trojan) and then scanned for any useful information such as names, addresses, dates of birth, passwords, account numbers etc.



### Phishing emails/websites.

Spoof emails are sent out in the millions and they appear to look very genuine with logos and corporate branding appearing to be from banks, building societies, Microsoft or the government departments. These emails then ask for you to fill in your account details either by replying to the email or by clicking on a link contained within the email, which brings up a website that again looks very convincing and may even ask for your username and password, to appear safe and secure. In actual fact it is simply logging your username and password so that when you continue to update your account details as the email asked, the fraudster has everything they need to access your account.

## So What Can Be Done?

There are some very simple steps you can take to help protect yourself from the dangers of the internet and minimise the risk of being a victim of Identity Theft and Online Fraud. Over the page you will find a checklist of things you can do to secure your PC and things to look out for when using the internet. There are also some addresses of websites with valuable information on the subject. If you follow the advice contained in this leaflet you should be able to enjoy the convenience of online shopping and banking without all the worry.

# Internet Security & Online Safety

## The hazards and the solutions

Internet Security & Online Safety are becoming much talked about subjects by the government, banks, and businesses. Identity Theft and Online Fraud are becoming the fastest growing crimes in the UK and cost the UK economy over £23 Million in 2005. This figure is estimated to rise by 17% in 2006 to nearly £27 Million. Across Europe Online Fraud is estimated to be around €1 Billion (£688 Million) per year. Online fraudsters are not targeting big businesses for large sums anymore; the vast majority of these figures come from the general public. A recent survey conducted by the Internet Service Provider AOL found that as many as 1 in 20 internet users in the UK had fallen foul of some form of Internet related fraud. Fraudsters are taking small sums of money usually less than £100 from 1000's of accounts and as such can often go undetected.

So you are now aware that the problem is big, and ever growing but just how do these people steal your account details and commit fraud?

## Know Your Enemy

There are many ways fraudsters can obtain your personal details, account information and passwords, enabling them to commit fraud. Below are a few examples of how they do so.



### Trojans

Trojans are files that disguise themselves as legitimate programs (usually games, antivirus software, or computer updates). Once run, the Trojan infects the computer and can create an opening to the internet that goes unchecked by your computer's firewall. This opening can then be exploited by fraudsters to access files on your computer or place further programs on your system to assist them in their illegal activities.

Trojans can also steal passwords by either pretending to be a legitimate site asking for your password or scanning through your system for a stored passwords list.



### Key-loggers

Online banking and internet shopping are completely safe from anyone stealing your details whilst the information is being transmitted across the internet. All banks, building societies and reputable online retailers will encrypt any data before it is transmitted over the internet so that it is safe from hackers. To get around this security mechanism, a program called a key-logger infects your computer system and logs every keystroke you make on your keyboard, saving the information to a file hidden on your computer. This file can later be accessed through a vulnerability in your computer's security (usually created by a Trojan) and then scanned for any useful information such as names, addresses, dates of birth, passwords, account numbers etc.



### Phishing emails/websites.

Spoof emails are sent out in the millions and they appear to look very genuine with logos and corporate branding appearing to be from banks, building societies, Microsoft or the government departments. These emails then ask for you to fill in your account details either by replying to the email or by clicking on a link contained within the email, which brings up a website that again looks very convincing and may even ask for your username and password, to appear safe and secure. In actual fact it is simply logging your username and password so that when you continue to update your account details as the email asked, the fraudster has everything they need to access your account.

## So What Can Be Done?

There are some very simple steps you can take to help protect yourself from the dangers of the internet and minimise the risk of being a victim of Identity Theft and Online Fraud. Over the page you will find a checklist of things you can do to secure your PC and things to look out for when using the internet. There are also some addresses of websites with valuable information on the subject. If you follow the advice contained in this leaflet you should be able to enjoy the convenience of online shopping and banking without all the worry.