

## Top Tips to Protect Yourself

### Don't be fooled!

Don't click links in an email which supposedly take you to your favourite online shop, banks or other trusted companies. Always type the full company address into the browser window. This will help prevent you from becoming a victim of a phishing attack. One method phishers (email scammers) use is to email fake versions of genuine voucher deals to get their victims to visit illegitimate websites. Once there they can steal your passwords, logins, credit card information, or indeed your whole identity.

### Keep your identity safe

Don't share passwords or choose one that can be easily guessed. Make sure you change them often. And where possible, use two-factor or strong authentication which combines something you know (username and password) with something you have (a credential such as a card, token or mobile phone) to verify an identity or verify a transaction.

### If it's too good to be true

Only shop at reputable websites as unknown sites can be risky. If you've found designer goods for a tenth of the price, then they're probably not real. Cybercriminals are professionals at creating websites and making them look like your favourite brand sites. Noticeable differences which can sometimes signal an illegitimate website include: big price reductions which persuade you to part with your credit card details, spelling mistakes, links or pages which don't load, insufficient product information or blurry product images. If you think it's unprofessional, then it very well may be.

### Keeping your personal details private

Never use a public or shared computer, or even a public wireless network to make a payment. It's always best to make payments from the comfort of your own home, using a private computer and network; otherwise hackers can capture your account and login information more easily, and steal your money.

### Organise your online shopping

Set-up an email account specifically to deal with online shopping. Provide as little information as possible to get the account set-up and don't use it for anything else such as online banking, business correspondence or family matters.

### Treble check the URL

Check the web page where you enter personal information such as your address or credit card details, and make sure those sites use encryption. You can tell if a page uses encryption by the web address - it will always start with "https." A green coloured address bar also indicates that the website is has an Extended Validation SSL certificate. This means that the organisation has also been rigorously authenticated and so can be completely trusted

### Protecting your bank details

If you like the convenience of online shopping, always look out for the 'padlock' icon at the bottom of the browser frame when making a payment online. This indicates that the website you are visiting uses encryption to protect you so no sneaky cybercriminals can capture your personal information.

### Checking your statements

Make sure you check your credit card statements as often as possible to look out for unexpected transactions. This is one of the best ways to know who is using the card and allows you to spot problems before they are too difficult to resolve. Credit card companies offer protection and will work with you to manage any disputed or unauthorised charges.

### Be smart with your passwords

Use a complex password for each online account you have and update your passwords regularly. Strong passwords use a mixture of numbers, symbols, and letters in upper and lower case. It doesn't need to be a word – just something that you'll remember.

### Back-up your Stuff

If your computer catches a virus or crashes, the only way to definitely ensure that you will be able to retrieve your lost data is by backing it up and doing so on a regular basis. This also means that if you mislay data or accidentally delete something, it can always be recovered. This will allow you to store old files and content on the backup and leave your valuable disk space for current content and information.

### Up-to-date internet security package

With online threats becoming increasingly more sophisticated and cybercriminals willing to jump on any social trend to spread malware, online threats are changing by the minute. Security software from a recognised name like Norton is the best and safest option when it comes to stopping malicious software installing on your PC. Try Norton Internet Security 2012 for advanced protection to surf, bank and shop online without any interruption and to make sure you're protected at all times!

Keeping the  
Stuff that  
matters safe  
online.



# Internet Safety Guide

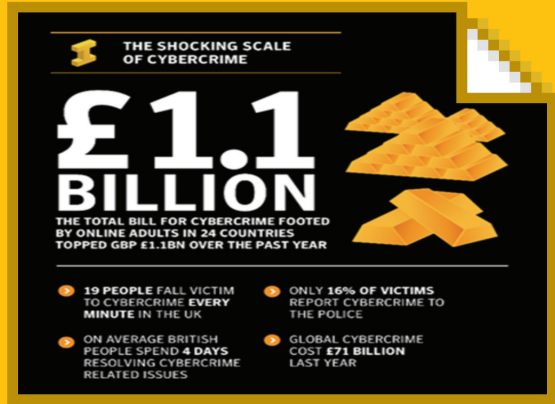
Norton in conjunction with National  
Identity Fraud Prevention Week

Mon 17th – Sun 23rd October 2011



Protecting the Stuff that matters™





Norton by Symantec has provided this downloadable internet safety guide to help people stay safe from cybercrime. Cybercrime can lead to identity fraud. This guide outlines the threat landscape, shows how online ID fraud can happen, and gives some top tips to stay safe online.

### The Threat Landscape

There have been several big cybercrime-related news stories in 2011. Whether it is large companies suffering data loss through hacks or human error, or celebrities failing to protect their personal information, it's clear that our digital and real lives have many crossover points and we need to be vigilant to protect our personal data.

Cybercriminals develop increasingly sophisticated ways to trick people out of their personal details and then make money from these details. criminals, it's important for people to think seriously about how they are protected online.

It's very difficult to resonate with what it feels like to be a victim of cybercrime until you've experienced it yourself, but as our global research shows, one million people a day are falling victim to cybercrime.

While good security software is critical, even perfect security software cannot prevent an individual from unintentionally giving too much information away.

### Quick facts according to the Norton Cybercrime Report 2011:

- Cybercrime is costing the UK on average **£474 million** a year
- 19** people fall victim to cybercrime every minute in the UK
- 51%** of those in the UK have experienced cybercrime in their lifetime
- Only **16%** of victims report cybercrime to the police
- On average British people spend around **4** days resolving cybercrime related issues
- Global cybercrime in **24** countries cost **£71 billion** last year
- 3 times** as many Brits have been victims of online crime in comparison to offline crime in the last 12 months
- The most common and most preventable type of cybercrime in the UK is **computer viruses** and **malware** with 38% of Brits having fallen victim
- Credit card fraud** and **social network hacking** are the next most common types of cybercrime affecting 10% and 6% of people respectively.

The consequences of being a victim of cybercrime can include handing over your hard-earned cash to cybercriminals, losing all your digital content, damaging your reputation, or getting malware installed on your computer. The common thread linking these tactics together is a focus on monetisation. Whether it's holding a computer for ransom, poisoning search-engine results, or exploiting social trust, the tactics used by cybercriminals continue to evolve so long as there is money to be made.

### How might your ID get stolen online?

Here are some common criminal tactics to watch out for:

#### Social networks

People can very often get caught out by giving away too much personal information online, particularly on social networks, such as a mother's maiden-name, date of birth, or sibling information. What we've noticed is that cybercriminals are building threats that are designed to trick social network users. The bad guys have realised that people are much more likely to trust a link or attachment that a friend or family member has sent them, and they are exploiting that trust.

#### Bogus websites and fake anti-virus software

Unsuspecting Internet users who enter login and password information on legitimate-looking but ultimately bogus sites also put themselves at risk, as do users who are fooled into purchasing misleading and useless fake PC software programmes. If you enter your personal details and any financial data into a site you're not 100% sure of, you're at risk.

#### Search engine results

Most people believe that the top search results are always safe, and clicking on a link to a malicious site can lead to the compromise of their computer or their online accounts when "rootkit" software is installed to monitor every keystroke that they type.