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 to 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.

Keep your mobile phone protected

Your mobile phone is full of personal information that is hugely valuable to identity thieves and cybercriminals. Always make sure that your phone is pin protected and that you have downloaded a security app which allows you to wipe any personal data should your mobile be stolen.

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 verified by independent security company Verisign, 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 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 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 Identity Fraud Prevention Week

1st - 5th October 2012

Protecting the Stuff that matters.™ Norton™ by Symantec

THE SCALE OF CONSUMER CYBERCRIME

GLOBALLY, 556 MILLION VICTIMS PER YEAR

MORE THAN THE ENTIRE POPULATION OF THE EUROPEAN UNION

12.5 MILLION IN THE UK

1.5+ MILLION VICTIMS PER DAY

27,186 IN THE UK

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 2012. Whether it is large companies suffering stolen data through hacks or human error, or friends falling victim to scams via social media, 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, in the UK it is estimated that more than 12.5million people fell victim to cybercrime in the past twelve months, suffering over £1.8 billion in direct financial losses.

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

UK CONSUMERS' SECURITY IQ

44% AREN'T 100% SURE THEIR COMPUTER IS CURRENTLY 'CLEAN' AND FREE FROM VIRUSES

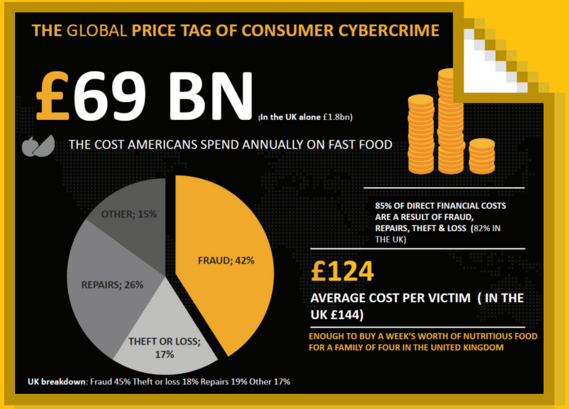
20% ONLINE ADULTS IN THE UK DON'T UNDERSTAND THE RISK OF CYBERCRIME OR HOW TO PROTECT THEMSELVES ONLINE

38% ARE ONLY USING BASIC ANTIVIRUS PROTECTION

Quick facts according to the Norton Cybercrime Report 2012:

- Cybercrime is costing the UK on average **£1.8 billion** a year
- **27,186** people fall victim to cybercrime every day in the UK
- **57%** of those in the UK have experienced cybercrime in their lifetime
- Global cybercrime in **24** countries cost **£69** billion last year
- **27%** of people in the UK do not think about cybercrime because they do not expect that it will happen to them and **17%** do not take steps to secure their personal info when accessing the internet
- **73%** of people in the UK don't use a security solution for their mobile phone
- **Social network hacking** is among the most common types of cybercrime **- 7%** of users have fallen victim to a scam or fake link on social network platforms

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 made.



THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME

£69 BN (In the UK alone £1.8bn)

THE COST AMERICANS SPEND ANNUALLY ON FAST FOOD

85% OF DIRECT FINANCIAL COSTS ARE A RESULT OF FRAUD, REPAIRS, THEFT & LOSS (82% IN THE UK)

£124

AVERAGE COST PER VICTIM (IN THE UK £144)

ENOUGH TO BUY A WEEK'S WORTH OF NUTRITIOUS FOOD FOR A FAMILY OF FOUR IN THE UNITED KINGDOM

UK breakdown: Fraud 45% Theft or loss 18% Repairs 19% Other 17%

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, but 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.