Nottinghamshire Police

Crime Prevention

Advice

Protecting yourself online

To speak to us call **101** or in an emergency **dial 999**

nottspolice nottspolice **www.nottinghamshire.police.uk**
Sign up for advice and crime alerts at **www.nottinghamshirealert.co.uk**

Introduction

Many of us use the internet as part of our daily lives, for banking, shopping, socialising and entertainment.

Follow the advice in this guide to help protect your personal data and keep you and your family safe online.

Protecting your computer

- Make sure your Wi-Fi connection is encrypted with a password so that others cannot access your internet connection.
- Ensure that your computer anti-virus software and firewall software is kept up-to-date and is enabled at all times.
- Keep your computer operating systems up-to-date and make sure you download updates regularly.
- Keep your internet browser up-to-date.
- Make sure you use strong passwords that contain a mixture of letters, numbers and punctuation. Regularly change your account passwords and don't share these with anyone. Don't use the same password for all your accounts.
- You should never reply to spam or unsolicited emails from an unknown or untrusted sender. Also, don't download attachments or click links to web pages within spam emails as these can often contain viruses.
- When you receive spam, delete the email and adjust your mailbox settings to ensure future spam emails are put into your junk folder.
- When downloading files make sure you disable file-sharing to prevent unknown individuals accessing your files.
- Ensure your webcam is disconnected and covered when not in use to prevent hackers from remotely accessing your computer.

- Register your laptop or computer on property database **www.immobilise.com** for free.
  Registering your details makes it more likely that you will be reunited with your laptop or computer if it is stolen and later recovered by us.

Protecting yourself online

- Never share your personal data such as bank details, identity details or where you live with anyone that you don't know or can't verify their details.
- Don't give your email address out to people you don't know.
- Remember people that you meet online, might not be who they claim to be. Don't arrange to meet people that you don't know. If you do agree to meet someone you've made contact with online, make sure you tell someone when or where you are going, and take someone with you if possible.
- Regularly review your privacy settings on social networking sites so that only people you know can see your information and photos.
- Be cautious with pop-ups that appear on your computer. Some pop-ups can say that your computer has been 'locked' by the police due to inappropriate material being viewed and request payment or vouchers to resolve the issue. These pop-ups are fraudulent and in no way associated with the police. If you get a pop-up like this, report it by calling 101.

Protecting yourself on social media

This information mainly applies to Facebook but should be applied across other social media sites along with the information in the 'protecting yourself online' section.

- Set your privacy settings to 'friends only'. This means only your friends can see most of your information. However, you should consider that your friends' privacy settings and lack of security could make your information available.
- Regularly check Facebook privacy terms of service. Facebook regularly changes its privacy terms of service. Make sure you check your profile and privacy settings frequently to be aware of any changes that have taken place.
- Consider who you are friends with. You should only accept people who you know well and can trust. Regularly check your friends list and keep it up-to-date.
- Disable location settings. This can prevent location details being included on photos. Don't display your address, telephone number or email address - if you have one, use privacy settings to remove these from public viewing.
- Think before commenting on and posting statuses. For example, do you want to advertise the fact that you are going on holiday? Think about your home security. Remember that others can view and share your posts. Make sure you select only the people you wish to view your information, and be aware that your postings may feature on your friends' newsfeed too.
- Monitor your photos and 'tagging'. Ensure your privacy settings are set so that only your friends can see your photos and ones you're tagged in. If you don't want to be tagged in photos, you can remove your 'tag'. You can also set your account to approve tagged photos before they appear in your newsfeed.
- Be cautious when clicking on links. Ensure you don't click on

links unless you are sure of the source. These can often contain malware. Malware is malicious software intended to harm your computer or steal personal information.

- Common harmful links claim to be from your friends asking you to watch videos and others offer 'free' software downloads. Remember, think before you click!
- Be careful with your photos. Don't post images of yourself or family members which could be used to identify you. For example house numbers, street names, place of work, car registration etc. Don't use a child's name in a caption or photo tags, or share online information about your child's life such as their school name or the names of their friends that could compromise their safety. You can restrict access to your photos or block specific people from seeing them.
- Ensure you log out. Make sure you always log off. Otherwise the next person to use the computer will already be logged into your account. However, if you do forget to log out of an active session you can remotely close the session from the account security section of the account settings page.

Shopping online

Make sure you check the following when purchasing online.

- Check that the company you're wishing to purchase from is genuine. If you're not sure, contact them to confirm before purchasing, or purchase from an alternative online retailer.
- When making online purchases make sure the connection is secure by looking for the padlock icon at the top or bottom of the internet browser. Secure web addresses should also begin with 'https'.
- Purchasing online with a credit card could provide you with

more payment protection than using a debit card. Check with your bank or use other secure payment methods such as PayPal.

- Always check your credit card and bank statements to make sure that the correct amount has been debited and there are no other suspicious transactions, which could indicate you may have been defrauded. Ensure you shred bank statements and receipts using a cross-cut shredder.
- Don't provide personal details via email. Your bank will never ask for passwords or security codes online via email.

Scams

- Most scams and frauds against companies and individuals fall into two categories:
  - Lying/deceiving in order to get someone to part with money or goods. For example, a person orders and pays for goods or a service, and it turns out to be an inferior or different product. It may not even exist.
  - Acquiring personal and financial data which is used to defraud the victim and/or used to defraud others. Usually this information is obtained either by requesting the information over the telephone or internet. The victim is tricked into revealing it to the fraudster or the victim's computer is attacked so data can be directly acquired or diverted. Once the information has been acquired it can be used to obtain goods via credit card details.

With thanks to the Metropolitan Police Service's Operation Sterling Team who have created the Little Book of Big Scams booklet to increase awareness of scams and teach you some easy steps to protect yourselves.
www.met.police.uk/docs/little_book_scam.pdf

For additional information on scams visit the A-Z of Fraud section on

the Action Fraud website.
www.actionfraud.police.uk/a-z_of_fraud

Spotting 'phishing' emails

Phishing is an attempt to trick users into revealing personal information or financial data.

- Phishing emails are not usually sent to your own name, general terms are used such as 'Dear account holder'.
- Emails tend to request immediate action such as changing your password or providing bank details, otherwise your account may be closed.
- Phishing emails usually contain spelling and grammar mistakes.
- The email address of the sender is usually different to that of the trusted company's website address.
- Links within the email direct you to an insecure website that does not feature the padlock icon or a secure web address starting with **https://**

Spam emails

- Spam emails tend to be from someone you don't know. Although sometimes if someone's email address has been compromised emails can be circulated to their address book.
- Spam emails usually contain spelling and grammar mistakes.
- Often spam emails contain special offers or promotions.
- Never click an embedded link in an email from someone you don't know or an untrusted source. These can contain viruses or take you to websites containing inappropriate material.
- **Remember, if it sounds too good to be true, it usually is!**

Advice for parents and guardians

It's important to make sure you know how to use your computer and how to look up the websites your child is accessing. Make sure you restrict or block websites and material if necessary to protect your child.

Ensure your child:

- Understands that people online might not be who they claim to be.
- Doesn't access private chat rooms.
- Knows never to meet up with someone they have contacted online without your permission.
- Knows not to open emails or files sent from an unknown or untrusted sender.
- Knows not to respond to messages that are sexually suggestive, provocative or threatening.
- Thinks carefully before commenting or posting photos of themselves online and on social networking sites.
- Knows to talk to you, a teacher or someone else they can trust if they are worried about something they have seen or been sent online.
- Knows to talk to you if they are being bullied online.

How to report a problem online

- If you or your child sees inappropriate content on a website or social networking site, make sure you report it directly to where the content appears online.

- If the content relates to a crime committed in the UK, report it to the police on **101**. In the case of an emergency always dial **999**.
- Contact your Internet Service Provider.

How to report fraud and get advice

You can get more advice and report suspected fraud to Action Fraud UK:

- Call **0300 123 2040**
- Visit the Action Fraud website **www.actionfraud.police.uk** and report the fraud online.

For more online safety advice visit **www.getsafeonline.org**

PROTECT REGISTER IT

Register your property for FREE and improve your chance of getting it back if it is lost or stolen

IMMOBILISE PROPERTY CRIME

www.immobilise.com

For more infromation contact
Crime Prevention Unit
Nottinghamshire Police
Sherwood Lodge, Arnold
NG5 8PP
crime.prevention@nottinghamshire.pnn.police.uk