KEEPING CHILDREN SAFE

Technology – not least the internet – plays such a key role in our lives that it's a positive move to introduce children to it in a careful and appropriate way.

Young people are naturally curious and like to explore … it's how they learn and develop. For them, the internet can be a fascinating and exciting place – not least the ability to easily access entertainment and interaction with others.

However, the internet is relatively unpoliced, making it vital to safeguard your kids against issues like inappropriate contact which may lead to abuse or grooming, adult or malicious content or the temptation to share private information or images … to name but a few.

Essentially, our advice on bringing children up in the digital age falls into three categories:

- Working with your children as they grow and develop to guide them in the right direction, understand what they are doing and being on hand to answer any concerns.
- Having technical measures in place such as parental control software and network and device-level filters in place.
- Being aware of the latest developments in apps, social networking and gaming by reading up on them and speaking to your kids and other parents.

Because of space limitations, this advice is very broad, so for more in-depth information on keeping your children safe on the internet please visit **www.getsafeonline.org** and select ***Safeguarding Children***.



RUNNING YOUR BUSINESS

Running a business is challenging enough without having to deal with fraud and other online and data-related issues.

Here are some basic rules to safeguard your business:

- Run regular online safety and information security awareness sessions for all employees. Get staff to question and challenge things that seem irregular.
- Ensure physical access to computers and servers is strictly controlled.
- Introduce and reinforce rules about mobile devices, including keeping them safe, use of public internet and secured home access, and the use of employees' own smartphones and tablets in the business.
- Perform regular backups to a reputable service, preferably one that is in the cloud and easily accessible.
- Enforce strict access to company, employee and customer data.
- Make sure you and all staff can spot the signs of a social engineering scam and know how to avoid the company being defrauded in this way.
- Have a software policy firmly in place including usage, updates, licences and what to do with redundant programs and apps.
- When disposing of redundant computers, servers and mobile devices, ensure all data is thoroughly erased (not just deleted) to ensure it doesn't fall into the wrong hands.



REPORT IT

If you, a family member or your business suffer fraud, identity theft or abuse, you should report it immediately to avoid repeat victimisation and prevent it happening to others.

This is the case however small the amount you have lost or the abuse suffered.

Report the problem to the website, social network, ISP or organisation used by the fraudster, identity thief or abuser to commit their crime. If you receive a fraudulent email, phone call, text or social media post, report it to the organisation being falsely represented (for example your bank or HMRC).

Report actual or attempted fraud to Action Fraud at **www.actionfraud.police.uk** or by calling Action Fraud on **0300 123 2040**.

MORE ADVICE

For comprehensive, simple, free advice on keeping yourself, your family, your finances and your workplace safe online, please visit:

www.getsafeonline.org



www.westsussex.gov.uk/campaigns/staying-safe-online

CYBER AWARE

We work closely with the Government's cyber security campaign, Cyber Aware, which provides advice for small business and individuals to help protect themselves from cyber crime. To supplement the advice in this leaflet, please note the Government's advice on two key areas of online safety.

Use three random words to create a strong password



Numbers and symbols can still be used if needed, but three random words provide a good compromise between strength and memorability. Never share your passwords with anyone and ensure you use different passwords for your most important accounts, which are your email, online banking and social media.

Always download the latest software and app updates

They contain vital security upgrades which help protect your device from viruses and hackers. On top of having the most up to date security, software updates also usually include new features and functionality – so why wouldn't you install them?



This is based on advice from the National Cyber Security Centre.

www.cyberaware.gov.uk

GET SAFE ONLINE: WORKING TOGETHER WITH...

TESCO, HSBC, KASPERSKY, airbnb, LLOYDS BANK, HALIFAX, BANK OF SCOTLAND, creativevirtual, Standard Life, PayPal, TalkTalk, M&S BANK, Royal Mail, Gumtree, Royal Bank of Scotland, NatWest, first direct, HM Government, NPCC, CITY OF LONDON POLICE, NATIONAL TRADING STANDARDS eCrime Team, CYBER AWARE, METROPOLITAN POLICE, Ofcom, NCA National Crime Agency, ActionFraud, VICTIM SUPPORT, STOP FRAUD, cifas

Get Safe Online in WEST SUSSEX



YOUR ESSENTIAL GUIDE TO STAYING SAFE ONLINE

www.getsafeonline.org

www.westsussex.gov.uk/campaigns/staying-safe-online

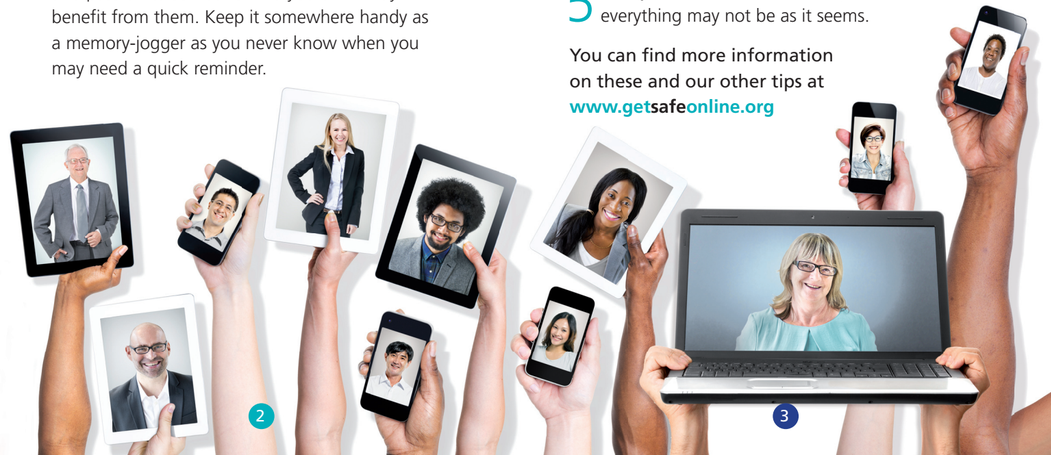
INTRODUCTION

With most of us relying on the internet to one degree or another to communicate, manage our finances, obtain products and services and enjoy entertainment, it really is a wonderful resource.

Unfortunately, however, things can and do go wrong online, with an increasing number of people of all ages and backgrounds being affected by fraud, identity theft and abuse – some of it originating in the UK, but a great deal from abroad.

There are simple technical steps we can all take to protect ourselves, but most problems can be avoided by making sure we always follow some simple rules and use our common sense.

This booklet provides some useful tips which we recommend you read and follow when online, and pass on to someone who you think may benefit from them. Keep it somewhere handy as a memory-jogger as you never know when you may need a quick reminder.



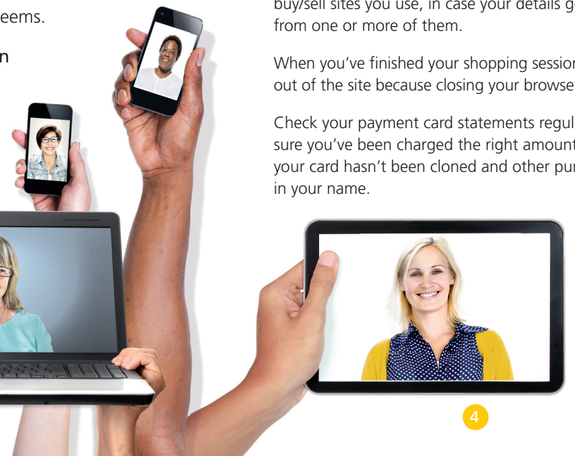
2

PROTECTING YOUR DEVICES

Here are some 'golden rules' you should follow whenever you're online. That way, you have a better chance of staying safeguarded.

1. Choose, use and protect your passwords carefully, and use a different one for every account.
2. Ensure you always have internet security software/app loaded, kept updated and switched on.
3. Never reveal too much personal or financial information … you never know who might see it, or use it.
4. Don't click on links or open attachments if the source isn't 100% known and trustworthy.
5. Take your time and think twice, because everything may not be as it seems.

You can find more information on these and our other tips at **www.getsafeonline.org**



3

SHOPPING

If you're buying online from a retailer or individual you're not familiar with, make sure they're reputable and honest by getting recommendations or customer reviews.

Is the payment page secure? There should be a padlock symbol in the browser window frame which appears when you attempt to log in or register, and the address of the page should start with 'https://' The 's' stands for 'secure'.

Unless you know the seller personally, never pay by direct transfer into their bank account. This is a common scam and you'll have little chance of getting your money back.

Don't buy online when you're using unsecured Wi-Fi, such as a hotspot in a café or hotel. Logging in to a hotspot is no indication it's secure, so use 3G/4G instead, or wait until you get home to your secure Wi-Fi.

Remember that paying by credit card offers greater protection from fraud, non-delivery and dishonoured product warranties.

Use different passwords for the shopping, auction and buy/sell sites you use, in case your details get hacked from one or more of them.

When you've finished your shopping session, always log out of the site because closing your browser isn't enough.

Check your payment card statements regularly to make sure you've been charged the right amount, and check your card hasn't been cloned and other purchases made in your name.

4

FINANCE

Never disclose passwords or other personal information in response to an email, phone call, text, social media post or letter purporting to be from your bank or other official organisation, however genuine they may seem. Real organisations never ask you for this information. Any communication from banks will use your actual name (not 'Sir', 'Madam' or 'Customer') and possibly another verification of authenticity such as your postcode or part of your account number.

However desperate you are to check your account or make a payment, don't bank online when you're using unsecured Wi-Fi, such as a hotspot in a café or hotel. Logging in to a hotspot is no indication it's secure, so use 3G/4G instead, or wait until you get home to your secure Wi-Fi.

Only ever visit your bank's website by entering the address into your browser or using a bookmark you have created using the correct address.

Don't lend your payment cards or reveal their PINs – to anybody else, however trustworthy they may seem.

Always check your statements, and if you notice any unusual transactions report them immediately.

You never know if the person behind or beside you is dishonest. You need to be aware of 'shoulder surfers' viewing your computer or mobile device screen, or at the ATM. Also, if you spot anything irregular at the ATM like an unusual card slot or fascia, don't use it, but report it to your bank.



5

SOCIAL MEDIA

Be careful who you accept as friends or contacts, especially if you get a request from people you don't know personally. They might not be who they seem, and could potentially cause you harm.

Don't get persuaded into actions or thoughts that you're not comfortable with, or that you know deep down are wrong. Sending intimate images and being persuaded into extremist behaviour are just two examples.

Be careful about what private or confidential information about yourself or your family you reveal in posts or profiles, that could let criminals piece together a picture of you. Phone numbers, pictures of your home, workplace or school, your address or birthdays are all examples.

What goes online stays online. Don't say anything or publish pictures that might offend or embarrass you or someone else, get you into trouble or mean lost opportunities now or at any point in the future.

Review your privacy settings and friend/contact lists regularly.

Set up a separate email account to register and receive mail from the site. Consider a Hotmail, Yahoo! Mail or gmail account as these are fast and easy to set up.

Never post comments that are abusive or may offend individuals or groups of society. Trolling can be very upsetting for the victim, and some cases may be a criminal offence.

Be on your guard against phishing scams, including fake friend requests and posts from companies inviting you to visit other pages or sites.



6