Keeping Children Safe

- Talk regularly with your child about what they're doing online. Get to understand new technologies and trends. Discuss stranger danger, inappropriate content, bullying, oversharing personal information and spending too much time on their devices.
- Discuss and agree boundaries and rules including time limits and appropriate online usage.
- Apply parental control software and apps on computers, mobile devices and consoles, privacy features on social media sites, safety options on search engines and safe location settings on devices and apps. Turn on ISP family filters.
- Explain and encourage safe searching, websites and apps. Check what your child is watching and sharing on streaming sites like YouTube and TikTok.
- Social networking, picture/video sharing, gaming and other sites and apps have lower age limits for a reason. Download apps only from official app stores. Add your own email address when setting up accounts and apps for your child.
- Ensure your child's video call safety by updating to the platform's latest version, following its safety advice and making sure call invitations and responses aren't shared outside the call group.
- If your child is into online gaming, make them aware of things like chatting to strangers, in-game purchases (including using your credit card) and spending too much time online.
- Advise your child that they shouldn't believe – and share – everything they read or see online.

Running a Business

Running a business is challenging enough without having to deal with fraud and other online and data-related issues. Here are some basic tips:

- 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 secure 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 attempted fraud, data theft or other scams and deal with them appropriately.
- 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.

For more information on keeping your business protected, visit **www.getsafeonline.org/business**

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. In Scotland, report fraud to Police Scotland by calling 101.

If you have received a suspected phishing email, forward it to the NCSC's Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk

More advice

Thank you for visiting our Get Safe Online live event. We hope you have found our advice useful.

In this leaflet, we have featured a few areas in which the internet is very widely used, and which we are frequently asked questions about at events like the one you have visited.

For comprehensive, simple, free advice on keeping yourself, your family, your finances and your workplace safe online, please visit **www.getsafeonline.org**

Check a website

The Get Safe Online website features a free, easy to use tool where you can check if a website or link is a scam, phishing or legitimate, simply by entering its address. Visit **www.getsafeonline.org/checkawebsite**

www.getsafeonline.org

OFFICIAL PARTNERS

TESCO, HSBC, Standard Life, Royal Air Force, Lloyds Bank, Halifax, Bank of Scotland, airbnb, M&S Bank, NatWest, Royal Bank of Scotland, ClearScore, first direct, creativevirtual, NPCC, City of London Police, cifas, Europol EC3, Metropolitan Police, Ofcom, neighbourhood ALERT, ActionFraud, Victim Support, Llywodraeth Cymru Welsh Government, National Trading Standards eCrime Team

Get Safe Online in

West Sussex

YOUR ESSENTIAL GUIDE TO USING THE INTERNET WITH SAFETY AND CONFIDENCE

www.getsafeonline.org

Most of us rely on the internet to one degree or another to communicate, manage our finances, purchase products and services, download entertainment and much, much more.

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 also from abroad.

There are simple technical steps we can all take to protect ourselves from these issues, but most can be avoided by making sure we know how to identify and deal with them.

This leaflet provides straightforward, easy-to-follow tips that you can use every day and pass on to family members, friends, colleagues and other internet users. They are divided into different headings so that you can find the advice quickly and easily.

Let's start with some back-to-basics dos and don'ts...

- Devise the most secure passwords you can. You could start by joining three random words with upper and lower case letters, and mingling in numbers and symbols. Use a minimum of 12 characters.
- Never share passwords, and use a different one for every account or website, in case one gets hacked.
- Ensure you always have internet security software/app loaded, kept updated and switched on.
- Download software, operating system and app updates when prompted. Better still, set them to update automatically.

- Never reveal more personal or financial information than is essential, whether on a website or in response to an email, text, message or call.
- Don't click on links in emails, messages or posts – or open attachments – if the source isn't 100% known and trustworthy.
- Don't use public Wi-Fi hotspots when doing anything confidential online.
- Stay alert, take your time and think twice, because everything may not be as it seems and if it seems too good to be true, it probably is.

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

Buying Online

- 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. This applies whether you're buying products, tickets, holidays and travel, vehicles or anything else.
- 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 your data, a secure broadband dongle or reputable VPN 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.

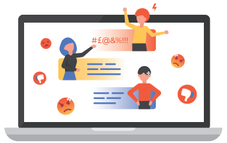
- When you've finished your shopping session, always log out of the site because closing your browser isn't enough.
- Check bank statements regularly to make sure you've been charged the correct amount, and check your card hasn't been cloned and other purchases made in your name.

Banking & 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. Genuine 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 Wi-Fi hotspot, for example in a café or hotel. There's no guarantee it's secure, so instead use your data, a reputable VPN or a mobile broadband dongle, 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.
- Who's behind or beside you? You need to be aware of 'shoulder surfers' viewing your 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.

Using Social Media

- Be careful who you accept as friends or contacts, especially if you get a request from someone you don't know personally. They may not be who they seem.
- Review your privacy settings and friend/contact lists regularly.
- Be careful about what private or confidential information about yourself or your family you reveal in posts or profiles, that criminals could piece together. Phone numbers, pictures of your home, workplace or school, your address or birthdays and children's names 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.



- 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.
- 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 on your guard against scams, including fake friend requests and posts containing links to other pages or sites.