Scam
Protection

Ten top tips to keep you and your devices secure

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you hoping you'll let your guard down for just a moment.

They can contact you by phone, email, text, letters, on social media, or in person. They will try to trick you into parting with your money, personal information, or buying goods or services that don't exist.

1. **Verify any unexpected contact is genuine by using a known number or email address to contact organisations directly.**
   Is this caller who they say they are? After hanging up, wait five minutes and make sure you can hear a dial tone before making any other calls, or use your mobile. **Never allow** an unsolicited caller remote access to your computer or devices.

2. **Don't be pressurised into sending money.**
   Stop, think and check with a trusted source or person. It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you. Have confidence in yourself, if it feels wrong to you – it probably is.

3. **Use someone you know and trust for shopping & other essentials.**
   Don't hand money over to someone on the doorstep.

4. **Authorities like the Department for Work and Pensions (DWP) and Her Majesty's Revenue and Customs (HMRC) will never ask for banking details like your password or PIN on the phone or in person.**
   You will **never be asked** to move money to a 'safe account'. Police or banking representatives will never ask you to help in an investigation by moving money or withdrawing funds.

5. **Check IDs and get them verified.**
   Genuine officials will be more than happy to wait while you verify their ID.

6 **Pick strong passwords.**
Choose three random words with a mixture of upper/lower case, numbers and special characters. Do not use the same password across sites. Enable Two Factor Authentication (2FA) on your accounts and devices that offer it, this provides a second layer of security.

7 **Be wary of phishing scams.**
Don't click on any links or attachments in unexpected emails.

8 **Social Media.**
For those of you who use social media, make sure that it is set up correctly, review your privacy settings to ensure your profile is appropriately locked down.

9 **Use antivirus and ensure you are using the latest versions of software, apps and operating systems on your phones, tablets, desktops and laptops**. Update these regularly or set your devices to automatically update so you don't have to worry.

10 **Backups.**
Always back up your most important data such as your photos and key documents to an external hard drive and/or cloud storage.

Report suspicious texts by forwarding them to **7726**, which spells SPAM on your keypad.

If you think you've received a phishing email forward to **report@phishing.gov.uk**

If you think you've fallen victim to a scam contact your bank immediately and report it to Action Fraud by visiting **www.actionfraud.police.uk** or calling **0300 123 2040**

☎ **101** in an emergency always call 999
www.derbyshire.police.uk

@DerbysPolice | Find us on Facebook | Follow us on Instagram

Making Derbyshire Safer **Together**