Scam Protection

Ten top tips to keep you and your devices secure

Verify an unexpected contact is genuine by using a known phone number, email address or website to contact the organisations directly –

Is this caller who they say they are? After hanging up wait five minutes and make sure you can hear the dial tone before making any other calls, or use your mobile. Never allow an unsolicited caller remote access to your computer. Do not give them your Wi-Fi or computer passwords.

Don't be pressured into sending money -

Stop, think and check with a trusted source or person. It is ok to reject, refuse or ignore requests. Only criminals will try to rush or panic you into sending money. Have confidence in yourself, if it feels wrong then it probably is.

Use someone you know and trust for shopping and essential items -

Do **NOT** hand over money to someone on your doorstep who you do not know.

Check IDs and get them verified -

Genuine officials will be more than happy to wait while you verify their identification.

Authorities such as the Police, Department for Work and Pensions (DWP) and Her Majesty's Revenue and Customs (HMRC) will never ask for your personal details, banking details, password or PIN number -

You will **NEVER** be asked to move money to a 'safe account'. The Police or a banking representative will never ask you to help in an investigation by moving money or withdrawing funds.

Use STRONG passwords and enable 2FA -

Choose three random words with a mixture of upper/lower case, numbers and special characters. Do **NOT** use the same passwords across all of your online accounts. Enable Two Factor Authentication (2FA) on your devices and accounts as this provides an extra layer of security.

In an emergency call **999**
For non emergencies call **101**

www.northants.police.uk

Northamptonshire Police

Fighting crime, protecting people

Be wary of phishing and scam emails. These are emails designed to trick you into providing your personal and/or financial details -

Do **NOT** click on any links or attachments in unexpected emails. Always verify that the contact is genuine by using a known number, email address or website.

Social Media -

Make sure that you have your accounts set up correctly, review your privacy settings to ensure that you have the best protection and keep these apps updated.

Use an antivirus and ensure that you are using the latest versions of software, applications and operating systems on all of your devices -

Keep these updated – set your devices to update automatically so you don't have to worry about remembering.

Backups -

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

Contact Cyber Investigations

cyberprotect@northants.police.uk

Follow us on Twitter

@NorthantsCyber

For further advice and guidance visit

www.northants.police.uk

www.ncsc.gov.uk

www.internetmatters.org

www.getsafeonline.org

www.gov.uk

Report suspicious texts by forwarding them to 7726

If you think you have received a phishing email forward it to report@phishing.gov.uk

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

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

TAKE FIVE TO STOP FRAUD

takefive-stopfraud.org.uk

Northamptonshire Police
Fighting crime, protecting people