







Social media checklist







THINK BEFORE YOU SHARE

-  Is it inappropriate or embarrassing – for yourself or for others?
-  Would it be OK if your manager saw it, or it was shown in a meeting?
-  Once you have posted something, be aware it can quickly go out of your control. Anyone can copy, screenshot, share and use your information how they wish, even if you later delete it.
-  Have you shared your mother’s maiden name, first school you went to or first car? These may all be answers to your security questions on various platforms.
-  Have you have ‘liked’ a particular bank on social media? That could show a fraudster who you bank with – and you could receive a scam call from someone pretending to be from your bank.
-  Be careful when ‘checking in’ and letting the world know your location. This can allow a criminal to work out patterns of behaviours, which could compromise your home and online security. ‘Checking in’ to your local pub or posting pictures of your children in their school uniform could enable people to work out where you live. Anything that reveals you are away from home could also be a tempting offer for burglars.





IS YOUR SOCIAL MEDIA PRIVATE?

-  Make your account private to enable you to approve who follows you and what you get tagged in. This simply puts you in full control of what happens on your account.
-  ‘Hide’ your friends list to protect their security too and help prevent cloning.
-  Don’t add or accept friend requests from people you don’t know. Not everyone using social media is necessarily who they say they are. Take a moment to check if you know the person, and if the friend/link/follow is genuine.
-  Check your friend or followers list. Do you REALLY know everyone? Go through your existing friends and followers, and remove anyone that you don’t know or that don’t check out as real.



HAVE YOU GOOGLED YOURSELF?

-  Type your full name and where you live into Google. How much information do you find? Remember - if you can find it, then so can other people.
-  Check that your email address and mobile number cannot be used to find your social media accounts in a search engine, and change your security settings so that your profile can’t be either.

*** PASSWORDS

- ✓ Use three random words, e.g *tablechairbrush*, and have a different password for each of your social media accounts.
- ✓ You can use numbers, capital letters and special characters to make passwords even stronger e.g. *RedConnect!pug27*
- ✗ Avoid using information that may be in the public domain or easily worked out from social media or ancestry sites, such as your mother's maiden name or your place of birth.
- 💡 Need help to remember passwords? Use a password manager to securely store passwords.
- ! Make sure your account recovery details are up-to-date.

🛡️ TURN ON TWO FACTOR AUTHENTICATION (2FA)

- 🔒 2FA is a free security feature that gives you an extra layer of protection online and stops cyber criminals getting into your accounts - even if they have your password.
- ! 2FA reduces the risk of being hacked by asking you to provide a second factor of information when you log in, such as getting a text or code, to check you are who you say you are.
- 💡 Set up alerts to notify you that an unknown device has logged into your account (this might be already set up).

📄 USEFUL RESOURCES

Follow **@SYPFraud** on Twitter

National Cyber Security Centre:
www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

Get Safe Online: www.getsafeonline.org/social-networking/