SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit

NHS England and NHS Improvement

Remote Working

With many people now having to work from home there are extra steps we can all take to ensure that we remain cyber aware, and protect ourselves and the NHS from cyber crime.

Keep accounts secure

Strong Passwords: Ensure that you have strong, unique passwords for all of your accounts. We recommend using three random words e.g. **TrainBasketTree**

You can make this stronger using special characters, capital letters and numbers e.g. **TrainBasketTree --> Tra1nb@sk3tTr3e!**

Password Managers: To avoid password overload, consider password managers, but make sure you research a reputable one which meets your needs.

Default passwords: Change the default password for all of your devices (e.g. routers, smart devices) and accounts. Default passwords for these devices are often available online.

Two-Factor Authentication (2FA): Switch on 2FA for all accounts where possible. This means that as well as your username and password, you'll need a one time code, often delivered via text or an app. Office365, online banking and most social media platforms are examples of programs which allow 2FA.

Keep devices safe

Working from home means that you might have work devices, paperwork and data in your home environment. It's important to keep all of these physically safe as well as digitally.

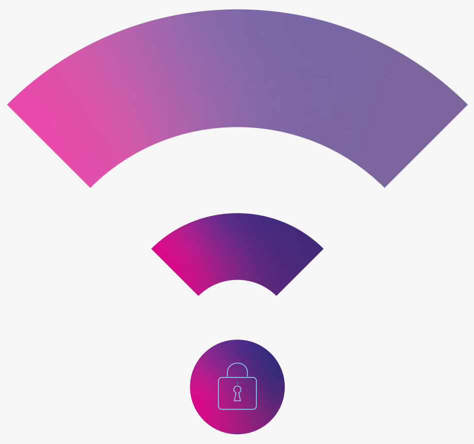
- Store items in a safe place when not in use and only use them in areas where they cannot be read or used by other members of your household.
- If you have to travel, store items safely and don't leave them unattended.

- For devices which store personal sensitive data, consider encrypting them. If they then get lost or stolen, the data cannot be accessed. You can encrypt devices such as laptops, mobile phones and USB sticks.

Use secure Wi-Fi connections

When connecting to the internet, always make sure you use a secure connection.

- Don't use public Wi-Fi which doesn't ask you for login credentials. You don't know who these networks belong to, even if they're called something like 'hotel_guest'.
- If you know a network genuinely belongs to someone e.g. the cafe you're working in, then these networks are generally ok to use, but not for anything sensitive. Sensitive tasks may include online banking or sending work documents.



Two options for connecting securely include:

- Use a reputable **Virtual Private Network (VPN)**, which encrypts your connection. If you don't currently have a VPN, do your research to find a reputable one which meets your requirements.
- Use your mobile data connection (**3G, 4G, 5G**) and tether your laptop to it, if you need to use it.

Communication is key

Just because you aren't working alongside colleagues doesn't mean that communications should stop.

Always follow process including any segregation of duties.

Ensure that if you receive an email you aren't expecting, always call the person involved to verify the communication is genuine.

For more information on staying secure whilst working remotely, see the National Cyber Security Centre (NCSC)'s guidance at https://www.ncsc.gov.uk/guidance/home-working

swrocu.police.uk/cyber
@swrccu
SW Regional Cyber Crime Unit