Data security – a guide to the basics

The COVID-19 pandemic is changing what we do and how we do it. If you've never had to think about keeping other people's personal data secure, this guide will help.

1. **Lock it away when not in use.** Keep anything with personal data on it locked away in a cabinet or drawer when you're not using it. Things like laptops, tablets, paperwork and USB sticks. This will reduce the risk of things being lost or stolen.
2. **Keep software up to date.** Don't be an easy target for hackers. Keep your security software up to date to make it more difficult for them to get in.
3. **Communicate securely.** If you need to share data with others then choose a secure messaging app or online document sharing system. If you have to use email, which isn't always secure, consider password protecting documents and sharing the passwords via a different channel, like text.
4. **Be extra vigilant about opening web links and attachments in emails or other messages.** Don't click on unfamiliar web links or attachments claiming to give you important COVID-19 updates. We're seeing a rise in scams so follow the National Cyber Security Centre's (NCSC) guidance on spotting suspicious emails.
5. **Back up your information.** Keep a separate copy of any important information to avoid losing access to it. Online storage is an easy way to keep a remote copy of your data should you need it. Or keep a copy on a separate hard drive or USB stick. Just remember to set a strong password to protect your information and lock it away when you're not using it.
6. **Use strong passwords.** Whether using online storage, a laptop or some other technology it's important to make your passwords hard to guess. The NCSC recommends using three random words together as a password (eg. 'coffeetrainfish' or 'walltinshirt'). Make sure you use different passwords for different services too.

For more guidance, visit ico.org.uk/coronavirus