7 SIMPLE STEPS TO PROTECT YOURSELF ONLINE

YORKSHIRE BUILDING SOCIETY

These are 7 simple ways you can protect yourself from becoming the victim of online security scams. They are recommended by the National Cyber Security Centre (the police/security services organisation who look after cyber security for UK organisations).

1. VIP EMAIL

Your email account is probably your most important digital asset. It's central to many other processes like password reset or recovery. So it's crucial to look after it and give it a good, strong, unique password.

2. KEEP IT WEIRD

Making passwords unpredictable is a good idea. The best advice is to use three unconnected words together, and make a long password that's easy to remember but hard for anyone else to guess. Add numbers or special characters to make it even harder to guess.

Also, it's important that you consider the accounts you already have, and review the services you use the most and update your passwords with unusual ones.

3. PASSWORDS

No one likes remembering passwords.

Using password managers, or letting the browser manage them is a good, safe solution if you can't remember your passwords.

This also means that you can use very long and complex passwords, which are difficult to attack.

4. DOUBLY SECURE

Two factor authentication provides an extra layer of security. If you have the option to set this up on a website or service, you should do so. This means that when you log in, you'll be asked to provide a code or a number from a text message (or something similar).

So in the future you'll need something you know and something you have to login, which is much safer.

5. STAY UP TO DATE

It's a good idea to Install the latest software and keep phones or PCs up to date. Cyber criminals exploit flaws and weaknesses, so it's a good idea to fix these problems.

Software vendors like Microsoft and Apple put lots of resource into finding bugs and fixing them, so it makes sense to take advantage of this work by applying their updates.

6. SAFETY WHILST SLEEPING

Why not make all that updating easy?

By setting phones to automatically update any software upgrades. Most of the time, it'll just apply the updates during the night. So when you use it in the morning, it'll be up to date.

6. HAVE A BACK-UP PLAN

If a device is stolen or compromised by a cyber criminal, data could be lost, damaged or held to ransom. So it's important to keep a copy of all valuable data by backing up, so that you can access it if you need to.