8. Secure Websites

Before you start entering your personal information online, always check for the padlock symbol. This symbol must appear in the address bar for it to be legitimate. That way, you know you're on a secure website.

9. Keep a Backup

Imagine if your device gets stolen or lost for whatever reason or if your device becomes infected with malware. All your photos, videos and important documents could be gone forever. "If only I had made a backup", you might say.

One way to preserve all your files is to save everything in the cloud. 'Cloud' storage is storage space on the internet and you may already have some free space through your ISP (internet service provider).

Cloud storage has the advantage that the backup is not at your house where there is a risk of flood, fire and theft. Even the cloud itself is backed up so there is little danger of losing your files.

For help with online services please email:
library.digital.support@westsussex.gov.uk

west sussex county council

LET'S GET DIGITAL

West Sussex Library Service

02.22

Help With...

Staying Safe Online

This short guide will introduce you to some top tips for staying safe online. It will highlight some of the risks to be aware of when using online products and services like email or online shopping. For more comprehensive guidance on anything outlined below, please see the following websites.

⇒ www.getsafeonline.org/westsussex/
⇒ www.westsussex.gov.uk/staying-safe-online/
⇒ ncsc.gov.uk/cyberaware/home

It is possible to do lots of things online, from shopping to staying in touch with loved ones, online banking and even dating. But what's at stake if it all goes wrong? And what precautions can we take to minimise the risks and stay safe online?

1. Passwords

Passwords are your first line of defence so it's really important to use passwords that only you know and that can't easily be guessed or worked out by someone or something else. This is called creating strong passwords.

- Create strong passwords - use three random words with capital letters and symbols e.g. Kettle2Cup$Tea, 10RosesCatNewspape%
- Never share your passwords with other people
- Never use the same password for multiple websites
- Consider using a password manager - an app that remembers all your passwords for you.

2. Software Updates

Cyber criminals can use weaknesses in software to attack your device. Updates are designed to fix these weaknesses and installing them as soon as possible will help keep your device secure.

Set your software to update automatically or if you are concerned that the update message may be fake go to your software settings and update it manually.

So when you get a prompt to update something on your device, don't ignore the message but be cautious - it could be malicious.

3. Security Software

Security software (also known as anti-virus software) helps to protect you from a range of threats that could put you at risk from hackers and fraudsters. Apart from security features that come with your device, a number of third-party products are available. To get the best protection from any security software, you need to keep it up to date.

4. Device Security

It's a good idea to use the security features built into your device to stop anyone else gaining immediate access to it. If you don't do this, it is like going out and leaving your front door wide open - a potential gold mine for thieves and hackers.

Here are the most common methods for keeping your device locked.

- PIN (Personal Identification Number) or Password - you type in a code
- Pattern lock - you draw a pattern on the screen with your finger
- Fingerprint scanner - you hold your finger on the screen
- Facial recognition - you look into the camera lens
- Two Factor Authentication - e.g. a code sent to your phone etc.

5. Official Apps

It's always best to go for genuine apps - that way you know they are safe to use. By choosing genuine, official apps from Google Play and the App Store, you can reduce the risk of getting a virus on your device.

All the apps on the App Store have been vetted by Apple to make sure they're safe. If you decide to use illegitimate apps you risk introducing malware (malicious software) onto your device so it's even more important to have security software installed. Malware can be very dangerous because it can trick you into inadvertently giving personal information to thieves and fraudsters.

6. Wi-fi

Avoid using public wifi if you plan to go on any websites where you'll be entering personal information like email addresses, passwords, credit card details or where you'll be doing online banking.

This is because it's very easy for criminals to tap into a public wi-fi network and see all the information you are entering. You can never be sure public wi-fi is private.

7. Email

When you receive an email, always assume it may ***not*** be from the person it says it's from. Fraudsters are very skilled at sending 'phishing' emails where they impersonate trusted organisations like your favourite online shop or your bank. So, when you're reading an email, be very cautious about clicking on any links in the email or downloading an attachment unless you are 100% sure you know who the email is from. You should also take care with links in SMS text messages.