u3a learn, laugh, live Higham and Rushden

Registered Charity Number 1164952

Security

Online safety

Before setting foot in the big online world it is essential to ensure that your computer has security software to keep you safe from malware (a general term for all sorts of online threats).

Install security software on your computer.

- Anti-virus software will look for and remove viruses before they can infect your computer.
- Anti-spyware software prevents unwanted adverts from popping up and stops programs tracking your activities or scanning your computer for private data, such as credit card numbers or bank details.
- A firewall will provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic.

Windows 10 and 11 come with Microsoft Defender antivirus, part of Windows Security. This is not the highest-ranked antivirus software in tests but it does a reasonable job, costs nothing, and does not keep suggesting you upgrade to a paid version. Windows Security also monitors your device and turns off components when a third-party application is installed since it is not recommended to run 2 AV programmes in case they counter each other.

The most popular paid security suites are McAfee, Norton, Kaspersky (although as this is Russian it is less popular these days), Eset, Panda, Total and Bitdefender, and there are paid versions of most of the free third-party programmes such as Avast, AVG, Avira (and many, many more).

If you only go online occasionally it is well worth updating your security software at the beginning of your internet session before you start surfing the web. If you are a regular browser your software should update itself in the background without needing your intervention too often.

Passwords

Keep your passwords strong. Setting up strong passwords is one of the simplest, most effective things you can do to stay safe when you're on the internet. Avoid passwords made up of common words, numbers or keyboard patterns (such as 'password' or '123456'), and don't include personal information, like your name, date of birth or any family member's details. Use different passwords for different accounts. 2 random, unconnected, words strung together (like “ovenpainting”) is a good start, and changing one or more letters to numbers (a to 4, o to 0, e to 3 for example) or adding a special character like an exclamation mark makes the password even stronger. Foreign words are also much more difficult for others to guess.

That is of course the official version and most of us ignore some or all these rules! It is possible to find password management software which will generate and store different passwords for all the sites into which you regularly have to log. Most are online programs meaning that they can be accessed from different devices as long as you can remember the master password.

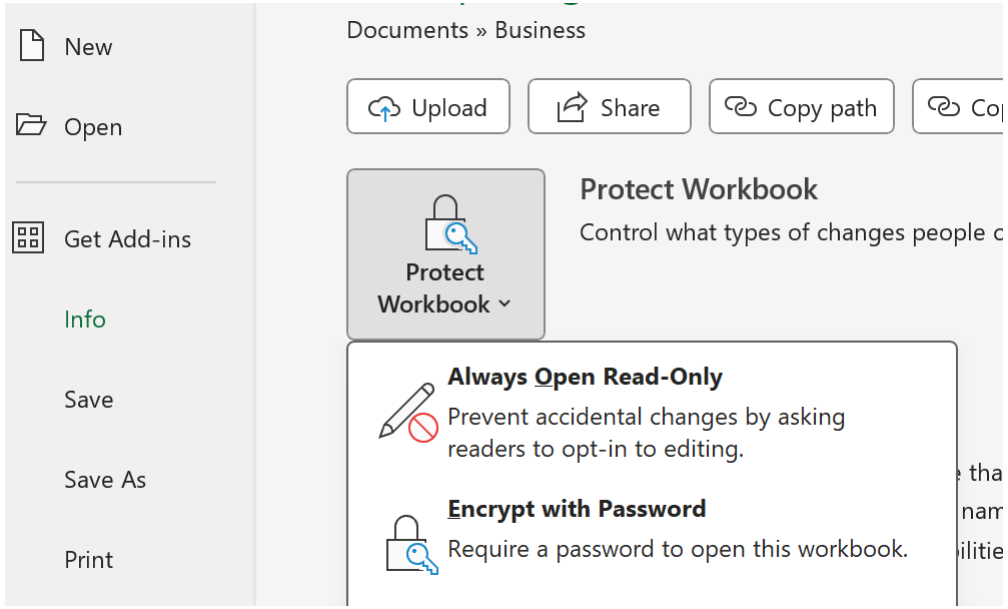
Protect your tablet and your mobile phone as well. You can check emails, shop and bank online on tablets and smartphones, so they need protecting too. Start by password-protecting any devices. You can download anti-virus and anti-spyware protection for tablets and phones and a lot of the apps are free.

Protect your wireless network. You need to protect your wireless network (also known as Wi-Fi) so that people living nearby can't access it. Read the instructions that come with your wireless router to find out how to set up a 'key' (a type of password) so that no one else can access the internet through your router.

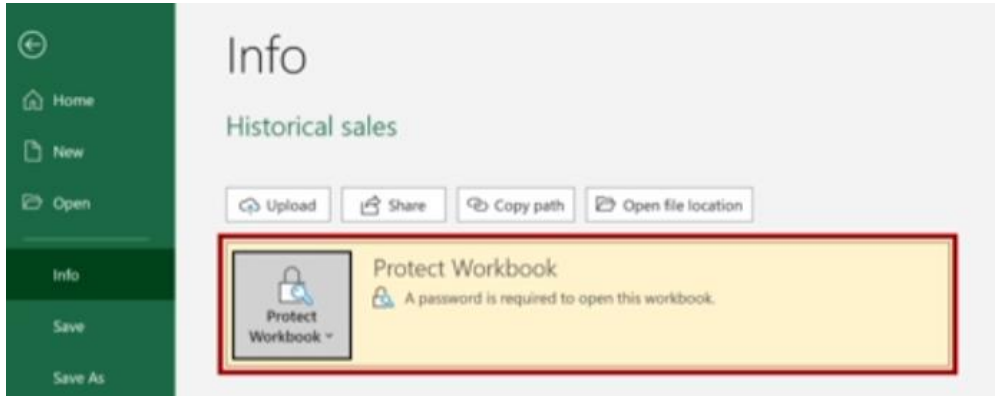
Keep your device updated. Every device has an operating system, which is the software it needs to function properly. Computers will use Windows or Mac OS, and tablets and smartphones use Android or iOS. Your device can be better protected from viruses if you keep the operating system updated. You should receive notifications when new updates are available, but you can also update your system manually.

If you decide to get your passwords under control then you can install a password management program and either use your existing password for each site or let the program generate a different password for each site you visit regularly. (A search for “best password manager” should locate independent reviews of the available products.) Both options require quite a bit of dedication and time but are probably worth it in the end.
If you store your passwords on your device in an Excel spreadsheet, we recommend that you password protect that workbook just in case someone has access to your device.

In Excel click on File, then Info, then “Protect Workbook” and “Encrypt with Password”. You will then have to enter a password twice (the second time to ensure you didn’t make a mistake the first time), clicking OK each time.



When you exit the Info tab should now look like this:



and a password is needed to open the file every time.

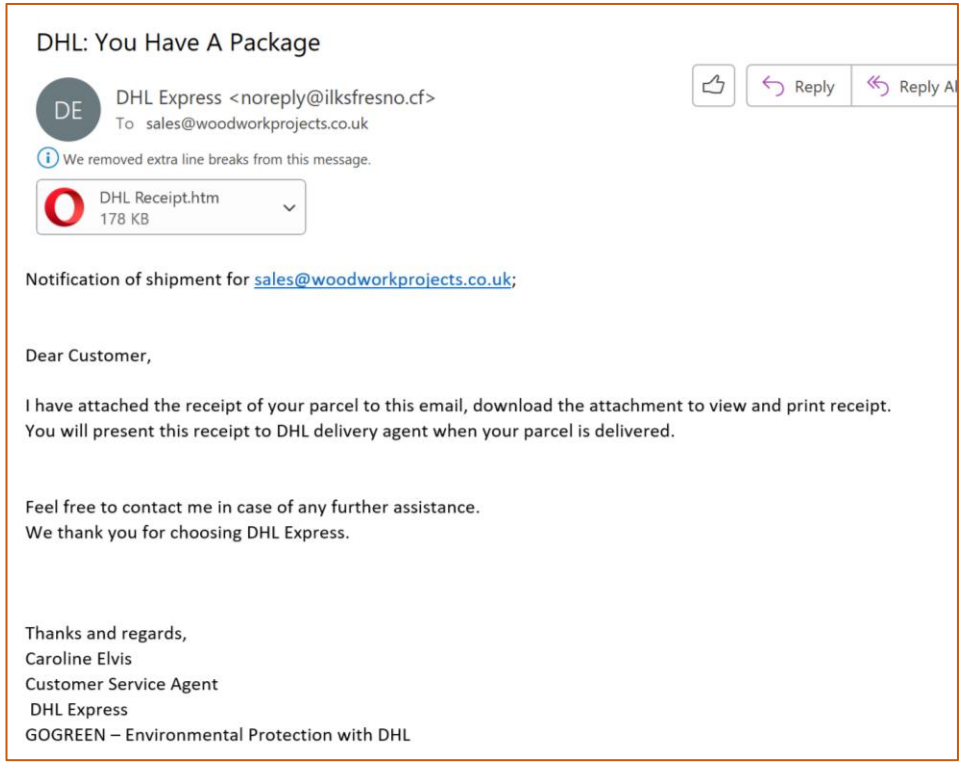
Email scams

Scammers send bogus emails in the hope that people will enter their personal or financial details. They may direct you to a fake website or trick you into thinking you've won a lottery or prize. Have a think about the chances of a company of which you have never heard randomly selecting you for a giveaway, or the chances of winning a lottery without ever entering. If a deal looks too good to be true, it probably is, and be cautious of anything offered in an unsolicited email.

Some emails, known as spam or junk, may also have a link or file attached for you to click on or open. Opening these links or downloading the files may harm your device.

Scam emails can look genuine and appear to be from official places, like HMRC or a bank, but you can often tell it's a scam. Look out for:

- errors in the spelling or grammar, or an unusual style of writing.
- requests for personal information, such as your username, full password or bank details - genuine organisations will never ask this.
- threats that unless you act now, a deal will expire or your account will be closed.
- an email address in the header which is different from the purported sender.



Fake websites

Many scam emails will try to lure you into clicking on a link to a website purporting to be a genuine shopping, financial or Government site when in reality these are completely false. Scammers create fake websites which look official, requesting you to provide personal or financial information. For example, a fake bank website may be set up asking you to update your account or security information. Often, they will look very similar and only a few details may be different. False PayPal sites appear from time to time as well, and are often quite realistic.

If you receive an email purportedly from a financial or official website which you use regularly it is **always** safer to log in to that site in your normal way rather than by clicking on a link in the email.

There are also websites set up to look like a copy of a service offered by government websites. For example, websites which offer to help you apply for a passport renewal or a new driving licence. Although they are not illegal, these websites charge extra money if you use them, rather than going directly through the official government department where the service is free of charge.

Online shopping

It is better to use online retailers with a good reputation, such as well-known supermarkets, high-street shops, or established online stores. If you don’t know a company, look for its full contact details: a reputable company will always display this information on its website. To be extra safe you can search for the name of the company on the internet to see if anyone has experienced problems with the retailer and also see any reviews left by previous customers.

Beware of pop-up messages that warn you about a website's security certificate. They may direct you to a fake website that’s designed to get you to hand over your security details.

Check your bank or credit card statements regularly for any unusual transactions and contact your card issuer immediately if there's a problem. While not essential, using only one card for internet transactions will make this process simpler.

Use a credit card, rather than a debit card, for internet transactions for additional protection. If your purchase costs more than £100 and you use a credit card, the seller and your card company are equally responsible if anything goes wrong.

We recommend using a PayPal account. This is an online account that you link to your bank account or payment card. It's secure and comes with more payment protection than a debit card.

How do I know if a website is secure?

Make sure that you're using a secure website before entering any personal details. There are ways to spot that a website is secure, depending on your browser, including:

- the website address starts with 'https' – the 's' stands for secure.
- the address bar is green, which is an additional sign that you're using a safe website.
- a padlock symbol in the browser where the website address is (but don't be fooled if the padlock appears on the page itself).
- a current security certificate that is registered to the correct address – this appears when you click on the padlock.
- the website ends in '.com' or '.co.uk' – websites that end in '.net' or '.org' aren't usually used for online shopping.

Be aware that a padlock symbol is not an absolute guarantee of safety. If you ever have doubts, it's best to leave the page.

Having said all that, you only really need to worry about the security of a website if you are going to send information such as personal details to it. If you are merely browsing the internet then it generally does not matter whether the site is secure. There are a few dangerous websites but your security software will normally try to prevent you going there.

Online banking: what can I do to keep my money and identity safe?

Online banking is generally safe but there are steps you can take to make sure your money stays where you want it and your identity is not stolen:

- Don’t re-use the same passwords for different accounts.
- As mentioned previously, use a strong password. Avoid passwords made up of common words, numbers or keyboard patterns (such as 'password' or '123456'), and don't include personal information, such as your name, date of birth, or any family member's details.
- Never share your full password or PIN number. Banks will never ask for your full PIN or password – instead, they will ask for specific numbers or letters, for example, the first and third character from your password.
- Always log out of your online banking session, especially if you use a device that others have access to.
- Be cautious when using a public computer to access your online banking, for example, library computers. They may not have the right level of security software. Ask the library staff for more information.
- Only use secure Wi-Fi networks to access your online banking. Don't use public networks, such as those in cafes or train stations – it may be possible for people on the same network to access your details.
- Check your balance and transactions regularly, and report anything you don’t recognise to your bank.
- Regularly check that your personal details are correct and up to date.

False hyperlinks

Let’s have a look at a normal hyperlink, as found on websites and in documents. The most common format for a link is blue, underlined text (although this can be changed and an image can also be a hyperlink).

Please open your web browser and navigate to https://www.highamandrushdenu3a.org.uk/online.html where you will see a couple of (safe) real-world examples.

Cookies

What are internet cookies?
Cookies are small text files containing unique data to identify your computer to the network. When you visit a website, it gives your browser a cookie to store in a cookie file that's placed in your browser's folder on your hard drive. The next time you visit the same website, the browser will give back the cookie to identify you. Then the website loads with a personalized experience.

Cookies do contain data, and that typically includes a unique identifier and a site name. A cookie could also include personally identifiable information such as your name, address, email, or phone number if you've provided that information to a website.

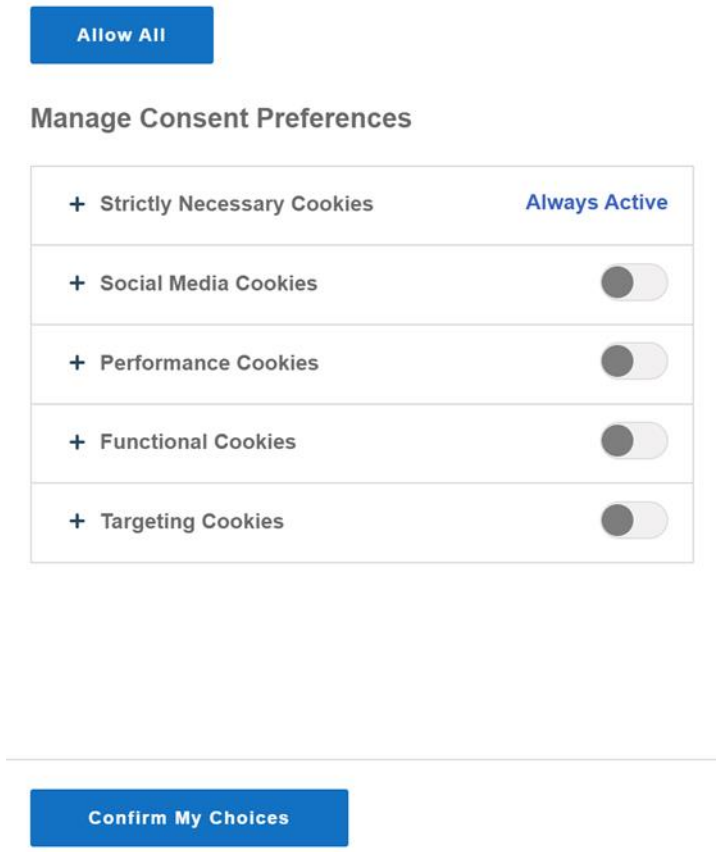
A simple example of cookies is when you open up a website and your username and password are auto-filled. Cookies provided your login information to the website. Another example is when you go online shopping on Amazon and find items that are still in your cart from your last purchasing spree.

Officially, the main purpose of web cookies is to make the internet experience easier for users. When websites can remember your past visits, they can load their website with your preferences. Here are a few things cookies can do when you visit a website:

Set your chosen language preference
Remember items in a shopping cart
Remember if certain settings are turned on
Authenticate your identity
Prevent fraud
Create highly targeted ads
Track how you interact with ads
Make personalized content recommendations
Track items you view in an online store
Auto-fill information in forms

This list shows quite clearly that in addition to “making the internet experience easier” there is quite a strong link to generating revenue for the website owner by encouraging you to buy its own or affiliated products.

You will often see a footer or pop-up asking you to set cookie preferences, and clicking on this should take you to another screen on which you can select which type(s) of cookie to accept.
A responsible website will have options similar to the screenshot on the right, but some websites have incredibly complicated cookie option settings including terms like “consent” and “legitimate interest”. My own personal preference in situations like this is to reject all cookies or find a different website.
Personally I have no objection to “functional” and “performance” cookies but always reject “social media” and “targeting” cookies, but this is a matter for personal choice.



Clearing cookies

If you want to remove cookies from your computer, the process depends on which browser you are using as each is slightly different. Generally speaking you should start with the browser's settings button then "privacy and security" or similar wording.
Somewhere among the options there will be one to "clear cookies" or "clear browsing history".

In some browsers there is also an option to clear cookies at the end of each browsing session.

Note that clearing cookies may mean that you lose the more useful cookies stored on your device, such as those which remember items you have "saved for later" in an online shopping basket or cart.

THE END