# Staying Safe Online

1. Protecting your computer
2. Email
3. Passwords
4. Online shopping and banking
5. Social networking
6. Computer scams
7. Smartphones and tablets

# Protect your computer

**Install anti-virus software**

Viruses are malicious programs that can spread from one computer to another by email or through websites. They can display unwanted pop-up messages, slow your computer down and even delete files. Anti-virus software helps to find, stop and remove these malicious viruses.

**Install anti-spyware software**

Spyware is an unwanted program that runs on your computer. It allows unwanted adverts to pop up, tracks your online activities and can even scan your computer for private data such as credit card numbers. It can make your computer slow and unreliable and make you a target for online criminals. Installing anti-spyware software helps to protect your computer from these threats.

It may seem like you need a lot of software to protect yourself from online risks, but it's actually very easy. You can buy a complete package that includes everything you need, or get effective free software such as AVG (http://free.avg.com) or Avast (www.avast.com/free-antivirusdownload).

These work on both Windows computers and Apple computers.

For computers that use Windows 7 or above, there is built-in anti-spyware software called Windows Defender.

Once your software is installed, keep it up to date when prompted. Online threats evolve constantly so this ensures that you have the highest level of protection.

**Turn on your firewall**

A firewall is a protective barrier between your computer and the internet. It will stop some viruses getting through and will prevent anyone connecting to your computer without your permission. Most computers come with a firewall which is usually switched on automatically, but check to make sure that it is running.

**Keep your operating system updated**

The operating system is the main software program on your computer which manages all the other programs on it. Whichever operating system you have, keep it updated as this will give you stronger protection. You should receive notifications when new updates are available, but you can also update your software manually.

If you use Windows, go to the Windows Update site at http://windowsupdate.microsoft.com. There are instructions on the site that will enable your computer to automatically download and install updates as they become available.

**Protect your wireless network**

If you use wireless internet at home, you will have a wireless router. You need to protect your wireless network so that people living nearby can't access it. Read the instructions that come with your 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.

## Email

Have you received a suspicious email? It may claim to be from your bank, asking you to update your security information. Or maybe it's offering you something that sounds too good to be true. If you have received emails like these, you may have been the target of a common scam called 'phishing'.

Phishing is where criminals send bogus emails to thousands of people, in an attempt to get you to disclose private information. These emails may look as though they come from reputable organisations, such as banks, credit-card companies, online shops, and IT companies, but they are actually from fraudsters.

**Common types of phishing scams:**

- From your 'bank' asking you to update your information or your account will be closed.
- From a well-known software company asking you to update your account details or install a programme on your computer.
- An email saying you have won some kind of lottery or inherited a large amount of money.
- An email supposedly from someone that you may know asking for money because they are stranded somewhere or need medical assistance.

You may also get unsolicited emails with a link or document attached for you to open or click on. These are called 'spam' or 'junk mail'. These may even come from an email address that you recognise, such as a friend or family member, as sometimes accounts can be hacked into and fake emails sent out to all of that person's contacts.

**How to recognise phishing and spam emails:**

- The sender's email address may look official but it is not the actual email address of the bank or company. Always check with your bank if you are unsure what address they use.
- The email does not use your proper name, but instead starts with a general greeting like 'Dear customer'.
- There's a sense of urgency, for example, threatening that unless you act immediately, your account will be closed.
- It may contain a link to a website that looks very similar to the company's real one but is actually a fake site asking for your personal details. The link or site may be slightly different to the official website, so check it carefully. Be aware that you can be taken to a fake website even if the link appears to be correct.
- There will be a request for personal information, such as your username, password or bank details.
- There may be a request for money, for example, for processing your prize, or for helping someone in need.
- There may be a document or link to open and either no message or some short text saying "Check this out" or "See what I found" without further explanation.

**Top things to remember about email:**

- ✓ Banks and other financial institutions never ask for personal information in an email. If you receive a suspicious email claiming to be from your bank, contact your bank directly by phoning them or typing their web address into your browser (not by following the link in the email).
- ✓ Do not open a link or document in an unsolicited email.
- ✓ Do not reply to unsolicited emails, even to say no, as this demonstrates that your email address is active and they may contact you again.
- ✓ If in doubt – delete it without opening it.
- ✓ If it is about account information, phone the organisation directly to ask them, using the phone number found on the official website.
- ✓ Don't panic if you get an email that has a sense of urgency and threatens to close your account. Take your time to check the details first before reacting.
- ✓ Most email packages, including free email accounts from providers such as Yahoo! Mail, Hotmail or Gmail, have spam filters built in which can block unwanted emails.

## Passwords

Passwords are the most common way to prove your identity online, so it's very important to make sure you have strong passwords that can't be easily guessed. Weak passwords are made up of very common sets of letters or numbers.

**Examples of weak passwords that are used a lot include:**

- ✘ password
- ✘ 123456
- ✘ password123

**A strong password should:**

- ✓ Be at least 8 characters long
- ✓ Include a combination of upper and lower case letters
- ✓ Include some numbers and keyboard symbols such as & or !

**Tips to create a strong password:**

- ✓ Avoid using personal information, such as your name, date of birth or common words like 'password'.
- ✓ Make sure that you don't make your password too difficult to remember.
- ✓ Use different passwords for different websites. Using one password for all accounts is a potential security risk because if someone hacks into your account on one site, they will be able to log in to all the accounts that share that password.

For more useful tips on how to create a strong password, see www.microsoft.com/en-GB/security/online-privacy/passwords-create.aspx

It used to be advised never to write down your password. But as people get more online accounts with different and complex passwords they can become harder to recall. If you need to write down your passwords, try to write only a reminder or hint rather than the actual and complete password itself.

If you do write anything down, keep that information somewhere safe away from your computer. It's best to keep it in an unmarked notebook so it won't be obvious to other people what information is inside.

**Password managers**

Some internet browsers have built-in password managers. This is a tool that remembers your passwords for different sites and fills them in automatically for you. When you log in to a website for the first time the password manager will ask if you want it to remember the password.

You have the choice if you want it to or not. It can be timesaving to use this function, but it will only work on your computer. If you use someone else's computer, you will need to remember your passwords for any accounts you want to access.

If you use a password manager and you share your computer with someone else, they will be able to access all your log-in details through the password manager. Make sure that your computer is only used by people you trust.

# Online shopping and banking

The internet can offer a useful way to do your shopping and manage your money from home. More and more people are discovering that it's quick and convenient, and can even lead to some savings.

If you make purchases or bank online, make sure you protect your financial information. Use a secure website when entering card information. This ensures that the information you send can't be read by anyone else.

**How to spot a secure website:**

- The website address should begin with https:// The 's'stands for 'secure'.
- If the address bar is green, this is an additional sign that you're using a safe website.
- Look for a padlock symbol in the browser where the website address is. Don't be fooled by a padlock that appears on the web page itself.
- Websites that offer secure payments and other financial transactions, such as banking, need a security certificate. To view it, click on the padlock symbol to check that the seller is who they say they are and that their certificate is current and registered to the right address. However, the padlock isn't an absolute guarantee of safety, so err on the side of caution if you have any doubts.

**Tips for shopping and banking online safely:**

- Be aware that you will never be asked for your card pin number but you may be asked to provide the security number for your debit or credit card. This is also referred to as a 'CVV2 code' and can be found on the reverse of your card where the signature box is. It's the last 3 digits of the number on the back.
- If you get a pop-up message warning you about a website's security certificate, be very cautious indeed. If you continue, you may be redirected to a fake website, designed to let somebody else read the information you are sending, such as log-in details.
- Use a strong password that can't easily be guessed by others
- Use online retailers that have a good reputation, either as high-street shops or established online stores.
- If a deal looks too good to be true, it probably is. Be cautious of anything offered in an unsolicited email. You could do an internet search to see whether anyone else has had problems or if it's a well-known scam.
- Check where the seller is located. Don't assume that a seller is based in the UK just because their web address has 'uk' in it. The law says that the seller must provide you with their full contact details. If you buy from a seller or company based outside the EU, it can be harder to enforce your rights and problems can be harder to sort out. There may also be added or hidden costs, such as VAT or additional postage for overseas transactions.

- Always use a credit card for internet transactions, or check to see if your debit card provider offers any 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. (Be aware that there is sometimes a card handling fee when you pay with your credit card. Always check how much this is before completing your transaction.)
- Many banks offer free anti-virus software or browser security products – check if your bank offers this.
- After you've finished using a secure site always make sure you log out. That way anyone using the computer after you can't access your personal information.

## Social networking

Social networking websites are online communities where you can connect with people who share your interests. You can create a profile describing yourself, exchange public and private messages and join groups that interest you.

They are a great way to keep in touch with family and friends, make new friends, share your photos, find out about events and much more. Facebook (www.facebook.com) and Twitter (www.twitter.com) are among the most popular sites.

Social networking sites can be targets for people who want to steal personal information, but it's easy to stay safe by following a few sensible guidelines.

- Be aware of who can see your profile. Most social networks allow you to choose who can see your profile, but you may have to change your settings to make it private.
- Be wary of publishing any information that identifies you, such as your phone number, photos of your home, your address, date of birth or full name.
- Pick a username that doesn't include any personal information. For example, 'joe_glasgow' or 'annajones1947' would both be bad choices.
- Set up a separate email account that doesn't use your real name to register with the site. If you don't want to use the site any more, you can simply stop using that email account.
- Use a strong password that is different from the passwords you use for other accounts
- Be cautious of people you have just met online who ask you to reveal personal information or who want to meet you very quickly.

## Computer scams

Beware of a common scam. The fraudsters phone you claiming to be from a well-known IT firm, asking you to follow a few simple instructions to get rid of a virus or update your software. If you do as they ask, they will upload software called spyware onto your computer, which will allow them to access any personal details you have stored on your computer. Never respond to a phone call from someone claiming that your computer has a virus. If you get a call like this, hang up straight away. ***Legitimate IT companies never contact customers in this way.***

## Tablets and smartphones

Mobile phones and tablets can now be used to do things like check emails, shop and bank online or explore the internet. Tablets are small handheld devices with a touchscreen, although you can get a keyboard to attach to them if you prefer to type on one. Smartphones are mobile phones that have touchscreens and the ability to connect to the internet. A lot of people now use tablets or phones instead of computers.

Tablets and smartphones need protecting just like computers do. That's because they can still be infected with viruses or spyware. Just like on computers, viruses on your tablet or smartphone could be used to get your personal details, slow your device down or spread viruses to other tablets or computers.

You can download anti-virus and anti-spyware protection for tablets and phones. These are often referred to as 'apps' (applications), which is just another term for software. The best protection for your device may vary depending on what type of phone or tablet you have. If you're unsure about which is best, you could ask your mobile phone provider, pop into a local phone shop or look online for more information.

A lot of good anti-virus protection for phones and tablets is free and can be downloaded online.

You should also consider password-protecting your device