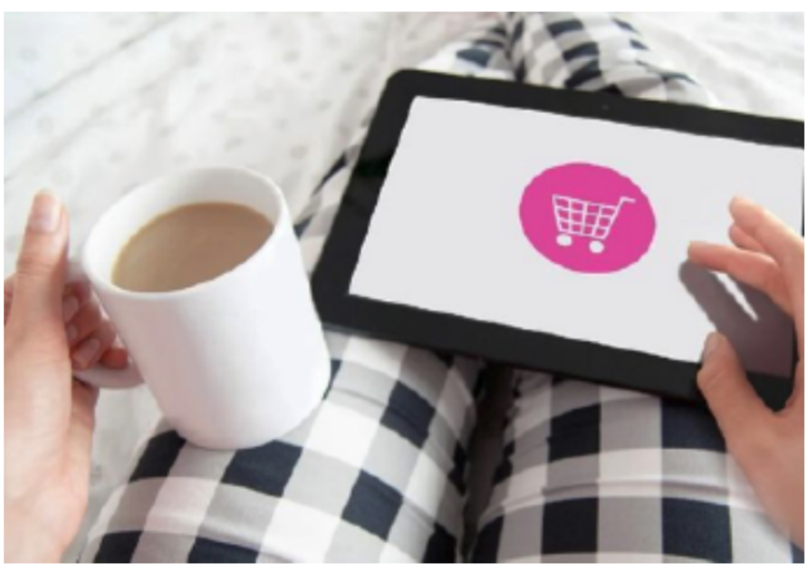
nipsa
Union Learning

Shopping Online Securely



With most high street shops still shut, many of us are spending more time shopping online. We've updated our online shopping guidance to help you to avoid scam websites, and to purchase items safely.

- Choose carefully where you shop
- Use a credit card for online payments
- Only provide enough details to complete your purchase
- Keep your accounts secure
- Watch out for suspicious emails, calls and text messages
- If things go wrong

Choose Carefully Where You Shop

It's worth doing some research on online retailers to check they're legitimate. Read feedback from people or organisations that you trust, such as consumer websites.
Some of the emails or texts you receive about amazing offers may contain links to fake websites. If you're unsure, don't use the link, and either:

- type a website address that you trust directly into the address bar
- search for it, and follow the search results

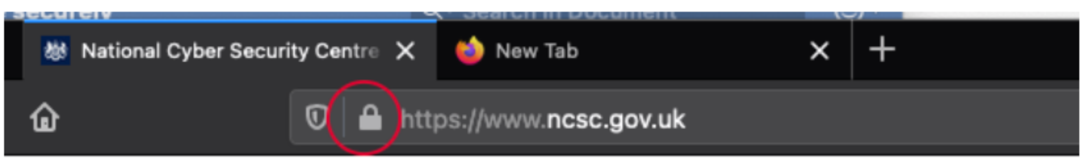
Use a Credit Card for Online Payments

Use a credit card when shopping online, if you have one. Most major credit card providers protect online purchases, and are obliged to refund you in certain circumstances. Using a credit card (rather than a debit card) also means that if your payment details are stolen, your main bank account won't be directly affected.

Debit card payments and purchases are not covered by section 75 of the Consumer Credit Act. But you might be able to make a claim for a refund under a voluntary scheme called 'chargeback'.

You should also consider using an online payment platform, such as PayPal, Apple Pay or Google Pay. Using these platforms to authorise your payments means the retailer doesn't even see your payment details. They also provide their own dispute resolution should anything go wrong. However, they may not provide the same protection as a card provider, so check their terms and conditions before your sign up.

When it's time to pay for your items, check there's a 'closed padlock' icon in the browser's address bar. It will look like this:



National Cyber Security Centre ✕ New Tab ✕ +

https://www.ncsc.gov.uk

The padlock icon doesn't guarantee that the retailer itself is legitimate/reputable (and that their website is secure). It means that the connection is secure. If the padlock icon is not there, or the browser says not secure, then don't use the site. Don't enter any personal or payment details, or create an account.

Only Provide Enough Details to Complete Your Purchase

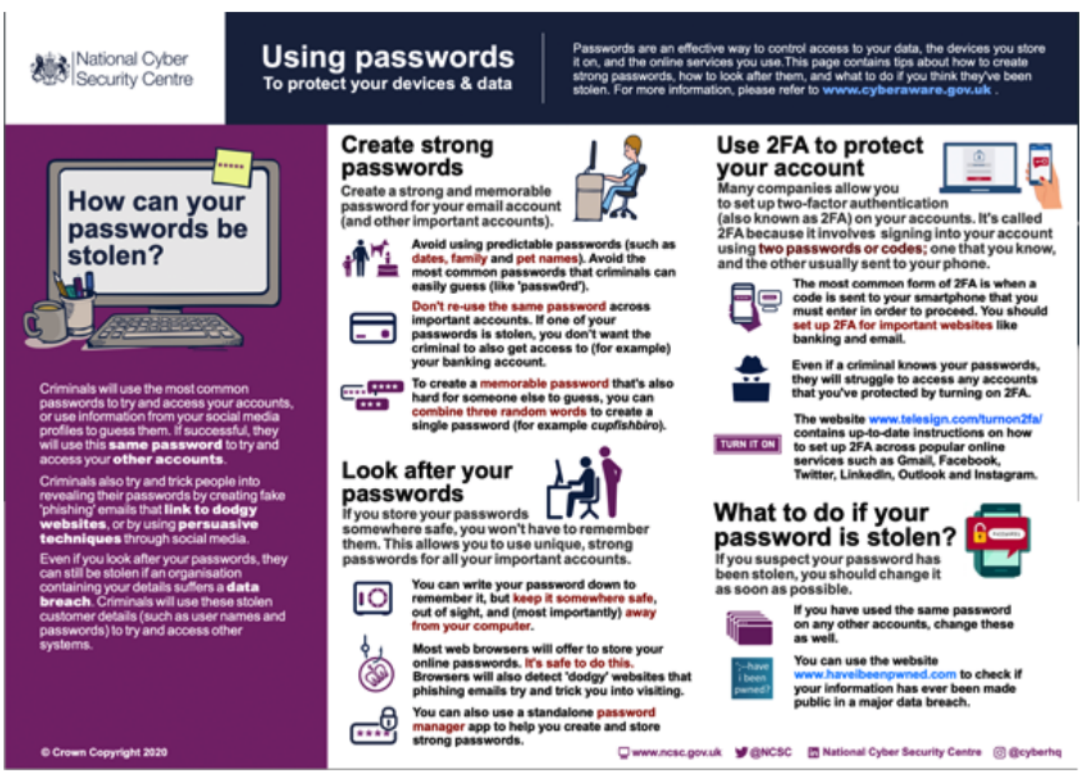
You should only fill in the mandatory details on a website when making a purchase. These are usually marked with an asterisk (*), and will typically include your delivery address and payment details. You shouldn't have to provide security details (such as your mother's maiden name, or the name of your first pet) to complete your purchase.

If possible, don't create an account for the online store when making your payment. You can usually complete your purchase without having to create an account, or by using an online payment platform (such as PayPal). If you think you'll become a regular customer with the store, then you may want to create an account with them.
The store may also ask you if they can save your payment details for a quicker check-out next time you shop with them. Unless you're going to use the site regularly, don't allow this.

Keep Your Accounts Secure

If you're using the same password for your online accounts (or using passwords that could be easily guessed), then you're at risk. Hackers could steal your password from one account, and use it to access your other accounts. For this reason, you should make sure that your **really important accounts** (such as your email account, social media accounts, banking accounts, shopping accounts and payment accounts like PayPal) are protected by strong passwords **that you don't use anywhere else**.

The trouble is that most of us have lots of online accounts, so creating strong passwords for all of them (and remembering them) is hard. This NCSC infographic explains how you can create strong passwords and store them safely (so you don't need to remember them).



National Cyber Security Centre

Using passwords
To protect your devices & data

Passwords are an effective way to control access to your data, the devices you store it on, and the online services you use. This page contains tips about how to create strong passwords, how to look after them, and what to do if you think they've been stolen. For more information, please refer to www.cyberaware.gov.uk .

How can your passwords be stolen?

Criminals will use the most common passwords to try and access your accounts, or use information from your social media profiles to guess them. If successful, they will use this **same password** to try and access your **other accounts**.

Criminals also try and trick people into revealing their passwords by creating fake 'phishing' emails that **link to dodgy websites**, or by using **persuasive techniques** through social media.

Even if you look after your passwords, they can still be stolen if an organisation containing your details suffers a **data breach**. Criminals will use these stolen customer details (such as user names and passwords) to try and access other systems.

© Crown Copyright 2020

Create strong passwords
Create a strong and memorable password for your email account (and other important accounts).

Avoid using predictable passwords (such as dates, family and pet names). Avoid the most common passwords that criminals can easily guess (like 'passw0rd').

Don't re-use the same password across important accounts. If one of your passwords is stolen, you don't want the criminal to also get access to (for example) your banking account.

To create a memorable password that's also hard for someone else to guess, you can combine three random words to create a single password (for example *cupfishbiro*).

Look after your passwords
If you store your passwords somewhere safe, you won't have to remember them. This allows you to use unique, strong passwords for all your important accounts.

You can write your password down to remember it, but keep it somewhere safe, out of sight, and (most importantly) away from your computer.

Most web browsers will offer to store your online passwords. It's safe to do this. Browsers will also detect 'dodgy' websites that phishing emails try and trick you into visiting.

You can also use a standalone password manager app to help you create and store strong passwords.

Use 2FA to protect your account
Many companies allow you to set up two-factor authentication (also known as 2FA) on your accounts. It's called 2FA because it involves signing into your account using two passwords or codes; one that you know, and the other usually sent to your phone.

The most common form of 2FA is when a code is sent to your smartphone that you must enter in order to proceed. You should set up 2FA for important websites like banking and email.

Even if a criminal knows your passwords, they will struggle to access any accounts that you've protected by turning on 2FA.

TURN IT ON

The website www.telesign.com/turnon2fa/ contains up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and Instagram.

What to do if your password is stolen?
If you suspect your password has been stolen, you should change it as soon as possible.

If you have used the same password on any other accounts, change these as well.

You can use the website www.haveibeenpwned.com to check if your information has ever been made public in a major data breach.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Keep Your Accounts Secure

You can further protect your important accounts from being hacked by turning on two-factor authentication (2FA). It's also referred to as 'two-step verification' or 'multi-factor authentication'. Turning on 2FA stops hackers from accessing your accounts, even if they know your password. It does this by asking you to confirm that it's really you in a second way - usually by asking you to enter a code that's sent to your phone.

Watch Out for Suspicious Emails, Calls and Text Messages

You'll probably receive many messages from online stores, as a result of 'opting in' to receiving communications from them. Lurking amongst these genuine messages, there may well be fake ones (containing links designed to steal your money and personal details) that can be very difficult to spot.
Of course, not all messages are bad, but if something doesn't feel right, follow the NCSC guidance on dealing with suspicious emails, phone calls and text messages:

- If you have received an **email** which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at **report@phishing.gov.uk**.
- If you've received a suspicious text message, forward it to 7726. It won't cost you anything, and allows your provider to investigate the text and take action (if found to be a scam).
- If you come across an **advert** online that you think might be a scam, report it via the Advertising Standards Authority (ASA) website. This allows ASA to provide online service providers with the details they need to (if appropriate) remove these from websites.

If Things Go Wrong

If you think your credit or debit card has been used by someone else, let your bank know straight away so they can block anyone using it. Always contact your bank using the official website or phone number. Don't use the links or contact details in the message you have been sent or given over the phone.
If you think you have responded to a suspicious email or text message, or visited a scam website, don't panic. Read the NCSC's guidance on dealing with scam emails, phone calls and text messages.
If you've lost money, tell your bank and report it as a crime to Action Fraud (for England, Wales and Northern Ireland) or Police Scotland (for Scotland). By doing this, you'll be helping to prevent others becoming victims of cyber crime.
If you don't receive the item (or it doesn't match the description given), Citizens Advice has some useful information about getting your money back if you paid by credit card, debit card or PayPal.