# Protecting yourself and your data whilst using our services

At CC Moore we take data protection and data security seriously, whether that's our customers' data or the data of our employees, suppliers and other contacts.

We have implemented within our business extensive internal procedures and policies to ensure our ongoing compliance with UK data protection law and to ensure the utmost protection for our customers. With this in mind, we wanted to make sure we do everything we can to not only protect your data when we're processing it, but to also help you protect yourselves when you're using our website and services and hopefully the advice and guidance in this document will also help you with other businesses and organisations you interact with too.

So, this guidance is intended to give you an overview of some of the tactics you can employ to protect yourself and your data when you're online. There are also some other online resources which can help as well, particularly the National Cyber Security Centre's (NCSC) "Cyber Aware" advice which can be found online here: https://www.ncsc.gov.uk/section/information-for/individuals-families

**1. Protecting your CC Moore account**

When you set up an account with us via our website you will be asked to set up a password which will be needed to access your account in future, so here's some tips about passwords:

- Use a strong password. The NCSC recommend using the 3 random words method to create a strong password. You want to avoid using words that could be guessed easily on our website (such as CC Moore, fishing, bait, etc.), but chose three random, unconnected words and include numbers, special characters (! @ £ $ etc.) and upper- and lower-case letters. Or if you want a really random generated password, use a password generator (which might be suggested by your computer) such as Norton's: https://my.norton.com/extspa/passwordmanager?path=pwd-gen

- Use a password locker or your web browser to remember your passwords. If you're having to remember multiple passwords, it can be tempting to write passwords down which run the risk of being found or seen by third-parties which would then give them access to your account. If you use a password locker (e.g. LastPass) or if your device provides functionality to remember passwords (e.g. Keychain on a Mac) then this will help you remember passwords rather than having to write them down or try to remember them. You can also use your web browser to store your passwords, and this will help auto-suggest passwords for particular websites and also help you spot fake websites (as the password won't be suggested for such sites). Of course, ultimately you will still need to protect access to these applications or functions on your devices with a sensible password, but you will only need to remember one password (e.g. for LastPass, your computer, etc.). You should also be mindful of any other users of your device as they may also be able to auto-login with your password if this is suggested

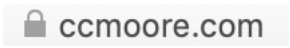
- Avoid sharing your password. This may seem obvious, but you do need to be careful, particularly if a fraudulent email or someone on the phone asks you to confirm your password. At CC Moore we will never ask for your password, so if you get an email or phone call from some claiming to be from CC Moore, they should never ask you for your password. Furthermore, if you are unsure whether the email or call are genuine you can always ring our main sales number (from our website) to confirm the contact is genuine

- Never give out your CC Moore login details. It's free to create a CC Moore account, so there is no reason for someone not to set up their own account, rather than asking for your login details. So, if you keep your password secure and safe, your CC Moore account should also be safe and secure

**2. Protect yourself online**

You'll find a lot of advice on the NCSC website (https://www.ncsc.gov.uk) to help protect yourself when you're online. But here are the key points:

- Be careful where you shop online. Only shop online at trusted sources, like CC Moore. If it sounds too good to be true, then it probably is, so if you find something online heavily discounted then do some research to check that the offer (and the company offering it) are genuine. They could be after your bank details, or will collect your payment but not deliver the goods you've ordered
- Use a credit card for online payments, if you can. This is because, unlike debit cards, most credit card providers protect online purchases and may be able to refund you if you've not received your goods. Alternatively, you may want to use a trusted online payment platform like PayPal, Apple Pay or Google Pay
- Only interact with or buy goods from websites which provide a secure connection. You'll know the connection to the website is secure because there will be a padlock in your browser's address bar. Whilst this will not determine if the site is genuine, it will mean any information, payment details, etc. entered via the website will be done securely. For example, you can trust our website because we have secured it:




- Be careful not to fall foul to "social engineering". Social engineering is when someone tricks into giving out information that doesn't seem obvious but might help them guess or work out what websites your use, your username and maybe even your password. They may be able to guess some of your information because you have a public social media profile, or by contacting your direct and getting to know you or by asking you questions

- Avoid insecure internet connections, by only connecting online using wifi hotspots you can trust. If you can, you should avoid using public wifi in public spaces like hotels, pubs, cafes, etc. as someone may have set up a fake internet connection. You may get access to the internet, but someone might be reading everything you're typing (like your login and password details)

**3. Keep your data and devices safe**

As well as having a safe approach to managing your passwords and access to your CC Moore account, you should also make sure you protect your devices and software. There's a number of ways you can do this:

- It is not unknown for device software to have security flaws which are then fixed by an update. If you don't update your device it is possible your device or software could be compromised by someone exploiting the flaw on your device. The same is true for our online shop. We make sure we're running on the latest website software to protect it from exploits and to make sure your

data is kept safe. If you're worried you don't really know how to keep things up to date, or you might miss an update, turn on automatic updates, so they're done automatically. You don't need to worry then, whether you're running on the latest software update.

- Maintain backups so you protect any information you need, should your device stop working, or if you lose your device or it is stolen. This can help you recover all your information on a new device, change account passwords, etc.

- Keep your anti-virus software up to date. Viruses and malware can be used to collect information from your or from your device. Ransomware can also lock you out of your data and device, unless you pay a ransom. By keeping your anti-virus up to date and avoiding clicking on links or download software from untrusted sources, you can protect yourself from opportunists trying to access your device and data (including passwords)

## 4. Don't fall foul of tricksters

We've all heard the news about people being tricked into handing over passwords, money, or providing access to their accounts. Whenever you are online or dealing with someone remotely (e.g. via the phone or email), always think, is the person contacting me, actually who they say they are? Phishing is a cyber-security term used to describe emails and messages that look like they come from genuine businesses, but are in fact fraudulent contacts or websites, to trick you into handing over your login and password details. You may well have seen some of this already if you've received a phone call or email about your bank needing you to reverify your identify, or that your Amazon account is going to be shut down, etc. These are all phishing scams.

If it looks like your account has been compromised, change your password immediately, and if necessary contact the company (e.g. bank, CC Moore, etc.) straightaway.

## 5. More information and reporting cyber-crime

We hope you found this simple guide helpful. If you have any concerns or questions, consider looking at the NCSC website for further guidance.

If you think you've been a victim of an online crime, you should report it to Action Fraud (http://www.actionfraud.police.uk/ or call 0300 123 2040).