Cybersecurity

Tips to keep yourself safe online

CHARLES STANLEY

Wealth Managers

Since implementing lockdown measures, our reliance on technology has increased, and it is important to keep yourself safe online and make sure the services you use have adequate security measures in place.

Preventing a Cyber attack

Credit score checking

Create an account with a free credit score service and check it regularly, as an unexpected change might indicate a criminal is trying to steal your identity. Pay particular attention to credit application searches; if you see a search that you don't recognise, this could be because someone has applied for credit in your name. If this happens contact your bank and Action Fraud.

Action Fraud on 0300 123 2040 or www.actionfraud.police.uk

Email and cloud

An email account is an attractive target. Hacking it allows criminals to reset other online account passwords, impersonate you, amend emails, activate auto-forwarding (so they receive a copy of emails you send or receive), and phish your contacts. Your cloud service accounts, e.g. Office365, are a close second. Use 2FA, see (see 'Two Factor Authentication') for your email accounts and cloud services. Change each account password to something unique, long (>15 characters), and strong (three random words with some numbers and symbols). Never reuse an email or cloud password; criminals have tools that automatically try one compromised password with other popular online accounts.

Insecure email and secure portals

The global internet is a public network. Standard email sent across the internet is insecure: it can be read or intercepted. Email accounts belonging to individuals are increasingly being hacked. Charles Stanley's 'MyCS' service is a secure website (known as a 'secure portal') that offers a safe messaging service for our clients and Investment Managers. As the messages stay inside Charles Stanley's network, and are not sent across the public internet, the risk of a message being intercepted or tampered with is greatly reduced.

Preparing for a Cyber attack

Backup

Always have at least two copies of data. You can either upload it to a cloud storage account, and/or copy it to another hard drive which you keep nearby (so you can update it easily) If possible keep a second copy away from your home so it won't be affected by things like fire, flood or theft.

Call recording

Consider putting a call recording app on your mobile phone. If you are called by a criminal you will have a copy of the call. This might be useful for Action Fraud (0300 123 2040) or the Police.

Clone your hard drive

Cloning takes an exact copy of your computer's hard drive and puts it on another disk drive. This isn't the same as a backup, and means that if you have a problem with your computer, like a ransomware attack, you can swap the ruined hard drive for the cloned hard drive. Refresh the cloned drive each time you add or remove programs or update your operating system, keep it disconnected from your computer and somewhere safe, and 'if you ever put it into your computer the very first thing do to is clone the drive you have just put in.

Separation

Separate your electronic content (photos, video, spreadsheets, document and purchased software etc.) from your internet connected computer by moving it to a separate, external hard drive. Then keep this hard drive disconnected (known as 'air gapped') from the computer when using the internet. If the computer is attacked by malicious software ('malware') or a cyber criminal, only the computer will be affected; the digital content will be safe on the separate hard drive. It is important to also have a copy of the separate hard drive, (see 'Backup'), and you can also create a copy of your computer's hard drive, see ('Clone').

Password hygiene

Starting with your email account, make the password long (over 15 characters) and strong (containing numbers, letters and symbols). You can try using three random words that you can remember easily but mean nothing to anyone else. Then replace some of the letters with numbers and symbols.

Only use this password for your email account. Then go through your other important online accounts, those that can complete transactions or hold useful information about you, and do the same to those passwords, but crucially don't use a password (or a variation of it) for more than one online account.

Password manager

A password manager stores all your online passwords in a secure vault that is protected by a single master password (this must be long, strong and not used for any other accounts). This means every website account you have can have a unique password. Password managers can also automatically sign you in when you visit a website, and can check the passwords in your vault and tell you which ones need improvement.

Push Payment Fraud

This is when a cyber criminal tricks you into sending a payment to their bank account. Try to use a secure payment service like PayPal, or pay by credit card, instead of sending a bank transfer. If you have no other option, always independently verify the bank account details first: never rely on bank account details in an email. You can also keep the balance of the bank account that you use for internet banking to a convenient minimum. That way if a cyber criminal does transfer money out of it, the amount taken will be much smaller.

Stay updated

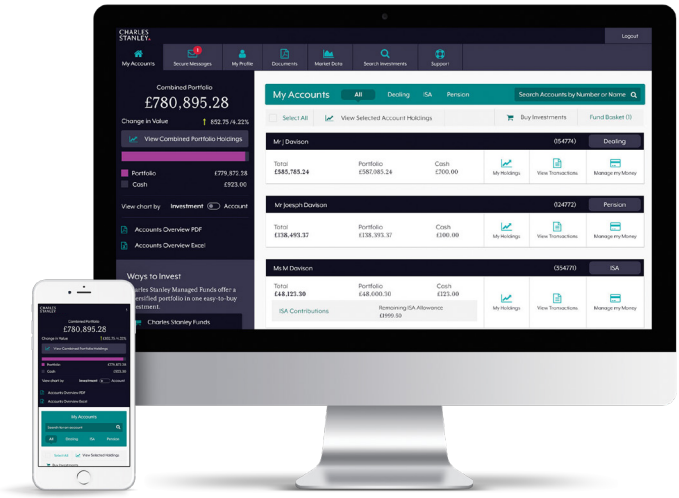
Keep all your software updated, not just your operating system, e.g. Windows. If you are running Windows 7 or older, upgrade it now, as any new security holes are no longer being fixed by Microsoft and cyber criminals can exploit them.

Two Factor Authentication (2FA)

2FA uses two pieces of information to prove (authenticate) your identity. Your password, 'something you know' is the first factor. The second factor will typically be 'something you have', like your mobile phone. After entering your username and password, a code is required before the account can be accessed. This might be sent as a text message or within an app on your moible phone. 2FA greatly reduces the likelihood of your account being hacked. An unexpected 2FA code also indicates a cyber criminal has your password, so you can immediately change it. 2FA is free and straightforward. Activate it for important accounts, starting with email and any cloud services.

Zero trust

People trust unexpected emails, text messages and phone calls, until their suspicions are aroused. Protect yourself by instead adopting a zero-trust mindset, when emails, text messages or phone calls are not believed until proven genuine. If you receive an email, text or phone call that is a) unexpected and b) asking you to do anything at all, even if it's from someone you trust, like tradesperson or a friend, pause and think it might be a cyber criminal pretending to be them. Independently verify the sender by, for example, contacting them using details obtained from a search engine or official web site.



Get in touch

We're always happy to help

020 7149 6210
www.charles-stanley.co.uk
Charles Stanley, 55 Bishopsgate, London, EC2N 3AS

CHARLES STANLEY
Wealth Managers