Date: June 2020

Cyber Security Advice

Below is some further information and guidance around staying safe online.

1. Protect your Email by Using a Strong and Separate Password

Cyber criminals can use your email to access many of your personal accounts and find out vital personal information, such as your bank details, address or date of birth.

Having a strong, separate password for your email means that if cyber criminals steal the password for one of your less important accounts, they can't use it to access your email account.

A good way to create a strong and memorable password is to use three random words. Numbers and symbols can still be used if needed, for example 3redhousemonkeys27!

Be creative and use words memorable to you, so that people can't guess your password. Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favourite sports team which are easy for people to guess.

Cyber criminals are very smart and know many of the simple substitutions we use such as 'Pa55word!" which utilises symbols to replace letters.

Never use the following personal details for your password:

- Current partner's name
- Child's name
- Other family members' name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team

You can remain even safer by having a separate password for each of your accounts.

2. Install the Latest Software and App Updates

Software and app updates contain vital security updates to help protect your devices from cyber criminals.

Cyber criminals use weaknesses in software and apps to attack your devices and steal your identity. Software and app updates are designed to fix these weaknesses and installing them as soon as possible will keep your devices secure.

You'll often receive a prompt on your computer, smartphone or tablet to inform you that a software or app is ready to be updated. Don't ignore this message.

The few minutes it takes to download and install the updates could save you a significant amount of time and trouble in the long run, reducing the risk of you falling victim to identity theft.

Software and app updates don't have to get in the way of what you're doing. You can choose to install them at night whilst asleep when your device is plugged in or set your mobile or tablet to automatically update them when you are connected to Wi-Fi. So why not have a look at your devices and install your software and app updates.

3. Turn on 2 Factor-Authentication on Your Email

Two-factor authentication is recommended for email accounts to make sure your data is secure.

Why do we want this? Because 2FA is the single best thing you can do to improve the security of your important accounts.

However good your passwords are, they can only provide so much protection. They could be stolen from your service provider or from your phone, tablet or laptop. Or you could get tricked into revealing them. This is why we want more people to use 2FA, both at work and at home.

Accounts that have been set up to use 2FA will require an extra check, so even if a criminal knows your password, they won't be able to access your accounts. This is reassuring if you suspect some of your passwords aren't as strong as they could be, or you've re-used them across different accounts, or you worry that (like anyone) you may one day fall for a scam email that reveals your password to a criminal.

When setting up 2FA, the service will ask you to provide a 'second factor', which is something that you (and only you) can access. This could be a code that's sent to you by text message, or that's created by an app. Some types of 2FA provide more protection than others (because the second factor is more difficult to steal), but since any 2FA is better than none, you should use 2FA wherever you can. It only takes a few minutes to set up for each account, and it's well worth it for the amount of additional protection it gives you.

4. Use a Password Manager

What is a password manager?

A password manager is an app on your phone, tablet or computer that stores your passwords securely, so you don't need to remember them all. Some password managers can synchronise your passwords across your different devices, making it easier to log on, wherever you are. Some can also create random, unique passwords for you, when you need to create a new password (or change an existing one).

Why would I want a password manager

Reusing the same password across different accounts can be dangerous. A cyber criminal might steal one of your passwords, and then use it to try and access other accounts. This means they could quickly break into several of your accounts despite only knowing one password.

We know that we're supposed to create a unique, hard-to-guess password for all of our online accounts, to prevent such a scenario happening. However the NCSC recognise that this virtually impossible to do without help. Password managers provide that help. They're designed to make **using** and **generating** passwords easier and more secure. Many can also automatically enter the appropriate password into websites and apps on your behalf, so you don't even have to type them in every time you log in.

What types of password manager are available?

You may be already using a password manager without knowing it. Many are **built into** your internet browser (such as Google Chrome, Microsoft Edge or Firefox), or are part of the operating system on your smartphone or tablet. You may have noticed when you sign into an account, a box appears asking you if you want the browser (or device) to remember your password. If you are **not** sharing the device with anyone else, then it is safe to tick the box. If it doesn't offer to save your password, you may need to turn this option on in your device settings.

Standalone password manager apps are also available to download, many of which can be installed on different types of device, and with extra features like the ability to create good passwords for you. It's worth finding online reviews of the password managers you're considering, and deciding on the features you need (and the support the vendor provides) before choosing one that's right for you.

How do I protect my password manager?

Whether you're using a standalone password manager or a built-in one, it is important to keep the password manager account secure because if a criminal accesses this, they'll potentially have access to all your passwords and associated accounts. You also need to take steps to make sure you can always get in yourself, so you don't lose access to all your passwords.

The NCSC strongly recommend that you:

- Set up two factor authentication on the password manager account. If you have the option, set up more than one type of second factor so you have a backup plan to get into your password manager account.
- Install updates for your password manager app as soon as you're prompted to update. If you're using your browser, always make sure you are using the latest version and you keep this up to date.

- Choose a strong password for the password manager account (for example using three random words). You can’t store this in the password manager itself, so you may want to write this one down and store it somewhere safe - away from your device - so you don't forget it.

Note that if you're using a built-in password manager through your browser or device, they may be protected by one of your existing accounts. For example, passwords saved in Apple's Keychain are protected by your AppleID, and passwords saved in Google's Chrome browser will be protected by your Google (or Gmail) account, if you have logged in. Again, make sure that you are using a strong password of these accounts.

5. Secure your Smartphone or Tablet with a Screen Lock

Screen locks offer your devices an important extra layer of security.

Screen locks offer your devices an important extra layer of security. Each time you want to unlock your device or switch it on, you’ll be asked to enter a PIN, password or fingerprint. This means that if someone gets hold of your device they can’t access the data on your device without entering your password, pattern, PIN or fingerprint.

Don’t use ‘1,2,3,4’ or an ‘L’ shaped pattern which are easy for other people to guess.

6. Always Back Up Your Most Important Data

Safeguard your most important data, such as your photos and key documents, by backing them up to an external hard drive or a cloud-based storage system.

If your device is infected by a virus, malicious software (malware) or accessed by a cyber criminal your data may be damaged, deleted or held to ransom by ransomware preventing you from accessing it. Backing up your data means you have another copy of it, which you can always access.

Make sure that the external hard drive you are using to back-up your data is not permanently connected to the device you are backing up either physically or over a local network connection.

The advantages of backing up your data in the cloud

A cloud service is useful because you are saving a copy of your data elsewhere, hosted by someone else out on the internet. This means that if your device is stolen/damaged/you have a fire or you suffer a ransomware attack, your data is not lost.

You may have heard about some of the high profile cyber attacks on cloud storage, such as celebrity photos being stolen. These shouldn't put you off using a cloud service because when protected by a strong password and two-factor authentication (where available) they can be a very convenient and secure way to store data you care about.

Most devices now include a cloud back up service, with a certain amount of free space, and are a sensible choice for most users. 3rd Party products may offer you additional features such as more storage space or better usability across multiple devices which you should consider against your needs.

More information on all of the above can be found at https://www.ncsc.gov.uk/

Finally, the National Cyber Security Centre have release a tool for reporting any emails you may believe to be suspicious. They Simply forward the suspicious email to they using the email address report@phishing.gov.uk. More information can be found about this service by visiting their website at https://www.ncsc.gov.uk/information/report-suspicious-emails.

By implementing these few simple steps, you will be able to remain more secure online.