Cyber Byte

February 2024

Cyber criminals are relentless, always looking for vulnerabilities to attack us and we are continuously having to protect ourselves and keep mindful of cyber threats.

Their persistence can cause us fatigue as the scams seem never ending. This can also cause us to put our cyber security to one side and maybe look at doing something about it tomorrow or next week….nothing will happen by then... will it?

One area that cyber criminals seek to exploit are weak passwords.

Our passwords are like digital keys, they allow us to unlock our devices and online accounts. Sometimes though, we use the same password for all these actions.

How do cyber criminals crack passwords?

There are a number of methods cyber criminals use to crack passwords and some of the common attack methods include:

- **Phishing and Social Engineering** – these are two ways of tricking us into divulging our personal credentials or providing criminals unauthorised access to our accounts. Phishing is the fraudulent practice of sending emails purporting to be from a reputable organisation or individual in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Social Engineering is the practice of manipulating someone into giving up sensitive information, usually through exploiting human error or taking advantage of trust.

- **Brute force attack** – a trial and error method that involves trying all possible combinations of the characters in a password in sequence. Cyber criminals use high powered computers to test trillions of passwords every second.

- **Dictionary attack** – a more sophisticated form of brute force attack in which common words are entered into password fields. Automated software is used by cyber criminals to crack passwords that are based on dictionary words, slang terms, common misspellings, words spelt backwards and well-known passwords, such as ‘password123’. A variation of this is known as ‘credential stuffing’ where leaked or stolen credentials are tried. To reduce the likelihood of your password being cracked, it is important to ensure that you use a long, complex password that is hard for someone else to guess. Always use unique passwords for every account.

Also, be careful about inadvertently revealing personal details via social media: you'll regularly see quizzes that ask you to share this kind of data. Doing them might seem harmless, but you can't guarantee your data will be safe or where your answers are being shared. Remember the Dictionary attack method of trying to crack passwords!

So, how many passwords or digital keys do you have? Is it just the one that you use for convenience? Or do you have more than one password or digital key to access your device/s and online accounts.

Another way of looking at it is by asking yourself “How many keys do I have to lock my house, shed, garage or car”. The answer is, that we use different keys to lock our property.

Imagine if you just had one key and it was stolen, the criminal would be able to gain access to your house, shed, garage, car etc. using that single key.

That would be the same if a cybercriminal guessed the single password you use for all your online accounts. They would have access to all your personal data, especially your online banking, shopping, social media and email accounts.

So, having more than one password for your different online accounts is the safest way to protect them from being attacked and to protect your data from being stolen by cyber criminals.

Our partner organisation the NCSC (National Cyber Security Centre) has created excellent guidance on how to create unique passwords by using three random words.

Three random word passwords are exactly what it says. Pick three random words from what you are seeing around you just now – “windowtreecloud”, “hillcupglasses”, “catsinkflower”

By adding a special character and a number, to these three random words, what you have created are unique passwords with no connection to such things as a favourite holiday destination, pets name, school or childrens’ names, hobbies etc. things which cyber criminals can easily find out about you from social media.

You can find out more at;

Three random words - NCSC.GOV.UK

You should also consider applying another level of protection known as 2-Step Verification (2SV) on your accounts, which will prevent anyone accessing your accounts even if they know your password. The following link will support you through adding 2SV to your online accounts.

Setting up 2-Step Verification (2SV) - NCSC.GOV.UK

The following link will take you to an easy to read infographic produced by the NCSC titled – Using passwords to protect your devices and data.

Using passwords to protect your devices and data (ncsc.gov.uk)

This Cyber Byte was sent out for your information by

Police Scotland Cybercrime Harm Prevention Team -
PPCWCyberHarmPrevention@scotland.police.uk

All information was correct at time of distribution.