Cyber Safety Fact Sheet: Strong Passwords

Some criminals try to steal from people or businesses by accessing information held securely online. Passwords, when implemented correctly, are an effective way to prevent unauthorised users accessing your information. However, if your password is discovered, the security of your personal, financial or business information could be in danger. If your email is hacked, it could be used to impersonate you, to re-set your other passwords or to defraud your contacts.

Many cases where someone's password has been compromised have occurred where an attacker cracked someone's password on a low-security site, but the victim had used the same password for another, high-value site. Therefore you should take care to use different passwords for each site, especially your email, your bank and any sites that hold confidential or financial information.

So what makes a good password?

Using your pet's name, your street name or a random word may be easy to remember, but can also be easy to crack. If your passwords are dictionary words, pet names or place names, experienced hackers can easily generate these possible passwords to try to access your account.

Your passwords will be more secure if they are a collection of numbers, letters and symbols that don't resemble a dictionary word. A way to create such passwords is to choose a memorable phrase and convert it.

For example, Sue and Ron married at St John's Church in 1995 could convert to: *S&R@StJ95*

Alternatively, pick a phrase or lyric that you can remember, for example "Hello, is it me you're looking for?" and take the first character from each word to get 'H,iimylf?'.

However, the need to remember large numbers of unique strings of characters (remember, a different password for each account) makes things difficult. According to advice given by CESG (the National Technical Authority), the average person in the UK has 22 online passwords.

While keeping your more sensitive passwords totally unique, you could think of a system for your other passwords, such as adding letters from the website's name to a core password,

eg. if your core password is ABC&123, then on the **B**BC site, your password becomes ABC&123**B**

The more complex your system, the better. Here are some do's and don'ts to be considered.

Do:

- Choose a password that is at least eight characters in length (the longer the password, the harder it is for criminals to break it, so the longer the stronger)
- Use a combination of upper and lower case letters, numbers and symbols (@ # $ % ^ &). Remember that changing letters to numbers (E to 3 and i to1) is well-known to criminals.

Don't use the following as passwords:

- Your username, actual name or business name.
- Family members' or pets' names or birth dates
- Your favourite football or sports team or other words easy to work out with a little background knowledge about you, for example things related to your interests.
- Numerical or keyboard sequences, such as 12345678.
- A single dictionary word, these are easily cracked by common hacking programs.
- When choosing numerical passcodes or PINs, do not use ascending or descending numbers (eg. 4321), duplicated numbers (eg. 1111) or easy keypad patterns (eg. 14789 or 2580).

Note: The most common passwords are 123456, password, 12345678, qwerty, 12345, football.

Protecting Your Passwords

There are a number of things that you need to do to ensure that your passwords are protected – remember, they are the keys to the valuable information that you want to protect. These include:

- **Ensure you use a unique and strong password for your email**, because, if compromised, your email could be used to reset or change many of your other passwords (via the "forgot password" option on many sites, which enables a new password to be set up via your email)
- Only consider using a browser's "remember password" facility on a machine that you are the sole user of, or one where you entirely trust all the other users. Never use this on public computers, eg. in a library or café.
- Beware public WiFi. Don't log onto secure sites when using public WiFi, as they may not be secure. If you need to log into a site when out and about, use 3G/4G or a VPN.
- Never visit and log into a secure site, such as your bank, as a result of an emailed link. Email links are a common way to send people to fake websites that look like the real thing, so their log in details can be captured. When visiting a site to log in, always go there via your browser.
- Before you enter a password into a website, ensure it is using a secure connection beginning with https:// (it might also show a small padlock beside the address) this means the site is using a secure link.
- Don't enter your password when others can see what you are typing (shoulder surfing).
- Never send your password by email.
- Don't share passwords with other people, or leave your passwords lying around in notebooks near to your computer, or in files on your computer where they can easily be found and read.
- If you must write passwords down to remember them, ensure they are stored securely (in a safe). Don't store it on your smartphone or in an unencrypted file on your phone or computer.
- Don't recycle passwords (use them again after a break).
- In the past, the advice was that you should routinely change your passwords, however, this is no longer recommended, unless the accounts to which they apply have been hacked, in which case they should be changed immediately.
- Consider using an online password vault or safe, but only use a reputable organisation.

Given the difficulty in creating and remembering good passwords, one alternative is to use a password manager such as LastPass, Dashlane and 1Password[1], which also have built in password generator tools. Password managers store all of your passwords for you and will automatically fill out your log-in forms so that you don't have to do any memorizing apart from the master password that you will use to access the password manager. It's worth noting, however, that like any other software, password managers are vulnerable to breaches. In 2011, LastPass experienced a security breach, however, users with a strong master password were not affected.

Consider using two-step-authentication

Any time a service like Facebook or Gmail offers "two-step verification," use it. When enabled, signing in will require you to also enter a code that's sent as a text message to your phone. This means that a hacker who isn't in possession of your phone won't be able to sign in, even if they know your password. You only have to do this once for "recognized" computers and devices.

There is no perfect answer to the problem of passwords but the application of the measures listed above will help you to improve the security that you get from them. Even then, all passwords can eventually be broken, given enough time and resources.

Government advice on passwords can be found at https://www.ncsc.gov.uk

[1] https://www.lastpass.com/ https://www.dashlane.com/ https://1password.com/