GCA Cybersecurity Toolkit Backgrounder: Beyond Simple Passwords Toolbox

One of the most common methods criminals will use to gain access to your accounts, network, and information is to log in as you. It is really important that you use unique, strong passwords (or passphrases) for each of your accounts and that you keep these passwords private, safe, and that you never reuse them.

- Reusing the same password across multiple accounts means that if a criminal gets hold of one of your passwords, they've effectively gained access to all of your accounts.
    - *The same username and password will be tried across many common applications.*

There are many techniques criminals will use to gain access to your passwords. There is also a very active market on the Internet (sometimes referred to as the 'dark web') for buying and selling this personal information should one of the companies with whom you hold an account be breached.

Methods used include:

- **Brute force attack**: Using computing power to automatically enter all possible combinations.
    - *Use long passwords or passphrases and special characters to make this more difficult.*
- **Dictionary attack**: A form of brute force attack that uses known dictionary words/phrases or common passwords.
    - *Use memorable words/passwords but not ones from a dictionary, common ones, or ones that might be associated with you.*
- **Credential stuffing**: Once one account has been compromised, they will try the same username/password elsewhere.
    - *Use a different password for each account as well as additional protection (2 Factor Authentication – 2FA) for accounts that have this facility.*
- **A phishing email:** i.e., 'Time to reset your password' with links to a malicious website or a keylogger installed by opening a malicious attachment (a keylogger will track your use of the keyboard).
    - *Be wary of opening, clicking on links, or downloading from any email even if they appear from people or organizations you are familiar with.*

- **Social Engineering**: Professionals are very skilled at manipulating conversations and using a variety of media (a phone call, text message, or social media) to trick you into revealing your passwords and other personal information by pretending to appear legitimate.
    - *Never give out your password, or parts of it, to anyone. A legitimate company will not ask.*
- **Manual Guessing**: Personal information, i.e., if names and dates of birth are used as part of your password.
    - *Don't be too personal with passwords – think about what the web and social media might reveal about you and avoid using that information in your passwords.*
- **Shoulder Surfing**: In a public place, or even at your desk, there may be someone 'eyesdropping' on your activity.
    - *Check who might be behind or next to you, or where a camera might be present, particularly while entering sensitive information.*
- **Interception**: Passwords can be intercepted as they are transmitted over a network.
    - *Check for the https padlock sign on websites and take care using Wi-Fi in public places; they may be insecure or 'hijacked' with lookalike names enabling others to 'see' what you are transmitting.*

Computing power has increased exponentially over time, as has our use of the Internet and social media. All this has made it quicker and easier for criminals to gain access to your information:

	1984 Apple MacIntosh PC:	2019 iMac 'Core i5' (standard)	Difference:
RAM:	128K	8G	64,500,000% increase
Processing speed:	8MHz	3GHz	37,400% faster
Cost:	$2,500	$1,500	40% reduction

- Rapid technology advancement has really worked to hackers' advantage because a modern laptop and program can crack a password faster than ever.
    - *The need to keep up with longer, more complex passwords and additional methods of protection increases alongside this advancement in technology.*

Two Factor Authentication (2FA):

2FA provides a secondary level of protection making it much harder for an attacker to gain access to your accounts because it is reliant on:

- Something you know:
    - A password
- And/or something you have:
    - A token (Google Authenticator, Okta, RSA)
    - A verification code sent to your phone (SMS)

- Or something you are:
    - A fingerprint or face (biometrics)

2FA requires this before it gives access, which provides an extra layer of defense.

There is plenty of guidance available for creating long, strong passwords or passphrases. Whatever guidance you adopt, make sure to:

- Ensure you have a strong company-wide policy and a system that prohibits the use of weak passwords.
- Steer clear of pet names or passwords that could be guessed through social media.
- Use a different password for every account.
- Consider using a password manager to store your passwords if you prefer.

Additionally:

- Update your passwords on any accounts where you have been compromised (you can check this via the 'Have I Been Pwned' tool in the toolbox).
- Delete accounts and uninstall applications that you no longer use.
- Ensure strong and unique passwords on all your accounts.
- Enable 2FA on all your accounts (where 2FA is supported).
- Check your remotely accessible devices for admin/admin default settings. Always change guessable default passwords before first use.

Use the tools in the Beyond Simple Passwords Toolbox for guidance, to check whether any of your accounts are known to have been compromised, and to help you implement improvements.

https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/