Office of Cyber-Security & Information Assurance

Office of Cyber-Security
& Information Assurance

Guidance Document

Issue Date 6th July, 2020

TLP: WHITE

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE

WHITE **Public** - May be distributed freely, without restriction.

5 Steps to Cyber Security: Step 1 - Protect Your Data Using Passwords

Passwords are the primary method we use to protect and access our data, devices and online services. Unfortunately, with the large amount of passwords we have to keep track of, people often create short, weak passwords and re-use the same password for their accounts.

Strong passwords and additional account security measures are an effective way to prevent unauthorised access to computers, devices, networks and data. This guidance document covers some basic recommendations for protecting your data with passwords.

Creating strong passwords and securing your data

- The UK National Cyber Security Centre (NCSC) recommends creating your passwords using **three random, but memorable, words**.

  By using a mixture of **upper and lower case characters, numbers and special characters** (£, $, ?, !) the strength of the password increases considerably, e.g. B1cycleSh0ePark!

- Create **unique passwords for all your important online accounts** such as your email, bank, social media, and any other service that stores personal information, banking or credit/debit card details.

- Before purchasing electronic devices, particularly those connected to your network and the Internet, **consider the security features**. Can you change the default password and is it capable of being updated?

- Change default passwords on all new devices and update them to ensure you are using the latest software. Regularly check for updates or set them to automatically update.

Office of Cyber-Security & Information Assurance (OCSIA)
OCSIA@gov.im (01624) 685 557

- Ensure all your computers and electronic devices are **password or PIN** protected. Where available**, use encryption features or software**. Consider encrypting your data when transferring from one party to another, particularly if the data is sensitive or contains personal information.

  Microsoft Windows 10 (excluding Home Edition) has a built in encryption feature called BitLocker on supported systems. **BitLocker will encrypt the data on your computer when not in use**. More information about BitLocker can be found here: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview-and-requirements-faq

  Instructions on how to set BitLocker up can be found here: https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

  Apple iOS and iPadOS devices use a file encryption methodology called Data Protection, while the data on Mac computers can be protected with an encryption technology called FileVault, which will encrypt your startup disk. More information about FileVault and instructions on how to turn this on can be found by visiting, https://support.apple.com/en-us/HT204837

Looking after your passwords

- If writing down your passwords, **ensure they are stored somewhere safe**, out of sight and away from the computer or device it is for. Organisations should consider providing a secure place for staff to store their passwords.

- It is not necessary to enforce regular password changes. If you suspect a compromise, then you should request that users change their passwords.

- Most popular web browsers will store passwords for you. They will also warn you if you are attempting to visit a website known to be malicious or dangerous.

- **Consider using a password manager**. This software can create and store very strong passwords for your online accounts and applications, so you just need to remember one strong password. A list with a table of comparison for a large number of password managers can be found at: en.wikipedia.org/wiki/List_of_password_managers

Multi-factor authentication (MFA)

Multi-factor authentication (MFA), also referred to as two-factor authentication (2FA), provides an extra layer of security to your accounts by confirming the identity of the user.

It is based on using a combination of **"what you know"** (e.g. password), **"what you have"** (e.g. mobile phone, key card) and **"what you are"** (e.g. fingerprint, facial recognition). Using at least two of these makes it more difficult for criminals to access your accounts.

Instructions on how to set up MFA across popular online services such as Gmail, Facebook, and LinkedIn can be found on this website: www.telesign.com/turnon2fa/

If your password has been stolen

- **Change your password** on any accounts using the stolen password.
- You can check to see if your information has ever been made public in a major data breach using the Have I Been Pwned website: www.haveibeenpwned.com/

If you have any concerns, or have been affected by a cyber-related issue, report it to the Office of Cyber-Security & Information Assurance (OCSIA) by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia.

Office of Cyber-Security & Information Assurance (OCSIA)
OCSIA@gov.im (01624) 685 557