Ledgard Consulting

FACT SHEET

No 053/ Ver: 1.0
Topic: General

Passwords

Introduction

A strong password is the first line of defence against cyber threats. Here's how to create and manage strong passwords:

Creating Strong Passwords:

1. **Length:** Aim for at least 12 characters, ideally 15 or more.
2. **Complexity:** Combine uppercase and lowercase letters, numbers, and special symbols. Alco can be three words separated by dots or hyphens, But bear in mind that some sites have very specific specifications for the passwords used on their site, so you should not use the same password every time, you also may not be able to use the same format of password every time
3. **Avoid Personal Information:** Don't use easily guessable information like birthdays, names, or pet names. Also, when creating an email address, it is generally acceptable to include some identifier for your name such as “firstname.surname@gmail.com. Do not use information such as Date of Birth or even year of Birth.
4. **Unique Passwords:** Use a different password for each account to minimise the impact of a breach and change regularly if possible, but also remember that if you do change a password, also change it in your Password Manager App

Password Management Best Practices:

5. **Two-Factor Authentication (2FA):** Enable 2FA whenever possible to add an extra layer of security.
6. **Regular Password Changes:** Periodically update your passwords, especially for critical accounts.

7. **Beware of Phishing Attacks:** Be cautious of suspicious emails and links that may trick you into revealing your passwords.
8. **Secure Your Password Manager:** Protect your password manager with a strong, unique master password. Make sure you write this down somewhere, say in a safe. It is also prudent to leave this master password in your Will envelope, as your dependents would be able to access the Password Manager and subsequently access all your other accounts. (Only if this is your wish of course). ***Ledgard Consulting has developed a legacy system for saving and accessing important documents and information for your surviving dependents after your death.***
9. **Offline Backup:** Consider creating an offline backup of your password manager's database in case of emergencies.

Tips for Remembering Strong Passwords:

The recommendations are that for each website, we have a unique password, ie, do not use the same one. The number of websites which the average person uses these days is growing, so remembering all the different passwords is impossible.[1] So people have to store their passwords somewhere. By far the best option is to use a Password Manager, such as 'BITWARDEN'

10. **Password Phrase:** Create a memorable phrase and use the first letter of each word to form a strong password.
11. **Password Generator:** Use a built-in or third-party password generator to create complex passwords.
12. **Mnemonic Devices:** Use mnemonic techniques like acronyms or visualiations to remember complex passwords.
13.

Biometrics:

Biometrics have become a cornerstone of phone security of late, providing a robust and user-friendly way to safeguard devices

Types of Biometric Security on Phones:

Fingerprint Recognition

[1] In terms of IT support, forgetting and recovering passwords is the most common activity, even though there are mechanisms to do this, the recovery options are not always set up in the first place. Ie, phone number or email.

14. The users place their finger on a sensor, which scans the unique patterns and ridges of their fingerprint. (the fingerprint/s must have been stored previously)
15. The fingerprint can be used to unlock the phone and authorise some transactions (say on the Banking App) or to pay on the Tap and Go at a shop (Apple Pay and Google Pay)

•

Facial Recognition

16. The phone's camera captures, analyses and stores unique facial features using advanced algorithms.
17. Just looking at the front camera can unlock the device

Advantages of Biometric Security

18. There are advantages to Biometric Security, as all the elements are unique to each individual and difficult to replicate, making unauthorised access less likely compared to traditional passwords or PINs.
19. Biometrics make unlocking a device quick and easy, . there's no need to remember complex passwords or PINs, making the user experience smoother.

Two-Factor Authentication (2FA):

Biometrics can be combined with other authentication methods, such as passwords, for added security. This means even if someone knows your password, they still need your biometric data to access the phone.

Secure Data:

Biometric data is stored securely on the device, often in a dedicated security chip (like Apple's Secure Enclave or Android's Trusted Execution Environment), ensuring it can't easily be extracted or misused. Manufacturers continuously update biometric systems to address new threats and improve accuracy so devices must be kept up to date. By integrating biometrics, phones can provide a higher level of security while maintaining user convenience. This technology continues to evolve, making it an increasingly reliable option for protecting personal data on mobile devices.

Password Manager:

Use a reliable password manager to generate, store, and autofill strong, unique passwords. 'BITWARDEN' is the recommended manager to use, it is free and it can be used on computers, phones and tablets, all synchronised together and you only have to remember one Master Password. However, there is no recovery option for this. So **DO NOT FORGET IT.** You can backup (or EXPORT) your Bitwarden Vault and restore from that if needs be. BITWARDEN also generates complex passwords for you and can auto-populate websites for easy access. Can store sensitive notes, bank details and secure notes all protected by your Master Password. Some applications also store passwords, such as Browsers and Dropbox has a system now. More details of BITWARDEN is contained in Appendix C.

By following these guidelines, you can significantly strengthen your online security and protect your sensitive information. Remember, a strong password is an essential component of a comprehensive cybersecurity strategy.

Passkeys:

Passkeys are a new type of digital credential that are designed to replace passwords. They are more secure and convenient to use than passwords, and a growing number of websites and apps is adopting them.

How passkeys work:

Creation:

When you create a passkey for an account, your device generates a pair of cryptographic keys. One key is public, and the other is private. The public key is stored on the server, and the private key is stored on your device.

Authentication:

When you want to sign in to an account with a passkey, you will be prompted to unlock your device. This could be by using your fingerprint, face recognition, or a PIN code. Once you have unlocked your device, the private key is used to sign a message that is sent to the server. The server verifies the signature using the public key, and if the signature is valid, you will be granted access to your account.

Security:

Passkeys are more secure than passwords because they are not stored on the server, eliminating the risk of unauthorised access. This means that they cannot

be stolen in a data breach. Passkeys are also resistant to phishing attacks, as they are tied to a specific website or app.

Passkeys are a promising new technology that has the potential to significantly enhance online security and convenience. They are easy to use and they are more secure than passwords. If you're looking for a more secure way to sign in to your accounts, consider using passkeys.

How to Set Up a Passkey:

To set up a passkey, the process can vary slightly depending on the specific website or app you're using. However, this is a general guide:

1. Enable Passkey Support:

20. **Check Compatibility:** Ensure your device and browser support passkeys. Most modern devices and browsers are compatible; however, it's recommended to check for updates.
21. **Enable in Settings:** Some websites and apps might require you to enable passkey support in your account settings.[2] Look for options related to security or login methods.

2. Create a Passkey:

1. **Sign In:** Log in to the website or app using your existing credentials (username and password).
2. **Initiate Passkey Setup:** Look for an option labelled "Add Passkey," "Set Up Passkey," or a similar phrase.
3. **Device Authentication:** You'll likely be prompted to authenticate your device using biometric authentication (fingerprint, face recognition) or a PIN code.
4. **Confirm Passkey:** Review the information associated with the passkey, such as the website or app name.
5. **Complete Setup:** Follow the on-screen instructions to finish creating the passkey.

3. Use Your Passkey to Sign In:

1. **Select Passkey Option:** When logging in, choose the "Sign in with Passkey" or similar option.
2. **Device Authentication:** Again, authenticate your device using your preferred method.
3. **Verification:** The website or app will verify your identity and grant you access.

Additional Tips:

- **Multiple Devices:** You can set up passkeys on multiple devices, allowing you to sign in from different computers or phones.[3]
- **Password Manager Integration:** Some password managers support passkey storage and synchronization.[4]
- **Security:** Always keep your device and biometric authentication secure.

Specific Examples for Google and Microsoft

- **Google Account:**
  1. Go to https://myaccount.google.com/signinoptions/passkeys
  2. Click "Create a passkey"
  3. Follow the on-screen instructions.

- **Microsoft Account:**
  1. Sign in to your Microsoft account.
  2. Go to Security settings.
  3. Choose "Add a new way to sign in or verify."
  4. Select "Face, fingerprint, PIN, or security key."
  5. Follow the instructions to set up a passkey.

By following these steps and keeping your devices secure, you can enhance your online security and simplify the login process with passkeys.