Password Creation & Management Checklist

Passwords and pins are how most of us log on to services at work, home, and when we are out and about. It is important to follow the do's and don'ts of password creation & management below.

DO'S

- □ The longer the password the better - length trumps complexity
- □ Create passwords with a combination upper and lowercase letters, numbers, punctuation, and special symbols
- □ Do not share your passwords with anyone
- □ Create a new password for every service that you use
- □ Use the 'Maths Method' to create memorable passwords like "*830-630=TwoHundred*"
- □ Check if your password is strong enough at https://password.kaspersky.com/
- □ You can check if any of your passwords have been breached at https://haveibeenpwned.com
- □ Ensure the password for your email account is long, complex and not shared - this is the key to the kingdom. If cracked all other accounts can be controlled.

DONT'S

- □ Use personal information like pets or kids names, publicly shared birth dates etc.
- □ Re-use passwords across accounts (if one account becomes compromised they all will)
- □ Save passwords in emails or browsers

PASSWORD MANAGER

- □ Get a password manager (think of this like an online safe box where you store your passwords)
- □ You will only need to remember one master password to access the password manager
- □ LastPass has a free option & generates passwords for you; https://www.lastpass.com/

safeireland
Creating safety for women and children

Cyber Awareness Ireland