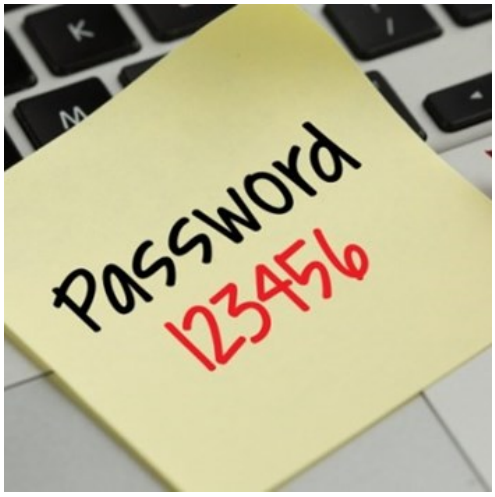
Heddlu Police
DYFED-POWYS

Passwords



Passwords can only do so much, even when implemented correctly; passwords are limited in helping prevent unauthorised access. If an attacker discovers or guesses your password, they are able to impersonate you!

A few words about Passwords

1. **Boring** – Yes, everyone knows that they are a pain and no one wants to be told any more about them.
2. **Essential** – Yes, nothing in life seems to work without a password anymore.
3. **Key to your Digital front door** – Think of your password as just that – if you use a simple password and use it on multiple accounts – it's the same as having the same key for everything you have in the real world – and if you lose that key or someone finds it and uses it – they have access to all of your doors and drawers. If someone guesses or hacks your password – how many digital doors and drawers can they open?

4. **What's the worst that could happen? -** Using your email address and password, criminals can lock you out of your online life, pretend to be you and even sell your accounts.

Heddlu Police
DYFED-POWYS

Be Cyber Savvy, Not Cyber Sorry.
Passwords need to be strong secure and unique to each account

If someone knows or guesses your password, then they will have access to that online account.

So if you used the same password on more than one account, the criminal now has access to those accounts as well.

"It won't happen to me, I live in Dyfed Powys, and cyber criminals aren't interested in me".

Hundreds of Cyber related incidents are reported to Dyfed Powys Police each year and those are just the ones we know about, many are never reported.

- PINs and passwords are your first line of defence on your computer, mobile device, apps, online bank accounts and social media.
- Create passwords that are strong, don't share them and use a different one for every online account in case one or more gets hacked.

One secure password for all accounts is not the answer. If you use the same password on all of your accounts, no matter how strong it is; if that one password gets hacked or known, all of your accounts are now at risk.

Instead of creating extremely long and complex passwords, choose three random words. Examples used on the NCSC website are: 'coffeetrainfish' or 'walltinshirt'.

Avoid using easy to guess passwords, such as 'onetwothree' or the names of family members or pets as this will make you an easy target for hackers.

You can write it down safe and securely – not the best solution, but it's better than having one easy to guess password – if you do it this way, use a little black book that you keep safe somewhere. You could use a Word document which is password protected or possibly look at using a Password Manager.

Heddlu Police
DYFED-POWYS

Google, 'Password Managers' to find out more or visit the websites mentioned below:

- https://www.howtogeek.com/445274/how-safe-are-password-managers/
- https://www.getsafeonline.org/blog/password-managers-how-to-remember-all-your-passwords-by-remembering-only-on/

Whatever you do – make sure you have a unique and strong password for each of your online accounts. In that way you are making yourself a much harder target for the cyber criminal and 95% less likely to get hacked in the future.

Next time we will look at **Two Factor Authentication (2FA)** – but until then, take some time to look at sorting your passwords out.

Some light relief…

You Should Probably Change Your Password! | Michael McIntyre Netflix Special - https://www.youtube.com/watch?v=aHaBH4LqGsI