

## Cyfrineiriau



Dim ond hyn a hyn y gall cyfrineiriau wneud, hyd yn oed pan maen nhw wedi'u gweithredu'n gywir; mae cyfrineiriau wedi'u cyfyngu o ran helpu i atal mynediad heb awdurdod. Os yw ymosodwr yn darganfod neu'n dyfalu'ch cyfrinair, mae'n medru'ch dynwared!

### Ychydig eiriau am Gyfrineiriau

1. **Diflas** – Mae pawb yn gwybod eu bod nhw'n boen a does neb eisiau clywed mwy amdany'n nhw.
2. **Hanfodol** – Mae'n ymddangos fel pe na bai unrhyw beth yn gweithio heb gyfrinair bellach.
3. **Allwedd i'ch drws ffrynt digidol** – Dyna sut ddylech chi drin eich cyfrinair – os ydych chi'n defnyddio cyfrinair syml ac yn ei ddefnyddio ar gyfer sawl cyfrif – mae hynny fel cael yr un allwedd ar gyfer popeth sydd gyda chi yn y byd go iawn – ac os fyddwch chi'n colli'r allwedd hwnnw, neu mae rhywun yn dod o hyd iddo ac yn ei ddefnyddio – mae ganddo fynediad i'ch holl ddrysau a dreiriau. Os oes rhywun yn dyfalu'ch cyfrinair neu'n ei hacio – sawl drâr a drws digidol maen nhw'n medru agor?



4. **Beth yw'r gwaethaf a all ddigwydd?** – Gan ddefnyddio'ch cyfeiriad e-bost a'ch cyfrinair, gall troseddwr eich cloi chi allan o'ch bywyd ar-lein, eich dynwared, a hyd yn oed gwerthu'ch cyfrifon.

### **Byddwch yn seiber-graff!**

Mae angen i gyfrineiriau fod yn gryf, yn ddiogel, ac yn unigryw ar gyfer pob cyfrif.

Os oes rhywun yn gwybod eich cyfrinair, neu'n ei ddyfalu, bydd ganddo fynediad i'r cyfrif ar-lein hwnnw.

Felly, os ydych chi wedi defnyddio'r un cyfrinair ar gyfer mwy nag un cyfrif, mae gan y troseddwr fynediad i'r cyfrifon hynny hefyd yn awr.

### **"Bydd e ddim yn digwydd i fi, rwy'n byw yn ardal Dyfed-Powys, a does dim diddordeb gan droseddwr seiber ynof i".**

Mae Heddlu Dyfed-Powys yn derbyn cannoedd o adroddiadau bob blwyddyn am ddigwyddiadau seiber, a dim ond y rhai yr ydym yn gwybod amdanynt yw'r rheini. Mae llawer byth yn cael eu hadrodd.

- Rhifau PIN a chyfrineiriau yw'ch amddiffyniad cyntaf ar eich cyfrifiadur, dyfais symudol, apiau, cyfrifon banc ar-lein a chyfryngau cymdeithasol.
- Crëwch gyfrineiriau sy'n gryf, peidiwch â'u rhannu, a defnyddiwch un gwahanol ar gyfer pob cyfrif ar-lein rhag ofn bod un neu fwy'n cael eu hacio.

Nid un cyfrinair diogel ar gyfer pob cyfrif yw'r ateb. Os ydych chi'n defnyddio'r un cyfrinair ar gyfer eich holl gyfrifon, os yw'r cyfrinair hwnnw'n cael ei hacio, mae'ch holl gyfrifon yn awr mewn perygl.

Yn hytrach na chreu cyfrineiriau hir a chymhleth iawn, dewiswch dri gair ar hap. Mae enghreifftiau a ddefnyddir ar wefan y Ganolfan Seiberddiogelwch Genedlaethol yn cynnwys: 'coffitrenpysgodyn' neu 'waltincrys'.

Osgowch ddefnyddio cyfrineiriau sy'n hawdd eu dyfalu, megis 'undautri' neu enwau aelodau o'r teulu neu anifeiliaid anwes gan y bydd hyn yn eich gwneud chi'n darged hawdd ar gyfer hacwyr.



Medrwrch eu hysgrifennu'n saff a diogel - nid dyma'r datrysiad gorau, ond mae'n well na chael un cyfrinair sy'n hawdd ei ddyfalu - os fyddwch chi'n gwneud hyn, defnyddiwch lyfr bach du yr ydych yn ei gadw'n ddiogel rhywle. Fe allech ddefnyddio dogfen Word a reolir gan gyfrinair, neu fe allech ystyried defnyddio Rheolwr Cyfrineiriau.

Teipiwch 'Rheolwyr Cyfrineiriau' i mewn i beiriant chwilio er mwyn cael rhagor o wybodaeth, neu galwch heibio i'r gwefannau a nodir isod:

- <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/>

Beth bynnag a wnewch – sicrhewch fod genych gyfrinair unigryw a chryf ar gyfer eich holl gyfrifon ar-lein. Fel yna, rydych chi'n gwneud eich hun yn darged llawer anoddach i'r troseddwr seiber a 95% yn llai tebygol o gael eich hacio yn y dyfodol.

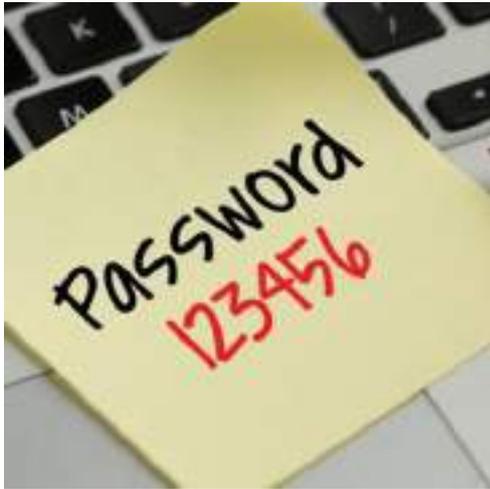
Y tro nesaf, byddwn ni'n edrych ar **Brawf Dilysu Dau Gam** – ond tan hynny, treuliwch ychydig o amser yn edrych ar eich cyfrineiriau a rhoi trefn arnynt.

### Rhywfaint o adloniant ysgafn...

Mae'n Siŵr y Dylech Newid Eich Cyfrinair! | Rhaglen Arbennig Michael McIntyre ar Netflix - <https://www.youtube.com/watch?v=aHaBH4LqGsI>



## 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.

### **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.

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>

