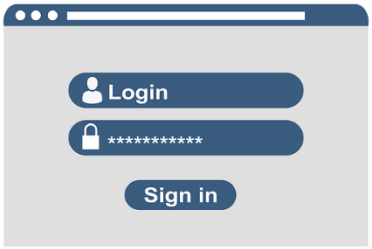
Change Your Password Day.

In 2012, Matt Buchanan came up with the idea of “Change your password day”, mainly for raising security awareness because of the increase of hackers' attacks on private and public targets.

By now, we should all know the importance of why passwords should be changed regularly, yet they are often neglected by people every day. Unfortunately, the benefits of updating your password are trumped by the inconvenience of remembering a new log in to a multitude of different accounts.



Not only is it advised to change your password every three to four months, but they should also be unique and hard to crack. Although it might be nice and easy to remember, avoid using personal information like your first name, surname or date of birth. Also, using memorable keyboard paths like qwerty or asdfgh are big no-no’s too! Try to combine different unrelated words, letters and symbols in your password to ensure your computer, email account or whatever it may be, has the best chance of protection against hackers and malicious software.

Creating various passwords for different services is always best practice. If you recycle your passwords or think you are safe by just switching the odd character, you are most likely not. Tatler explain ‘’the first thing hackers will do is try their luck by using a password they’ve obtained on other digital platforms.’’

Speaking of best practice, Techarrival suggest the following 11 important tips for password security:

1. More Cybersecurity Experts = Better Protection
2. Academic Education
3. Non-Formal/Workplace Education
4. Better Passwords
5. Cyber Hygiene
6. Don’t Use One Password for All of Your Accounts
7. Password Managers Are Here to Help
8. Don’t Fall for the Bait!
9. Protect Your Personal Data on Social Networks
10. Don’t Make Your Posts Public
11. Separate Your Work Email from Your Private Email

In 2021, it was predicted that a cyber-attack took place every 11 seconds with damages from ransomware attacks alone exceeding $20 billion worldwide, a whopping 57 times more than in 2015 (sumologic). Forbes unfortunately predicts continuous and worsening cybercrime in 2022 with high risks posed to both individuals and businesses. Whilst intimidating information, fortunately there are measures that can be taken to protect ourselves against these threats; firewalls, anti-virus software and training for people and employees on everyday efforts like having a strong and short-term passwords in place.

It’s more important than ever to keep safe in our digital world.