MCAST

A strong P@$$W0rd doesn’t (always) work

MCAST Freshers’ Week 2021

MCAST HackSpace

Basic Security Hygiene

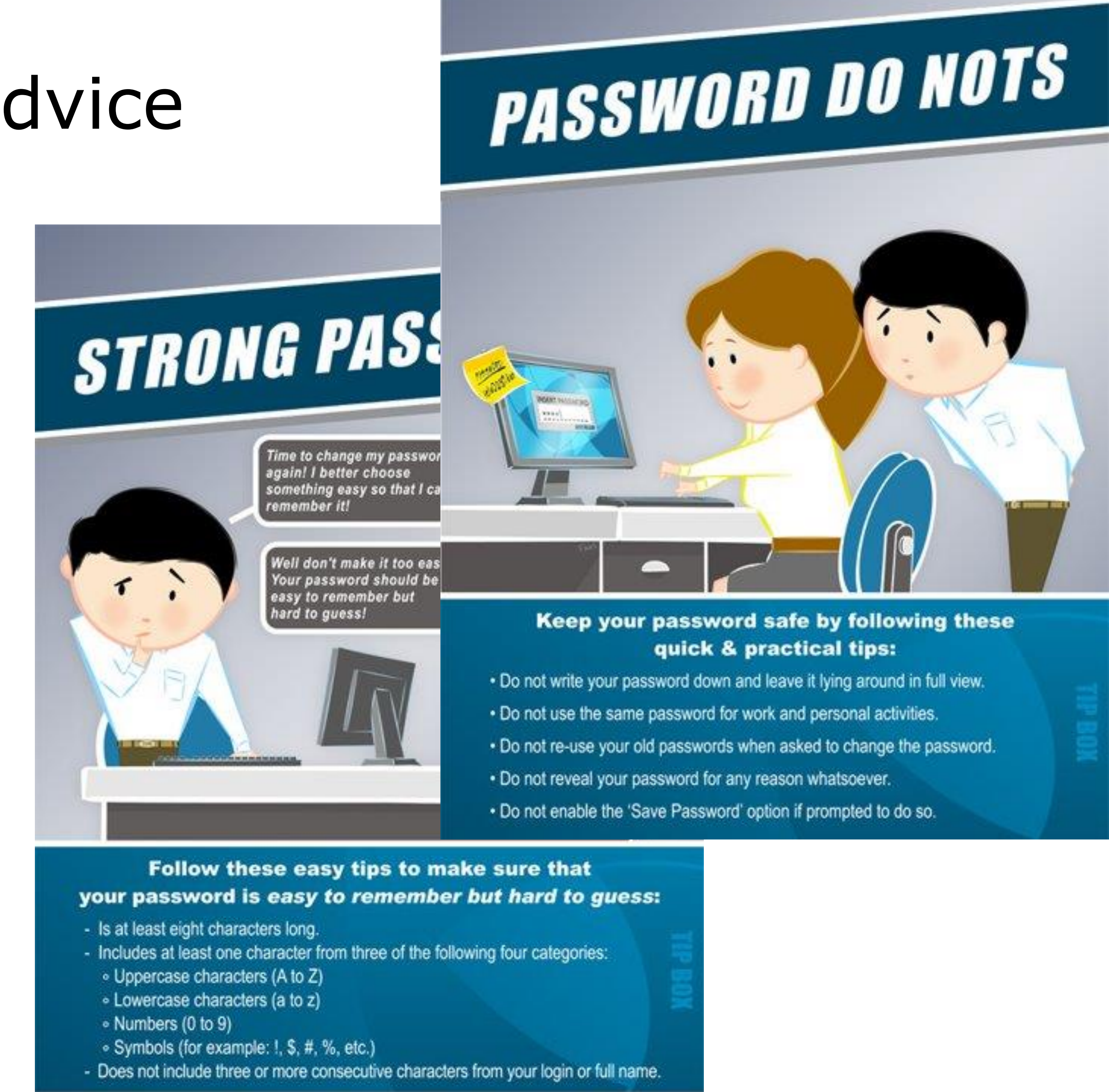
- Apply software updates
- Install anti-malware
- Use complex passwords

“I do all that, I’m ok right?” ...Not so fast

Traditional Security Advice

Passwords must be "easy to remember" **but also**:

- Longer than 8 characters
- Have uppercase
- Have lowercase
- Have numbers
- Have symbols
- Not include your username
- Not used elsewhere
- Not written down...


STRONG PASS
Time to change my passwor again! I better choose something easy so that I ca remember it!
Well don't make it too eas Your password should be easy to remember but hard to guess!
TIP BOX
PASSWORD DO NOTS
TIP BOX

Follow these easy tips to make sure that your password is *easy to remember but hard to guess*:

- Is at least eight characters long.
- Includes at least one character from three of the following four categories:
  - Uppercase characters (A to Z)
  - Lowercase characters (a to z)
  - Numbers (0 to 9)
  - Symbols (for example: !, $, #, %, etc.)
- Does not include three or more consecutive characters from your login or full name.

Keep your password safe by following these quick & practical tips:

- Do not write your password down and leave it lying around in full view.
- Do not use the same password for work and personal activities.
- Do not re-use your old passwords when asked to change the password.
- Do not reveal your password for any reason whatsoever.
- Do not enable the 'Save Password' option if prompted to do so.

Choosing a P@$$W0rd: Common Patterns

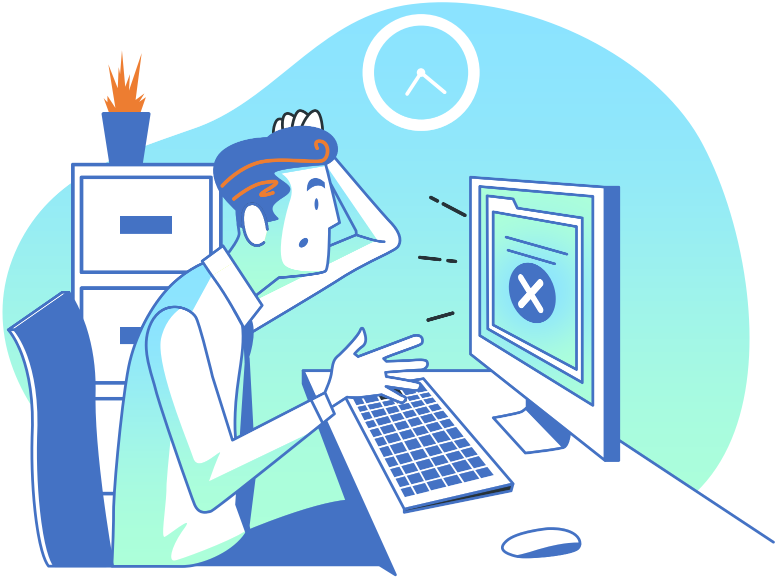
- Numbers? You'll likely add a "1" at the end.
- Capital letters? You'll probably make it the first one in the password.
- And special characters? Frequently exclamation marks.
- Length? Sequence of keys.
- Password expired? Add a number at the end.

Choosing a P@$$W0rd: Most used

- When passwords are hacked, researchers enjoy finding the most common ones.
- Can you see any of your passwords in the list?

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. 696969
18. shadow
19. master
20. 666666
21. qwertyuiop
22. 123321
23. mustang
24. 1234567890
25. michael
26. 654321
27. pussy
28. superman
29. 1qaz2wsx
30. 7777777

Problem & Solutions



I have 200+ accounts with a password and I have bad memory.

I don’t remember any my passwords (with the exception of two).

Use a Password Manager

- A password vault, locked by a master key.
- You only need to remember the master key, all passwords can be very complex.
- Automatically synchronised across multiple devices and browsers.

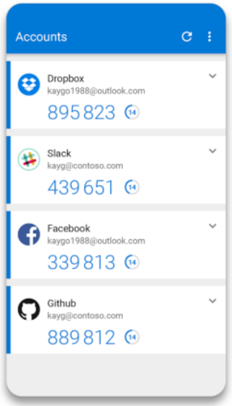
bitwarden
LastPass
1Password
Firefox Lockwise
KeePass
Password Safe
DASHLANE

Use Ridiculously Complex & Unique Passwords

- Typical password cracking performance (source):
  - 6 characters -> 8 seconds
  - 8 characters -> 20 hours
  - 10 characters -> 21 years
- Don’t reuse passwords, let the password manager generate them.
- You should not be able to remember your passwords! A password should look like this: A6Y)P(A98yf:2p@p`{3Gkt_"

Use Multi-Factor Auth

- Users confirm their identity with a one-time code, sensor or USB token.
- Guessing/stealing the password is not enough for an attacker to gain access.
- Is quickly becoming a standard in the move towards a password less world.



Accounts

Dropbox
kaygo1988@outlook.com
895 823

Slack
kayg@contoso.com
439 651

Facebook
kaygo1988@outlook.com
339 813

Github
kayg@contoso.com
889 812

> “Join MCAST **Hack**Space to learn more about protecting yourself online”

https://hackspace.mcast.edu.mt