A Short Guide to Passwords: Part 1

Why do we need good passwords?

- We are often told our passwords should be complex and unique, but why?
- Complex passwords are harder for other people to guess – although not much harder for a computer 'brute force' attack; more on this later.
- Unique passwords protect us if a single password is compromised.

How are passwords attacked?

- Less likely: someone trying to guess (or crack) an individual password eg for your email account or online bank – this is not efficient for the attacker.
- More likely: attackers use lists of known compromised passwords and try to gain access to many services at once – this is much easier if people reuse the same or similar password for several services (all too common!)
- Also likely: attackers will try common variations of known passwords, such as swapping letters for numbers (eg E -> 3) or increasing trailing numbers (eg flower1 -> flower2)

What makes a good password?

- Weak: any dictionary word (flower), keyboard sequence (qwerty, 12345), word or date associated with you (birthday, dog's name)
- Stronger: use a mix of upper and lower case, numbers and symbols; this adds complexity (F!0w3R)
- Even stronger: use a complex password, and make it longer!

Explanation of password strength

1. Six character word using only letters:
   - 26^6 = 308,915,776 possible combinations (308.9 million)
2. Six character word using letters and numbers:
   - 36^6 = 2,176,782,336 possible combinations (2.2 billion, 7 times better than example 1)
3. Eight character word using only letters:
   - 26^8 = 208,827,064,576 possible combinations (208.8 billion, 676 times better than example 1)
4. Twelve character word using letters, numbers and keyboard symbols:
   - 68^{12} = 9,774,779,120,406,941,925,376 possible combinations (9.8 sextillion)

Explanation of password strength

- Complex passwords are harder for humans to guess, but not much harder for a computer
- Longer passwords are harder for computers to crack

- A combination of length and complexity is best
- Don’t reuse passwords! A strong password for one site is useless if an attacker already knows it from another site.

Coming up with good passwords

- Avoid reusing a common password 'theme', eg adding increasing numbers to a base word

- The simplest way to get a strong password is to auto-generate a random character sequence. Many generators are available online or as part of a password manager app (more on these in future).

- Example: U+:w@{bG3[wJkSqZ
    - Generated from passwordsgenerator.net

Managing your passwords: options

- Password book
- Browser (coming in part 2)
- Password manager app (coming in part 3)

Keeping a password book

- Each entry requires: website, username, password
  - Make sure each one is clear – no use having a password when you don't know what site it's for!
- Write clearly!
  - Write in block letters, not joined up
  - Case matters, a ≠ A
  - Make sure you can distinguish ambiguous letters/numbers
    eg l ≠ I (lowercase L ≠ uppercase i)
- If you need to change your password, cross out the whole line and write the new username/password on a new line. This avoids later confusion, especially if the password is changed several times.