



# Improving the Strength of your Passwords

# Why Create a Strong Password?

---

A strong password helps you:

---

Keep your personal info safe

---

Protect your emails, files, and other content

---

Prevent someone else from getting into your account



# Meet Boston College Password Requirements

- Your password must contain upper case, lower case and a number or a symbol
- It must be at least 8 characters long and needs to be changed every 90 days
- Avoid using currency symbols as this is incompatible with some of the College software
- From the evening of 26<sup>th</sup> March all learners will be asked to enter a new password

# The Key Aspects of a Strong Password

---

Length (the longer the better)

---

A mix of letters (upper and lower case), numbers, and symbols

---

No ties to your personal information

---

Create a password with three random dictionary words with a number or symbol

# Creating a Unique Password - That's Also Strong

Use a phrase and incorporate shortcut codes or acronyms

These examples let you use phrases that either means something to you, or you associate with a type of website.

- **2BorNot2B\_ThatIsThe?** (To be or not to be, that is the question - from Shakespeare)
- **L8r\_L8rNot2day** (Later, later, not today)
- **4Score&7yrsAgo** (Four score and seven years ago)
- **John3:16=4G** (Scriptural reference)
- **14A&A41dumaS** (one for all and all for 1 - from The Three Musketeers)

# How to Keep a Strong Password Secure



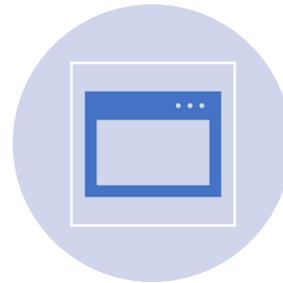
**Don't reuse your passwords.** If you're using the same password across email, shopping, and other websites holding sensitive personal data and one of those experiences a breach, you've now exposed the other services to the risk of being breached as well.



**Don't write your passwords down.** It can be tempting, especially in the workplace, to keep track of passwords the old-fashioned way, but these are easily discovered.



**Use a password manager.** There are many apps that store your passwords securely. For example LastPass



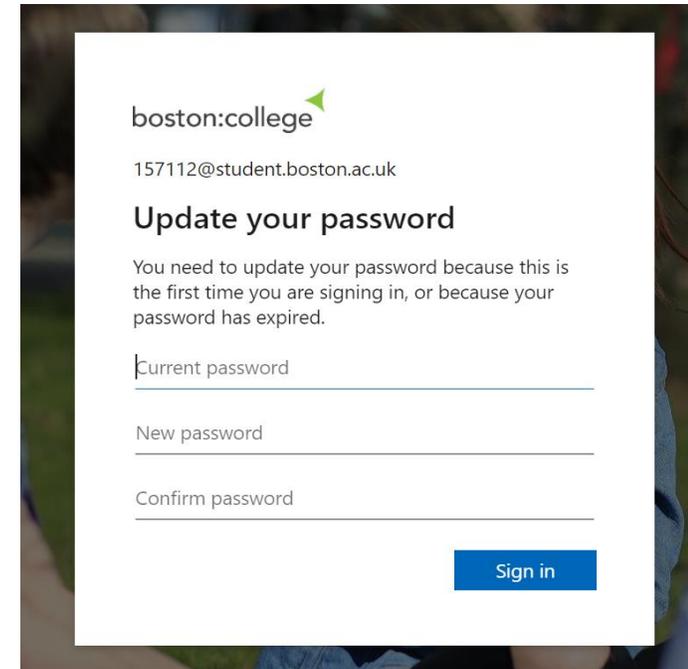
**Don't share your passwords.** This one is a no-brainer, and if you must share, change it as soon as possible.

# How to Easily Spot a Weak Password

- A common example is using a last name + year of birth combination. Marshall1968 - though this example uses 12 characters and includes letters and numbers, it includes both a name that can be associated with you or your family, and other identifying pieces of information such as your birth year, which means it can be easily hacked.
- “F1avoRs” as a password, mixing up capital letters and numbers. Here are two important reasons why this password example isn’t safe:
  - It’s too short. A long password is a strong password..
  - The number of substitutions can be easily guessed. Substituting the number 1 for the letter l is easy to guess for both humans and software.
  - Use of substitutions in a single word passwords are something hackers try

# How to update your password

- From this evening (26/03) after logging onto Teams or Office 365 you will be asked to update your password
- Enter your current password in the top box, followed by a new password in the subsequent two.
- Please make sure your new password is a complex password, make it at least 8 characters, containing numbers or a special character e.g. !?().
- **TIP:** Use a combination of 3 words to make a complex password like **pencillaptopbag95!**



boston:college

157112@student.boston.ac.uk

### Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

New password

Confirm password

Sign in