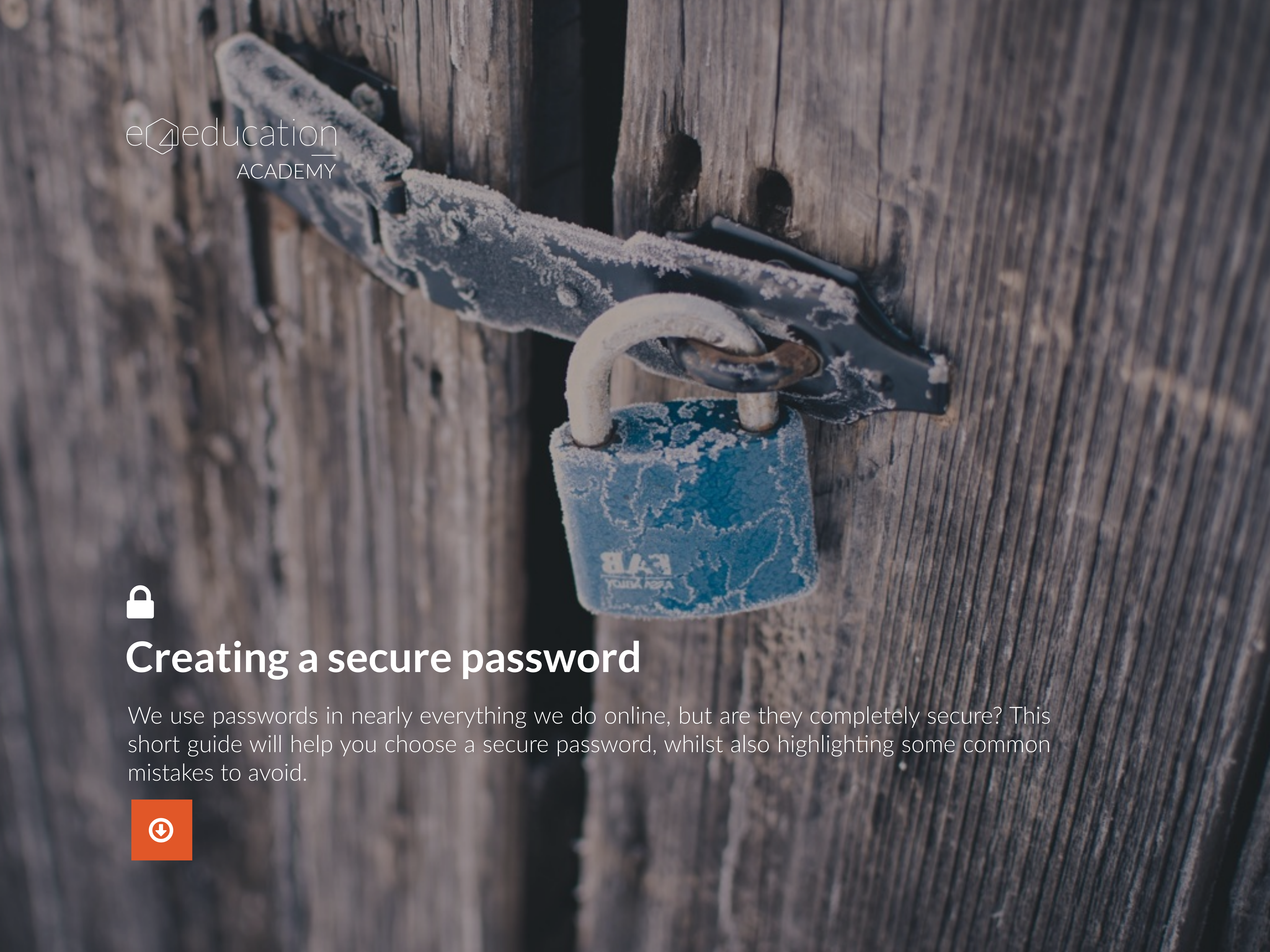


e4education
ACADEMY

Creating a secure password

We use passwords in nearly everything we do online, but are they completely secure? This short guide will help you choose a secure password, whilst also highlighting some common mistakes to avoid.

Choosing a secure password

You use it to log on to your computer, you have one for your emails and your social media profiles, and you may even have one to log into your phone. We use passwords every day, but do we ever think about how important they are?

This short guide will inform you of the importance of a secure password, the difference between a password and a passphrase, and the common password mistakes to avoid.

Being secure, online

Having a good password can be the difference between keeping your personal information private, and compromising your security. We're always being reminded that hackers can easily obtain simple passwords, so having a hard to guess password is definitely the way forward.

Password or passphrase?

A password is a single word, usually no more than 10 letters in length and can contain upper and lower letters, numbers and symbols. A passphrase is longer than a password, and is a short sentence, including spaces. A passphrase can also contain symbols and numbers, as well as upper and lower case letters.

Passphrases are traditionally considered more secure than a password as they are longer, and therefore harder to guess. Passphrase are usually easier to remember, with passwords being easier to hack as they are shorter, and users may use the same password for more than one site (so once they've accessed one account, they can access many others).

The most common password mistakes, and how to avoid them

• Not changing your password often enough.
Some email providers and work places require you to change your password regularly to ensure security. These types of updates may even make you choose a password that you haven't used before, or that isn't similar to a previous password. If you keep the same password for several years it can become easier to track or guess.

• Using the same password for multiple accounts.
If you use the same password for everything, or variations of the same password, then it will be much easier to guess. If your password is hacked from one site, and you only use one password, then the hackers will now have access to every site you use, and your personal information. It's better to use a range of passwords for different uses, and to change them if one gets hacked or compromised.

• Using a password that is easy to guess.
People don't crack passwords, computers do. So just because you've used your car registration plate as your password doesn't mean it can't be guessed easily, as a computer will quickly run though several thousand options until it finds your passwords. Use HowSecureIsMyPassword to find out how long it would take a computer to guess your password.

• It's not secret. Don't share it or write it down.
It might seem obvious, but you should never share your password, or write it down anywhere. Some of the most easiest passwords to guess are those placed on post-it notes in desk drawers, or those written on notepads. To stay safe just remember it, and don't share it.

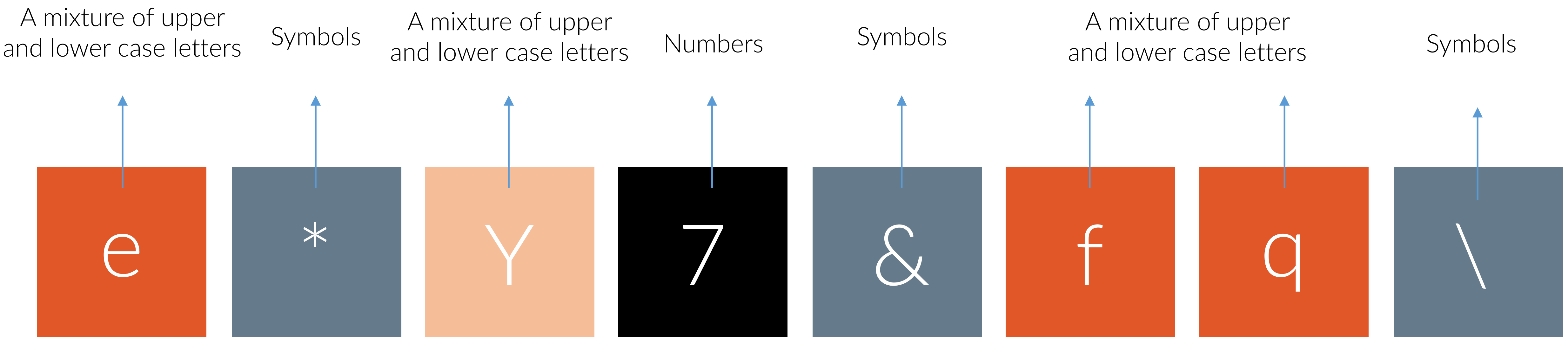
• If it only includes letters or just numbers.
The most secure passwords have a combination of letters, symbols and numbers, as well as a random mixture of upper and lower case characters.

• Too short.
The shorter your password, the easier it is to guess. If someone is looking over your shoulder, they could easily guess a password if it's less than 8 characters. A computer can also easily guess a short password, cracking it in mere seconds if it is under the recommended length. Most computer systems and social networks enforce a minimum password length purely for this reason, but always try to make sure it's long so it's much harder for someone else to guess.

Creating your secure password or passphrase

Below is an example of a password and passphrase which includes the secure elements highlighted in this resource.

We don't recommend you use these exact passwords: they will be easy to crack as we've shared them publicly in this resource!



A mixture of upper and lower case letters

Symbols

A mixture of upper and lower case letters

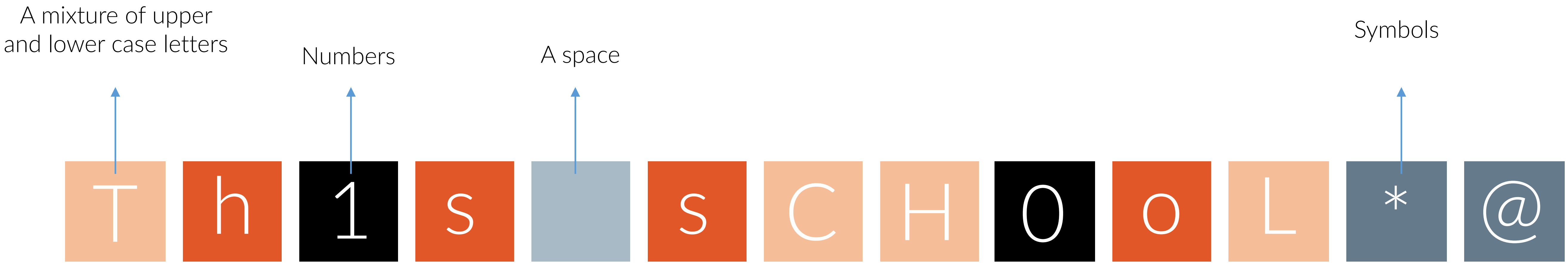
Numbers

Symbols

A mixture of upper and lower case letters

Symbols

e * Y 7 & f q \



A mixture of upper and lower case letters

Numbers

A space

Symbols

T h 1 s   s C H 0 o L * @

According to HowSecureIsMyPassword.net, it would take 465 million years to crack this passphrase!

e4education

Where ideas are formed and school websites are born. Our talented team design, create, and develop websites and branding for schools and academies across the UK.

Searching for school website inspiration, looking for new prospectus design, or just want to take a look at some of our recent work?
Head over to www.e4education.co.uk, or call our team on 03453 191 039.