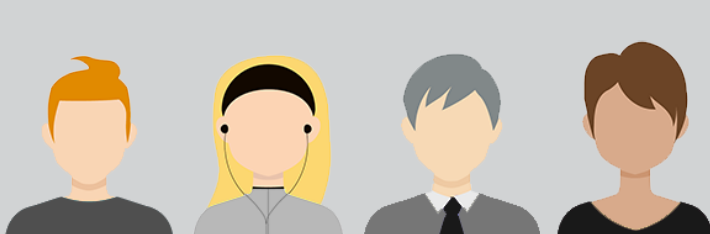project**five**

are your people leaving the door unlocked?

According to statistics from the UK's Information Commissioner's Office; human error is the 'main cause of data breaches'.

Cybsafe announced that **90%** of data breaches in the UK are caused by human error.
(1)

9 out of **10** of the **2,376 breaches** reported to the ICO were due to "**mistakes by users**".
(2)

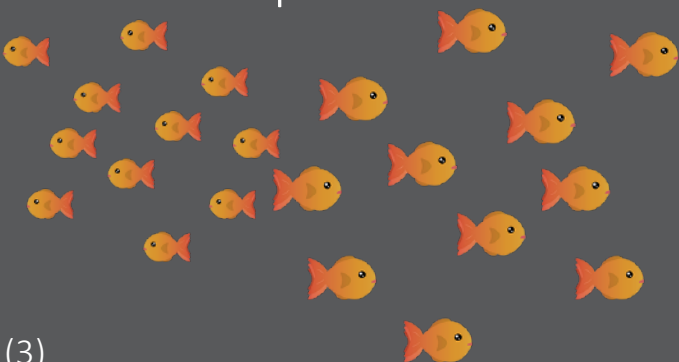UK's Information Commissioner's Office

Phishing was named as the main cause of breaches which was **45%** of all the reports to the ICO.
(3)

How can you prevent these security breaches?

The best thing you can do to make sure your team are operating securely is to educate them.

Teach them how to choose a **strong password**, with an emphasis on **length** over **complexity**.

password:
* * * * * * * * * * * *

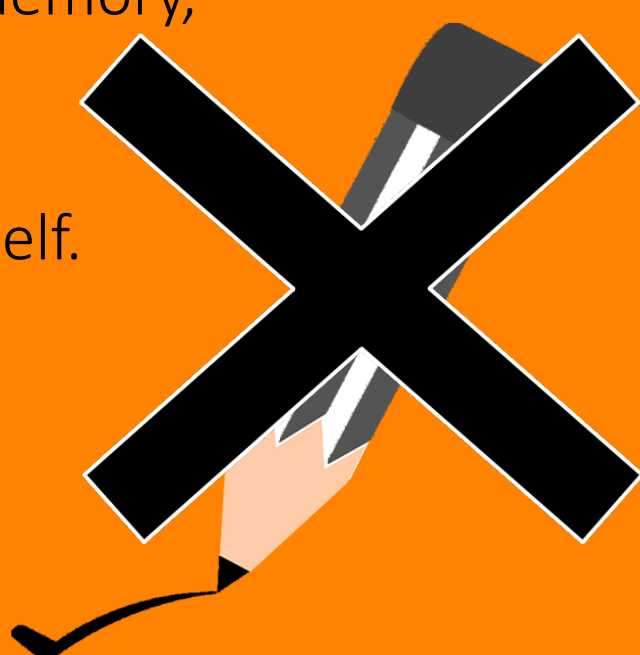Remind your team to **never share their passwords**, recent Government statistics show that a shocking **27%** of us admit to sharing our passwords. That's potentially over a **quarter** of your office!

" The password that I use is..."

Never write them down!
If you need to write a reminder, write something that jogs your memory, but has no link to the password itself.

Remind your team that if they have visitors coming to the office, give them the **guest wifi code**, rather than allowing them to use (**and potentially infect**) your internal network.

installing update

Explain the importance of keeping their PCs protected by installing the latest Windows Updates (this can be set to 'automatically install' but you do need to check that you're **up-to-date**).

Make sure your staff know how to spot the signs that an email may be a **fake** or **spoofed** email. The sender's email address, the name of the attached file (**don't open it**!) and how they greet you (no greeting at all, a generic 'Sir/Madam' or by name) can all be clues as to the authenticity of the email.

Beware the abandoned USB stick!

Remind your team to never put USB drives into their PC to find out who they belong to – they could be carrying a virus and infect you instantly.
This may sound obvious, but a 2016 study by University of Illinois, found that **48%** of people who found a USB Flash drive would put it in their PC to see what was on it.

Learn how to protect yourself!

Join the projectfive team for a
CyberCrime Awareness Training Course.
Call our team to find out more.

01276 455466

Reference links
(1) https://www.ncsc.gov.uk/report/weekly-threat-report-7th-february-2020
(2) https://www.ncsc.gov.uk/report/weekly-threat-report-7th-february-2020
(3) https://www.ncsc.gov.uk/report/weekly-threat-report-7th-february-2020