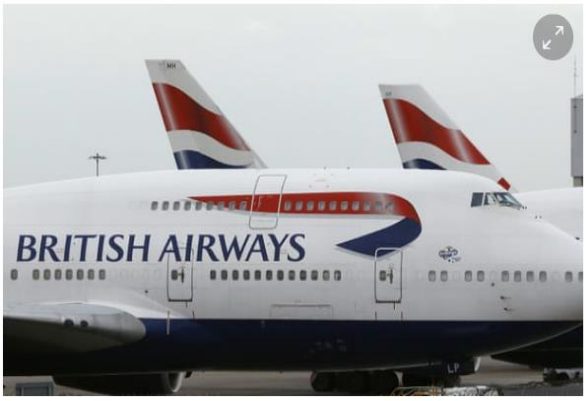
Staying safe online

ICO says personal data of 500,000 customers was stolen from website and mobile app



▲ A British Airways data breach in 2018 compromised customers' credit card information. Photograph: Frank Augstein/AP

British Airways is to be fined more than £183m by the Information Commissioner's Office after hackers stole the personal data of half a million of the airline's customers.

British Airways (BA) and US hotel group Marriott are facing significant fines, following high profile data breaches reported in 2018.

The Information Commissioner's Office (ICO) has issued notices of intent to fine BA a record £183m, whilst Marriott faces a £92.2m penalty. You can read the ICO's statements on their website.

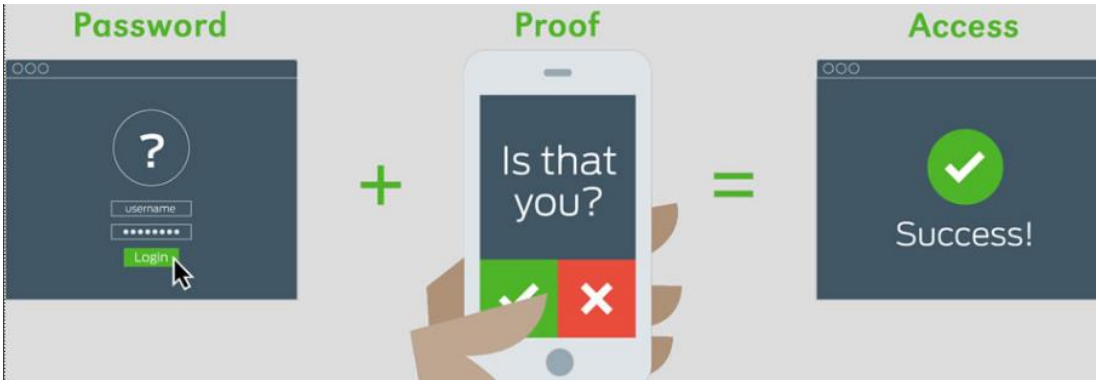
The data breach which affected British Airways was reported in September 2018. Customers on the BA website were diverted to a fraudulent site, where details of around 500,000 users were stolen

Marriott's breach, which was reported in 2018 but is thought to date back to 2014, saw millions of users affected.

Top tips for staying secure online

1. Protect your email by using a strong and separate password Cyber criminals can use your email to access many of your personal accounts, leaving you vulnerable to identity theft.
2. Install the latest software and app updates
3. Software and app updates contain vital security updates to help protect your devices from cyber criminals.
4. Turn on two-factor authentication on your email
5. Two-factor authentication is recommended for email accounts to make sure your data is secure.
6. Password managers: how they help you secure passwords
7. Using a password manager can help you create and remember passwords.
8. Secure smartphones and tablets with a screen lock
9. Screen locks offer your devices an important extra layer of security.
10. Always back up your most important data
11. Safeguard your most important data, such as your photos and key documents, by backing them up to an external hard drive or a cloud-based storage system.

TWO_ Factor Authentication… What is that.. ?



Two-factor authentication is recommended for email accounts to make sure your data is secure

TWO FACTOR = Two pieces of information, a password and a confirmation passphrase or 5 digit number sent to another device you have in your possession.

Accounts that have been set up to use 2FA will require an extra check, so even if a criminal knows your password, they won't be able to access your accounts. This is reassuring if you suspect some of your passwords aren't as strong as they could be, or you've re-used them across different accounts, or you worry that (like anyone) you may one day fall for a scam email that reveals your password to a criminal.

When setting up 2FA, the service will ask you to provide a 'second factor', which is something that you (and only you) can access. This could be a code that's sent to you by text message, or that's created by an app. Some types of 2FA provide more protection than others (because the second factor is more difficult to steal), but since any 2FA is better than none, you should use 2FA wherever you can. It only takes a few minutes to set up for each account, and it's well worth it for the amount of additional protection it gives you.

What's a Password Manager

A password manager is an app on your phone, tablet or computer that stores your passwords securely, so you don't need to remember them all. Some password managers can synchronise your passwords across your different devices, making it easier to log on, wherever you are. Some can also create random, unique passwords for you, when you need to create a new password (or change an existing one).

Reusing the same password across different accounts can be dangerous. A cyber criminal might steal one of your passwords, and then use it try and access other accounts. This means they could quickly break into several of your accounts despite only knowing one password.

We know that we're supposed to create a unique, hard-to-guess password for all of our online accounts, to prevent such a scenario happening. However the NCSC recognise that this virtually impossible to do without help. Password managers provide that help. They're designed to make **using** and **generating** passwords easier and more secure. Many can also automatically enter the appropriate password into websites and apps on your behalf, so you don't even have to type them in every time you log in.