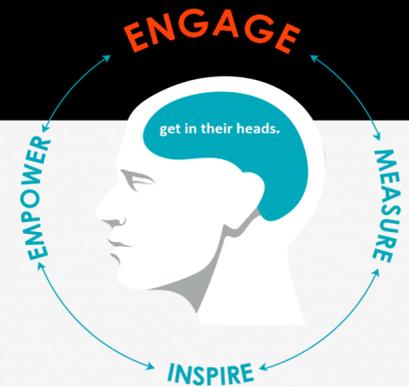


July 2019

HACK LIFE



eRiskology's Monthly Information Security Awareness Bulletin

STORY OF THE MONTH: BRITISH AIRWAYS & THE SKY HIGH 'FINE'

July has been a big month for our ICO – Information Commissioners Office. The ICO are the UK's Supervisory Authority, tasked with upholding information rights for the nation. After the principles of GDPR were enshrined in to UK law, their ability to fine organisations in breach increased dramatically – up from a maximum penalty of £500,000 (see [Facebook](#)) to £20m or 4% of annual turnover, whichever is greater. This suddenly became tangible when they issued a notice of intent to fine British Airways over £183m or 1.5% of their 2017 turnover. This was as a result of a breach to the BA booking web application where around half a million users' personal and financial data was compromised. You can see more on this story in our blog post [HERE](#). And it doesn't stop there, the very next day the ICO announced another intent to fine, this time Marriott Hotels for £99m as a penalty for their huge '[mega breach](#)'. This has caused a flurry of misleading and sensationalist headlines across news outlets, with many commentators not understanding the difference between a notice of intent to fine and actually issuing a fine – again, you can see more detail in our blog piece. It's going to be interesting to see the outcome of these notices, BA have announced they will be making representations, once the ICO have considered these they can maintain the fine, reduce it, or withdraw it altogether. After this, BA would have the right to appeal any fine issued

DID YOU KNOW?

Feeling poorly? Then just ask Alexa... 'Hapless Hancock', that is, Matt Hancock, our Health Secretary, gleefully announced he was "Making sure you get the best NHS advice if you ask Alexa – harnessing tech to empower people to take better control of their health". Great idea Matt – let's trust our public health to a company that lives off harvesting personal data – what could possibly go wrong!? This literally a couple of days after it came to light that Amazon stores your interactions with Alexa [FOREVER!](#)



RESOURCE OF THE MONTH

After it recently transpired that ZOOM conferencing software could be compromised to allow attackers to gain access to the webcam, Apple have reacted by issuing a silent update to disable the hidden web server concerned.



MONTHLY QUIZ

Which council had to remove data forms from its website after it was found personal data could be accessed simply by changing a few digits on the URL? - our winner will be chosen randomly from correct answers and will win a HACK LIFE t-shirt! info@eriskology.com

