Cyberwork

GDPR – behaviour change

Sarah Worley-James
worley-jamess@cardiff.ac.uk

The GDPR (General Data Protection Regulation), which came into law on 25 May, means it is essential that we *all* review our behaviour and habits to ensure that we do not unwittingly fall foul of the legislation.

Human error, often caused by a busy and stressful work life, is the biggest cause of mistakes happening. According to the 2014 IBM Chief Information Security Officer Assessment, 95 per cent of information security incidents involve human error.[1,2]

Human error can be defined as behaviour, actions or decisions which could, or potentially could, adversely affect safety and security, as 'an inevitable or natural result of being human'.[3] Easy-to-guess passwords, lost devices (especially if not password protected), sending information to the wrong email recipient, and double clicking on an unsafe URL (Uniform Resource Locator – website address) or attachment are all classic examples.

Considering how our own habits and behaviour could lead to data breaches is as important as ensuring formal policies and procedures are being followed.

Passwords: Here are some useful tips to help when creating passwords to make them stronger, as well as alleviating anxiety about remembering them. Try using the first letter of each word of an easily remembered sentence, plus transposing some of the letters for numbers, eg 'my first holiday abroad was in Lanzarote' makes 'm1sth@w1L'. Alternatively, you could use an app that creates, and stores, passwords safely.[5]

Phishing, vishing and smishing: These are terms we hear all too often these days, referring to fraudulent emails, phone calls and text messages (SMS) that try to get us to give away our money. Unfortunately, we are all on the receiving end of these on a regular basis and even a criminal psychologist got scammed recently.[6]

Never click on a website link from an email or text message, unless you are expecting it, eg a password reset request you have just made. Always carefully check the sender's email address. At first glance it may appear authentic, but on closer inspection it may be spelt incorrectly, or use a gmail or yahoo address, which a bank would never do. Always check that the email address starts with http**s** – the 's' indicates the website uses appropriate security. If you are unsure, google the organisation and confirm the address is https before clicking.

According to the 2014 IBM Chief Information Security Officer Assessment, 95 per cent of information security incidents involve human error[1,2]

Facebook and Google log in: A tempting, and easy, way to log into websites, as you don't need to remember and type in your password. However, this creates a weak point as you are in effect using the same password for multiple websites.[7]

Recommending apps: ACTO (The Association for Counselling and Therapy Online) advocates using Orcha,[8] the UK's leading health app evaluation organisation. They use ethical and security criteria set out by regulatory bodies across the world, including NHS Digital recommendations.

Online webcam appointments: Be aware not to use the client's full name in the appointment link, so that it does not appear in anyone's diary or notification pop-ups. And it is particularly important to disable your pop-ups if you are screen sharing.

Screen savers: These are a simple, yet key, way to keep others from unwittingly seeing sensitive data, but it is easy to forget to put a screen saver on when briefly leaving your office. Ensure it is set to come on automatically after one minute's inactivity; with 'on resume display log in', so you have to re-enter your password, not just move your mouse, to reactivate it.

I encourage you to take a minute to review your online habits and make any adjustments to keep yourself, as well as your clients, safe. ●

Sarah Worley-James is Chair of the Association for Counselling and Therapy Online (ACTO) and a senior counsellor and co-ordinator of the Online Service at Cardiff University.

REFERENCES

1 https://securityintelligence.com/how-to-reduce-human-error-in-information-security-incidents/
2 https://www.itgovernance.co.uk/blog/five-damaging-data-breaches-caused-by-human-error/
3 https://en.oxforddictionaries.com/definition/human_error
5 http://uk.pcmag.com/password-managers-products/39332/guide/the-best-free-password-managers-of-2018
6 http://www.thisismoney.co.uk/money/beatthescammers/article-4566082/Fraudsters-scammed-18-000-criminal-psychologist.html
7 http://uk.pcmag.com/software/41997/opinion/signing-into-websites-with-facebook-is-just-asking-to-be-hac
8 https://acto-org.uk/orcha-pph-health-apps-resource/