Cybersecurity advice from the police - How to protect yourself online

The police have issued the following advice for safe browsing and shopping online this Christmas.

Dilemma 1: You are in a coffee shop when you decide to check your online banking to review your festive spending. Should you use the coffee shop's public WiFi?

Answer: Do not use the public WiFi, use your own 4G connection instead. Public WiFi is often unencrypted, which means criminals could intercept your information. Do not use it for online banking or shopping. *UK victims lost £1.65 million to ticketing fraud in 2018/19 – that's £365 per victim.*

Dilemma 2: You have received a message on social media saying that if you forward the message to five more people, you will get a free gift. What should you do?

Answer: Delete it. No matter how appealing an offer of a free gift sounds, don't fall for it. Never reply to or forward these messages and do not supply any personal information. *The UK saw a 61% increase in malware offences in the last year.*

Dilemma 3: You are browsing the internet when an advert pops up with a very low price for a new tablet computer. The advert says the deal is only available for the next few hours. What should you do?

Answer: Do not follow the link. Search for reviews of the company online first. If you think it is genuine, go to the retailer's website directly, and make sure the web address begins with https://. Cybercriminals put fake adverts online, especially at Christmas. Make sure the site is reputable before you buy anything. *There were 122,437 incidents of bank transfer scams (known as Authorised Push Payment fraud) in the UK in 2019.*

Dilemma 4: You receive an email containing a receipt for an Amazon order. You have not purchased anything from Amazon. The email asks you to click a link to view the details. What should you do?

Answer: Do not click the link – log into the official Amazon website to check the details. Fake receipts, delivery updates or missed delivery notices are used by phishers to steal your sensitive information, especially at this time of the year. *80% of hacking breaches are due to weak or stolen passwords.*

Dilemma 5: A friend has sent you a social media game to find your reindeer name. You just combine your first pet's name and the name of the road you live on, then post it in a comment. Should you play?

Answer: No, this is personal information. These social media 'games' are a way for fraudsters to gather personal information that may help them crack your password, or even steal your identity. *More than 1,600 social media profiles were taken down in 2019 – all linked to scam activity.*

Useful links:

- www.met.police.uk/littlemedia - A repository of police booklets and videos with regards to fraud and cybercrime.

- www.haveibeenpwned.com - A website which keeps track of data breaches that are leaked onto the internet. By entering your email address, you can see if/when it has been involved in a leak. It's also possible to sign up to alerts from the site (recommended).

- www.actionfraud.police.uk - The reporting site for all fraud and cybercrime in England and Wales, and a good source of scam alerts and scam related news.

- https://www.ncsc.gov.uk/cyberaware/home - Cyber Aware is the UK government's advice on how to stay secure online.

- https://takefive-stopfraud.org.uk National campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud.

- https://www.getsafeonline.org UK's leading source of unbiased, factual and easy-to-understand information on online safety.