Fraud Awareness Quiz

Q1. You have an online Energy account.
Which of the following should be a cause for concern regarding fraud?

A: You go online and there's a problem with the website so their payment system is currently down.
B: You go online and attempt to make a payment but notice the last 4 digits of your bank details have been changed.
C: You have a smart meter but receive an email with a link to pay an overdue bill
D: You go online but can't access your account even though you know you have entered your correct email address and password.

Q2. Which of the following emails is most likely to be a scam?

A: An email from a retail outlet advertising their latest offers
B: An email from an internet dating site inviting you to join up now at a discounted price.
C: An email from your child's school containing a newsletter attached.
D: An email from your energy supplier asking you to confirm your bank details

Q3. 'Malware' is a term used to describe 'malicious software'
You receive an email claiming to be from a well-known energy supplier that you have previously had no dealings with.

What should you do?

A: Read the email and open any attachments, ensuring that you don't miss out on special offers.
B: Read the email, but do not open any attachments. First check any information contained in the email to help you check the legitimacy of the sender by looking at their website.
C: Do not open any attachments.
D: Do not click on any links contained within the email.

Q4. Fraudsters often contact people by telephone pretending to be calling from their bank.
Knowing what questions your bank will never ask you could help you know whether a call is genuine or a scam.

Which of the following will your bank never ask you?

A: To hand your bank card to the courier they've sent as they need it as a matter of urgency because your card details have been stolen.
B: To confirm the details of the last transaction you made with the card, to check that it was you who used it
C: To confirm a couple of random, but specific, digits of your security code.

D: To provide all your account details as there has been a cyber-attack and they need to set up a new account.

Q5. How can you protect yourself from identity fraud?

A: Shred personal documents and bank statements before putting in the bin.
B: Check your bank statements and check your credit report.
C: Keep your address information up to date and redirect mail when you move.
D: Be careful what applications you install onto your mobile phone and install antivirus on your mobile, not just your computer/laptop.

Q6. What is a WIFI hotspot?

A: It can be found in any location where anyone can obtain unsecured internet access.
B: It is a phone app.
C: It is part of the way a mobile phone is set up.
D: It is found in cafés only.

Answers

Q1. B, C and D
Q2. D
Q3. B, C and D
Q4. A and D
Q5. A,B,C and D
Q6. A - never make any payments or access your own accounts where personal data is stored using a WIFI hotspot.