1. The first example is a Smishing social engineering method, and the red flag is the url in the SMS which contains meaningless letters and digits combination
2. The second example is an impersonation social engineering method, this message comes in as a case of urgency with the attacker using the victims name thereby making the victim think it is from a known person and calls for quick response
3. The third example is a smishing social engineering method, the red flag is the malicious link
4. Smishing social engineering method is also used in the fourth example and also contains a malicious email and the red flag
5. The fifth example is a baiting social engineering method, the red flag involved in this method is the malicious link and the large amount of money said to have won
6. The sixth example is a smishing social engineering method which uses a malicious link
7. The seventh example is a phishing method, the attacker uses malicious link with meaningless words which

Activity 2: Using the case study below, what are the proactive measures Elera Caring should have implemented to prevent the data breach? https://portswigger.net/daily-swig/data-breach-at-healthcare-provider-elara-caring-exposes-100-000-patients-information

- Elera Caring should have carried our an awareness session for its employees the sensitize them on the different types of social engineering attack and how to protect themselves from these attack
- Elera Caring should have implemented company-wide password change and also implemented multifactor authentication for all users of its systems.

Activity 3: Using the case study below, what other types of Business Email Compromise (BEC) attack can be used other than CEO Fraud to perform the same criminal fraud on Ubiquiti Networks?

CASE STUDY

https://www.nbcnews.com/tech/security/ubiquiti-networks-says-it-was-victim-47-million-cyber-scam-n406201

- Phishing
- spoofing

Activity 4: Using the case study below, advice the two companies on how to further protect against such attacks in the future.

CASE STUDY

https://www.cpomagazine.com/cyber-security/the-phishing-scam-that-took-google-and-facebook-for-100-million/

- Ensuring that there is adequate vendor security
- Reviewing of senders email address to verify the website links or email address of the vendors