|  |
| --- |
| **1.5 Securing data and systems** |
| * Learners should understand the following threats to data stored on computer systems and online:   + accidental damage – identifying how data can be at risk from accidental destruction.   + malicious and deliberate damage. |

Specification points:

Skills audit:

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** |  |  |  |
| I can identify examples of accidental and malicious damage made to computer systems. |  |  |  |
| I can identify a wide range of social engineering techniques. |  |  |  |
| I can identify strategies that can prevent users becoming a victim of a social engineering attack. |  |  |  |

Teacher feedback:

|  |
| --- |
|  |

Student response:

|  |
| --- |
|  |

**Exam-style questions**

1. DC Banks run a call centre to allow customers to make enquiries about their bank accounts. The manager has expressed concerns about the risk of phishing.
2. State **two** ways phishing can take place at the call centre.

1…………………………………………………………………………………………………………………..

2…………………………………………………………………………………………………………………..

**[2]**

1. Identify **two** potential problems to the centre if phishing takes place.

1…………………………………………………………………………………………………………………..

2…………………………………………………………………………………………………………………..

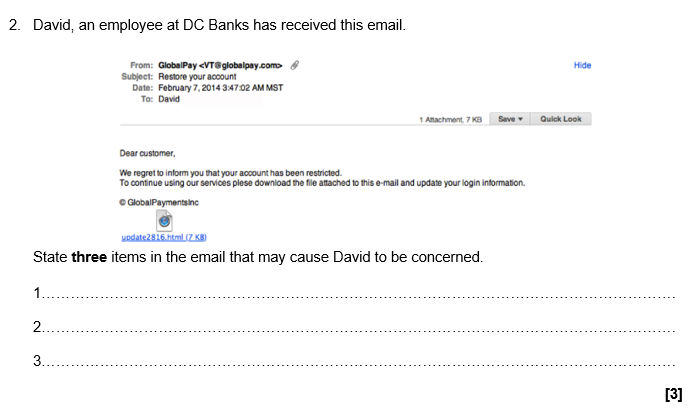
**[2]**

1. Describe **one** other social engineering technique.

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**[2]**

1. David, an employee at DC Banks has received this email.



State **three** items in the email that may cause David to be concerned.

1…………………………………………………………………………………………………………………..

2…………………………………………………………………………………………………………………..

3…………………………………………………………………………………………………………………..

**[3]**