1. Humans can be the biggest threat to data and sometimes damage caused can be accidental rather than malicious or deliberate.

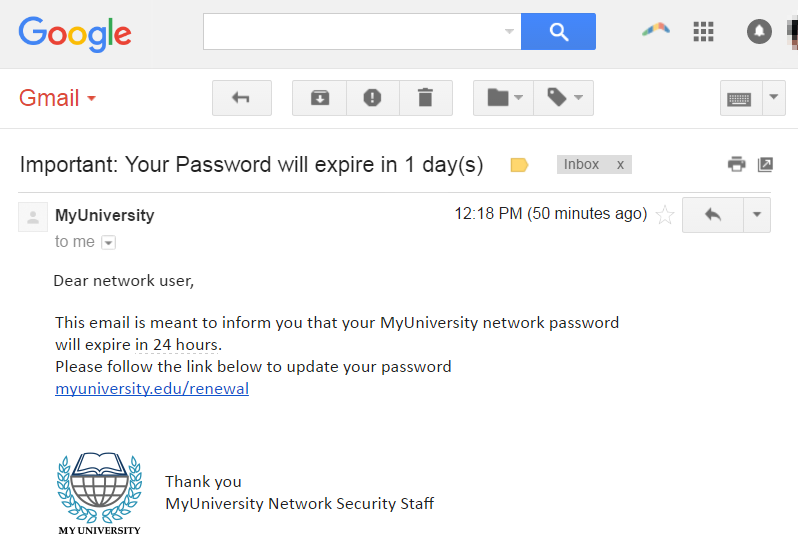
Identify examples of threats to data stored on computer systems and online.

|  |
| --- |
| Accidentally overwriting a file or deleting a folder.  Leaving a laptop on a train/taxi/plane.  Natural disasters e.g. flooding and fire. |

1. One common social engineering technique is known as Phishing.
2. Identify what is meant by the term ‘phishing’.

|  |
| --- |
| A fraudulent technique where an internet user is tricked (an email message is common) into revealing personal or confidential information. |

1. Look at the email below



Identify a few items in the email above the would cause a user to be concerned about this email.

|  |
| --- |
| * Lack of personalisation (e.g. Dear network user) * Sense of urgency stated in the email (e.g. your password will expire in 24 hours) * Link within the email to update your password. |

1. What measures can users put in place to prevent becoming a victim of a phishing attack?

|  |
| --- |
| * Never click on emails for unknown senders. * Hover the link provided to check to see if it’s genuine. In most cases, it doesn’t match up the URL of the company it’s come from. * Double check email address/sender name. * Contact the website of the company this email has claimed to have come from for further verification. * Report the email to anti-phishing agencies. * Block the sender * Avoid entering any personal information. |

1. Identify items in an email that could suggest that this is a phishing attack.

|  |
| --- |
| * Contains a link or download (exe file) * Urgently asking for your help. * Asking to donate to charity or promoting fundraising. * Presenting a problem (i.e. click on link to verify account) * Notify that you are winner of a big prize. * Pose as your employer or colleague within the same company. |

1. In the table below, use the internet to find out how different types of phishing attacks work.

|  |  |
| --- | --- |
| **Type** | **Description** |
| Malware phishing | This type of phishing introduces nasty bugs by convincing a user to click a link or download an attachment so malware can be installed on a machine |
| Spear phishing | A type of phishing that will target a specific person instead of casting a wide net like a traditional phishing attack does. |
| Smishing | SMS + Phishing = Smishing  SMS-enabled phishing uses text messaging as a method for delivering malicious links, often in the form of short codes. |
| Search engine phishing | Search engine phishing injects fraudulent sites, often in the form of paid ads, into results for popular search terms. |
| Pharming | Pharming reroutes legitimate web traffic to a spoofed page without the user’s knowledge, often to steal valuable information. |
| Vishing | Vishing involves a fraudulent actor calling a victim pretending to be from a reputable organization and trying to extract personal information, such as banking or credit card information. |
| Clone phishing | In this type of attack, a shady actor makes changes to an existing email, resulting in a nearly identical (cloned) email but with a legitimate link, attachment, or other element swapped for a malicious one. |
| Man-in-the-middle phishing | A man-in-the-middle attack involves an eavesdropper monitoring correspondence between two unsuspecting parties. These attacks are often carried out by creating phony public Wi-Fi networks at coffee shops, shopping malls, and other public locations. |
| Business Email Compromise (BEC) | This involves a phony email usually claiming to be an urgent request for a payment or purchase from someone within or associated with a target’s company. |
| Malvertising | This type of phishing takes advantage of exploits within advertising or animation software to steal information from targeted users. Malvertising is usually embedded in otherwise normal-looking ads—and placed on legitimate websites like Yahoo.com—but with malicious code implanted within. |

1. Shoulder-surfing is a common and a straightforward social engineering technique that can be used by anyone, even if they have limited experience of computer systems.
2. What is meant by the term ‘shoulder-surfing’?

|  |
| --- |
| Shoulder surfing, also known as visual hacking, refers to the act of obtaining personal or private information through direct observation. Shoulder surfing involves looking over a person's shoulder to gather sensitive information while the victim is unaware. |

1. List a few scenarios where shoulder-surfing could be a real threat?

|  |
| --- |
| This is especially effective in crowded places where a person uses a computer, smartphone or ATM. |

1. Identify a range of measures users could put in place to protect themselves from shoulder-surfing.

|  |
| --- |
| * Be aware of who is standing or sitting around and behind you * Spend more for a screen filter or protector to obscure the visibility of the display * Never give your password or any vital information to anyone * Locate a quiet spot away from the crowd * As much as possible, never open personal accounts in public * Tilt your device, block their view, sit out of their view |

1. Other social engineering attacks include: Scareware, Baiting, Blagging and Dumpster diving.
2. What is meant by the term ‘scareware’.

|  |
| --- |
| Malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection. |

1. Use the internet to find a screenshot of scareware and place it in the box below.

|  |
| --- |
| Student responses will vary.  What Is Scareware? Examples &amp; What to Know | InfoSec Insights |

1. Baiting is the use of a good deal that seems to good to be true such as a pop-up, which may contain malware.

Use the internet to find an example of pop-up ad that demonstrates the use of baiting.

|  |
| --- |
| Remove &quot;You Won Congratulations&quot; Pop-ups (Virus Removal Guide) |

1. What is meant by the term ‘blagging’?

|  |
| --- |
| This is when a criminal will make up a scenario in order to extract sensitive information. This could be done via email, over the phone or even in person. |

1. What is meant by the term ‘dumpster diving’?

|  |
| --- |
| Dumpster Diving is the act of an unwanted party going through the bin at a company whether it be inside or outside the building. The attacker is usually looking for some type of confidential information that got put in the trash. |

1. Provide a list of tips below that provides users with advice on how to stay safe from social engineering attacks.

|  |
| --- |
| * Delete any request for financial information or passwords. * Reject requests for help or offers of help. * Set your spam filters to high. * Secure your computing devices. Install anti-virus software, firewalls, email filters and keep these up-to-date. |