Phishing Scams

Student version

Task 1 Complete paragraphs 1 to 4 by writing down their correct topic sentences. Then, write down an appropriate heading for each of the paragraphs.

What is Phishing?

0. Phishing is the practice of sending **fraudulent** communications that appear to come from a reputable source. The goal is to steal sensitive data like credit card and login information, or to install **malware** on the victim's machine. Phishing is a common type of **cyber-attack** that everyone should learn about in order to protect themselves.

1. How it begins

Phishing starts with a fraudulent email or other communication that is designed to lure a victim.
The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is **coaxed** into providing confidential information, often on a **scam website**. Sometimes malware is also downloaded onto the target's computer. Emails are currently the primary **attack vector** of phishing scams.

2. _____

The severity of a phishing attack will vary according to the intention of its perpetrator.
Sometimes attackers are satisfied with getting a victim's credit card information or other personal data for financial gain. Other times, phishing emails are sent to obtain employee login information or other details for use in an advanced attack against a specific company. Cybercrime attacks such as **ransomware** often start with phishing.

3. Targeted attacks

Phishing attacks are at their most destructive when specific individuals are targeted instead
Known as **spear phishing**, this type of fraud is often combined with **social engineering**, a practice where attackers research their victims on social media and other sites. This allows criminals to customize their communications and appear more authentic. When such attackers go after a "big fish" like a CEO, it's then called **whaling**. These attackers often spend considerable time studying the target to find the right moment and means of stealing **login credentials**. Whaling is of particular concern because high-level executives are able to access a great deal of company information.

4. How to protect yourself

The key to protecting your organisation from phishing is user education.
Education should involve all employees. High-level executives are often a target. Teach them how to recognize a phishing email and what to do when they receive one. Simulation exercises are also key for assessing how your employees react to a **staged phishing attack**. Unfortunately, no single cybersecurity technology can prevent phishing attacks.

Source: Cisco

Task 2 Decide whether these statements are true (T) or false (F) according to the text.

1. Phishing scams involve fooling computer users and impersonating people or organisations they trust. _T_
2. One of the goals of phishing is to steal the victim's sensitive data. _T_
3. Phishing and malware are basically the same thing. _F_
4. Downloadable music is the main medium used to deliver phishing attacks. _F_
5. Phishing can sometimes be followed by a ransomware attack. _T_
6. Phishing causes more damage when aimed at a wider group of people. _F_
7. Social engineering is a form of targeted phishing. _T_
8. User education is more effective at reducing phishing risks than cybersecurity technology. _T_

Task 3 **General Vocabulary**

Refer to the set of highlighted terms in the text and write down a synonym for each of the given words below.

Given word	Synonym from text
tempted	coax
dishonest	fraudulent
harshness	
criminal	perpetrator
seduce	

Task 4 **Technical Vocabulary**

Refer to the set of highlighted terms in the text and write down a term related to cyber-security for each of the given definitions below.

Definition	Technical term from text
1. harmful software that threatens to publish or destroy the victim's data, unless a sum of money is paid to the attackers	ransomware
2. a type of phishing aimed at a high-profile individual such as the CEO of a big corporation	whaling
3. details given to the users of a computer system, to be used to identify themselves and be granted lawful access to the system	(login) credentials
4. a type of phishing targeting a specific individual	spear phishing
5. a practice where attackers research their victims on social media and other sites	social engineering
6. a simulated phishing attack launched by cyber-security experts at a firm, designed to assess the level of awareness on phishing amongst the employees	staged phishing attack
7. short for malicious software; software that is designed to cause damage to computer systems and their users	malware
8. a website used by cyber attackers in order to fool their victims	scam website
9. the medium via which a phishing scam is carried out, for example, an email	attack vector
10. a broad term for any attempt by hackers to damage or destroy a computer system and its data	cyber-attack