Module 6 PROTECTING COMPUTERS

UNIT 16 • COMPUTER THREATS

1 **Read the passage and decide if the statements are true or false. Then, correct the false ones.**

Malware and how to stop it

Malware, short for malicious or malevolent software, is software used or created by attackers to disrupt computer operations, gather sensitive data or gain access to private computer systems. It can appear in the form of code, scripts, active content and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes computer viruses, worms, Trojan horses, spyware, adware and other malicious programs; the majority of active malware threats are usually worms or Trojan rather than viruses.

In law, malware is sometimes known as a computer contaminant. Malware is not the same as defective software, which is software that has a legitimate purpose but contains harmful bugs that were not corrected before release.

However, some malware is disguised as genuine software, and may come from an official company website. An example of this is software used for harmless purposes that is packed with additional tracking software that gathers marketing statistics.

Malware has caused the rise in use of protective software types such as antivirus, antimalware and firewalls. Each of these is commonly used per personal users and corporate networks in order to stop the unauthorized access by other computer users, as well as the automated spread of malicious scripts and software.

Antivirus and antimalware software commonly hook deep into the operating system's core or kernel functions in a manner similar to how malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system does something, the antimalware software checks that the O/S is doing an approved task. This commonly slows down the operating system and/or consumes large amounts of system memory. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit bugs or trigger unexpected operating system behaviour.

Antimalware programs can combat malware in two ways:

1. They can provide real time protection against the installation of malware software on a computer. This type of spyware protection works the same way as that of antivirus protection in the sense that the antimalware software scans all incoming network data for malware software and blocks any threats it comes across.
2. Antimalware software programs can be used solely for detection and removal of malware software that has already been installed onto a computer. This type of antimalware software scans the contents of the operating system registry, files, and installed programs, and provides a list of the threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.

	T	F
1. Malware is short for malicious or malevolent software.	☐	☐
2. Malware is a specific term referred to software used to gain access to computer systems illegally.	☐	☐
3. The majority of active malware threats are usually viruses.	☐	☐
4. Malware is defective software that contains harmful bugs that were not corrected before release.	☐	☐
5. Some malware presents itself as genuine software and may come from an official company website.	☐	☐
6. Damages can be created by software used by companies to gather marketing statistics.	☐	☐
7. Malware has caused the rise in use of protective software types such as antivirus, antimalware and firewalls.	☐	☐
8. Any time the operating system does something, the antimalware software checks that the O/S is doing an approved task.	☐	☐
9. Antimalware stops any operations the malware may attempt on the system before they occur and corrects bugs.	☐	☐
10. Antimalware software programs can be used only for detection and removal of malware software that has already been installed onto a computer.	☐	☐

UNIT 17 • COMPUTER PROTECTION

1 Choose the right option.

1. PIN stands for...
- **a.** Password Identification Number.
- **b.** Programming Interface Number.
- **c.** Personal Identity Number.
- **d.** Personal Identification Number.

2. A firewall...
- **a.** rejects access requests from unsafe sources while allowing actions from recognised ones.
- **b.** allows access requests from any sources.
- **c.** allows access request from recognised sources.
- **d.** rejects access requests from any sources.

3. Important data must be...
- **a.** erased.
- **b.** backed up, i.e. copied must be made in case of the data being lost or becoming corrupted.
- **c.** backed up when the back-up session does not take too much time.
- **d.** saved.

4. Best practices are...
- **a.** used to maintain quality standards.
- **b.** not used because they are time-consuming.
- **c.** not applicable.
- **d.** inappropriate to many companies.

5. Troubleshooting means...
- **a.** correcting mistakes.
- **b.** dealing with software problems.
- **c.** dealing with hardware problems.
- **d.** dealing with hardware and software problems.

2 Read the text and answer the questions.

The origins of cryptography

Cryptology is a young science. Though it has been used for thousands of years to hide secret messages, systematic study of cryptology as a science just started around one hundred years ago.

The first known evidence of the use of cryptography was found in an inscription carved around 1900 BC, in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt. The scribe used some unusual hieroglyphic symbols here and there in place of more ordinary ones. The purpose was not to hide the message but perhaps to change its form in a way which would make it appear dignified. Though the inscription was not a form of secret writing, but incorporated some sort of transformation of the original text, and is the oldest known text to do so.

Fast forwarding to around 100 BC, Julius Caesar was known to use a form of encryption to convey secret messages to his army generals posted in the war front. This substitution cipher, known as Caesar's cipher, is perhaps the most mentioned historic cipher in academic literature. In a substitution cipher, each character of the plain text is substituted by another character to form the cipher text. The variant used by Caesar was a shift by 3 ciphers. Each character was shifted by 3 places, so the character 'A' was replaced by 'D', 'B' was replaced by 'E', and so on. The characters would wrap around at the end, so 'X' would be replaced by 'A'.

During the 16th century, Vigenere designed a cipher that was supposedly the first cipher which used an encryption key. In one of his ciphers, the encryption key was repeated multiple times spanning the entire message, and then the cipher text was produced by adding the message character with the key character modulo 26. As with the Caesar cipher, Vigenere's cipher can also easily be broken; however, Vigenere's cipher brought the very idea of introducing encryption keys into the picture, though it was poorly executed. Comparing this to Caesar cipher, the secrecy of the message depends on the secrecy of the encryption key, rather than the secrecy of the system.

Adapted from: *https://access.redhat.com/blogs/766093/posts/1976023*

1. What was the purpose of the Egyptian inscription?
2. How did Caesar cipher work?
3. What is the fundamental difference between Caesar and Vigenere's ciphers?