**Types of malware. Security protection.**

1. **Read and translate the descriptions of different types of malware. Define their types using the words from the box. Pay attention to the words in bold.**

|  |
| --- |
| ***spyware / bots / keylogger / bugs / Trojan horse / adware / ransomware / rootkit*** |

1. It is a type of malware that delivers advertisements. Examples are pop up ads and advertisements that are displayed in software. Software often offers “free” versions that come **bundled with** adware. It is sponsored by an advertiser and is used to make money. While some is solely designed to deliver advertisements, it is not uncommon for this type of malware to come bundled with spyware that is **capable of** tracking user activity and stealing information.
2. Software programs created to perform simple and repetitive operations. While some of these programs are created for harmless purposes (online contest, video gaming, and internet auctions) it is becoming increasingly common to see them used maliciously. They can be used in groups of computers to be controlled by a third party for distributed **denial of service (DDoS) attacks**, to spam large amounts of advertisement on the internet, as **web site scrapers**, and for distributing malware **disguised** as popular search items on download sites.
3. A type of malicious software designed to remotely control or access a computer without being detected. Since this software has administrative access, it has full control of any existing software. This means it can modify any software, including any that may be used **to detect or circumvent** it. As a result, detection relies on manual methods such as monitoring computer behavior for **suspicious** activity, **storage dump analysis**, and signature scanning.
4. Software that tries to gather information about a person or organization without their knowledge and may send this information to another computer without that consumer’s **consent**. It is mostly used for the purposes of tracking and storing internet user’s movements on the Web and serving up pop-up ads. It can collect almost any type of data, including personal information such as surfing habits, passwords, and bank or credit card information. It installs itself on a system by **deceiving** the user or by **exploiting software vulnerabilities**.
5. Are **a flaw** that produce an undesired outcome. Usually the result of human error, they normally exist in **source code** or compilers of a program. They can cause crashing or freezing. They can allow attackers to **bypass** privileges or **override** authentication.
6. A type of malware **that disguises** itself as a normal file or program to trick users into downloading and installing malware. It can give a malicious party remote access to an infected computer. Once infected, the attacker can steal logins, financial information, and research data. They can also install more malware, modify files, and monitor activity like screen watching and keylogging. They can be spread as an attachment in an email.
7. When it takes control of your computer or device, it locks you out of that computer or device entirely or certain files. To get it on your computer or devices, **cyber criminals** trick you into downloading a program that looks **legitimate.** But what you’re really downloading is a piece of software designed to take control of your information so you can no longer access it. They then refuse access to your computer, devices, or files unless you pay a ransom.
8. It is a type of **surveillance technology** used to monitor and record each keystroke typed on a specific computer's keyboard. It is often used as a spyware tool **by cybercriminals** to steal **personally identifiable information** (PII), login credentials and sensitive enterprise data.
9. **You are going to watch the video “Protect Your Computer from Malware” to learn more about how to avoid, detect, and get rid of malware. Before watching match the definitions (a–j) with the vocabulary (1–10) and complete the sentences below.**

|  |  |
| --- | --- |
| 1. **To commit** | 1. to take control of a computer belonging to someone else without their permission, especially for illegal purposes; |
| 1. **A pop-up** | 1. attractive or interesting; |
| 1. **To trick** | 1. to perform an act, usually with a negative connotation; |
| 1. **To suspect** | 1. a computer file that is sent together with an email message; |
| 1. **To be on the lookout** | 1. an action that is done to prevent something unpleasant or dangerous happening; |
| 1. **Appealing** | 1. an advertisement that is shown in a new window in front of the window that you are looking at on a website; |
| 1. **A precaution** | 1. to be continuing to search for something or someone; |
| 1. **A fraud** | 1. the crime of obtaining money or property by deceiving people; |
| 1. **An attachment** | 1. to think that someone has committed a crime or done something wrong; |
| 1. **To hijack** | 1. to make someone believe something that is not true, or to persuade someone to do something based on a false understanding of the facts. |

1. I'm always \_\_\_\_\_\_ for interesting new recipes.
2. Driving alone at night can be dangerous, so always take \_\_\_\_\_.
3. She \_\_\_\_\_\_ me into telling her what I was up to.
4. He was punished for a crime that he didn't \_\_\_\_\_\_.
5. He was prosecuted for \_\_\_\_\_.
6. We do not allow \_\_\_\_\_ of any kind on our website.
7. I'll email my report to you as an \_\_\_\_\_.
8. Hundreds of the department's powerful computers were \_\_\_\_\_\_ by hackers, who used them to send spam email.
9. The police \_\_\_\_\_\_ him of carrying out two bomb attacks.
10. He had a nice smile and an \_\_\_\_\_\_\_ personality.
11. **Watch the video. Put the statements in the order in which they are mentioned in the video.**
12. Steps for computer protection.
13. Description of malware.
14. Implicit signs of computer infection.
15. Purposes of using malware.
16. **Watch again and complete the following pieces of advice:**
17. Install security software from a \_\_\_\_\_ company and set it to update \_\_\_\_\_\_.
18. If you're not sure how, use the \_\_\_\_\_\_\_\_\_ and search for automatic updates.
19. Use a pop up \_\_\_\_\_\_\_, and don't click on links and popups.
20. Download software only from websites you \_\_\_\_\_\_and\_\_\_\_\_\_.
21. If you suspect \_\_\_\_\_\_\_\_\_\_, stop doing things that require passwords or personal info, such as online shopping or \_\_\_\_\_\_\_\_\_.
22. Update your security software and run a \_\_\_\_\_\_\_\_\_\_.
23. The most important thing you can do to \_\_\_\_\_\_\_ malware is to keep your computer software \_\_\_\_\_\_\_\_\_.
24. **Answer the questions:**
25. What is malware?
26. What types of malware do you know?
27. What are the goals of criminals when they use malware?
28. Why should you install security software only from a reliable company?
29. Why is it necessary to update your operating system and your web browser automatically?
30. What is often the purpose of unexpected calls or messages?
31. Why are email attachments sometimes dangerous to open?
32. What are the implicit signs of computer infection?
33. What should you do if you suspect malware on your computer?
34. Which tips (from the ones listed in the video) do you follow?
35. What tips can you add?