**Top Ten Online Threats**

There are now many threats that expose the vulnerabilities and weaknesses of computers and smart technology to steal sensitive data from individuals and organisations, much of the time we are unaware this is even happening, until it is too late.

The following list outlines the top ten online threats. Your task is to match the online threat to the correct definition:

|  |  |  |
| --- | --- | --- |
| **1. Spam** |  | 1. Secretly attach themselves to downloads and are designed to spread at an alarming rate. Can often be attached to files for download that are shared via CDs, DVDs, and USB sticks, or loaded on to computers by opening infected email attachments. |
| **2. Adware** |  | 1. Record a user’s keyboard actions, looking for distinguishable key entries, such as bank card details and passwords. This is often linked to identity and intellectual property theft. |
| **3. Trojan** |  | 1. Make their way on to a computer via a malicious email attachment or USB stick. Once your computer has been infected, it will likely send itself to every email address in your system. To the receiver, your email will appear harmless until they open it and are also infected by the same worm. |
| **4. Virus** |  | 1. The use of messaging systems to send multiple unsolicited messages to large numbers of recipients for the purpose of commercial advertising, manipulation intended to force lifestyle change or for fraudulent activity. |
| **5. Worms** |  | 1. Often found as web pages mimicking that of a trustworthy business, such as an online banking log-in page. Users will then enter their details, thinking they are logging in to their usual service and their details will be stolen. |
| **6. Phishing** |  | 1. A form of malware that is usually attached to pop-ups of downloadable files. Once installed on your computer it can monitor your keystrokes, read and delete your files, reformat your hard drive, and access your applications. Whoever takes control the has access to your personal details without you even knowing. |
| **7. Spyware** |  | 1. Present themselves as harmless computer programmes that can leave your computer or device completely unprotected so that hackers can penetrate your computer without being detected and steal any data they want from your system. A bit like somebody gaining access to your house keys without your knowledge and waiting for the right moment to steal your valuables. |
| **8. Keyloggers** |  | 1. A form of fraudulent activity. More often than not, official-looking emails are sent impersonating a well-known business such as a bank. These emails are sent to acquire people’s passwords and banking details. |
| **9. Pharming** |  | 1. Often sold as legitimate software but is in actual fact completely useless. Will often ask you to pay for extra protection, which is also a huge con. |
| **10. Rogue security software** |  | 1. A type of malware software that displays unwanted adverts when a user is surfing the internet. The ads often redirect searches to advertising websites and collect marketing data about the user. Some of these websites are infected with malicious content that is automatically downloaded to your computer upon access. |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|  |  |  |  |  |  |  |  |  |  |