IT

[Name of the Writer]

[Name of the Institution]

IT

**Main Post**

Network attacks are increasing day by day, and everyone is having threats of cyber attacks. Anyone can become a victim of a hacker, and they can infect their network by malware or Trojans. However, it is not appropriate to pay a ransom to have the system released from the attacker because if a one person pays attacker a ransom for releasing his/her system it will appreciate him/her and they will attack someone else again. They cannot only attack someone else but also to your system again. These attacks are not new as they were introduced in 1989 when the first attack occurred in which malware was spread between computers and floppy disks.

Many people are still only aware of the term virus, but they are not aware of malware and Trojan horses. However, there are certainly other methods which can help you to release system from the attacker instead of paying him/her ransom. If the attacker used encryption method to attack your system or network you can easily access to your system by putting your system into a safe mode. However, if an attacker uses another method simply to install a new operating system as soon as possible because you have no guarantee that an attacker will release your system after you pay the amount to them. It's better to try yourself because it is not that difficult (Efrony & Shany, 2018).

**Follow up 1**

Malware is a term that describes a malicious software or code that is very harmful systems. It can completely destroy your network, computer systems or mobile devices. Malware attacks can make changes in your computer and also can delete data from your computer easily. It may reduce the speed of your system and its difficult to identify.

**Follow up 2**

Trojan horse is another malicious computer program which bluff users and help attackers to get access to their systems. It can allow attackers to steal your confidential data and gain access to your system. They can also delete, modify, block and copy your data. Trojans can also disturb the performance of the computer network.

**References**

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? tallinn manual 2.0 on cyberoperations and subsequent state practice. The American Journal of International Law, 112(4), 583-657. doi: <http://dx.doi.org/10.1017/ajil.2018.86>