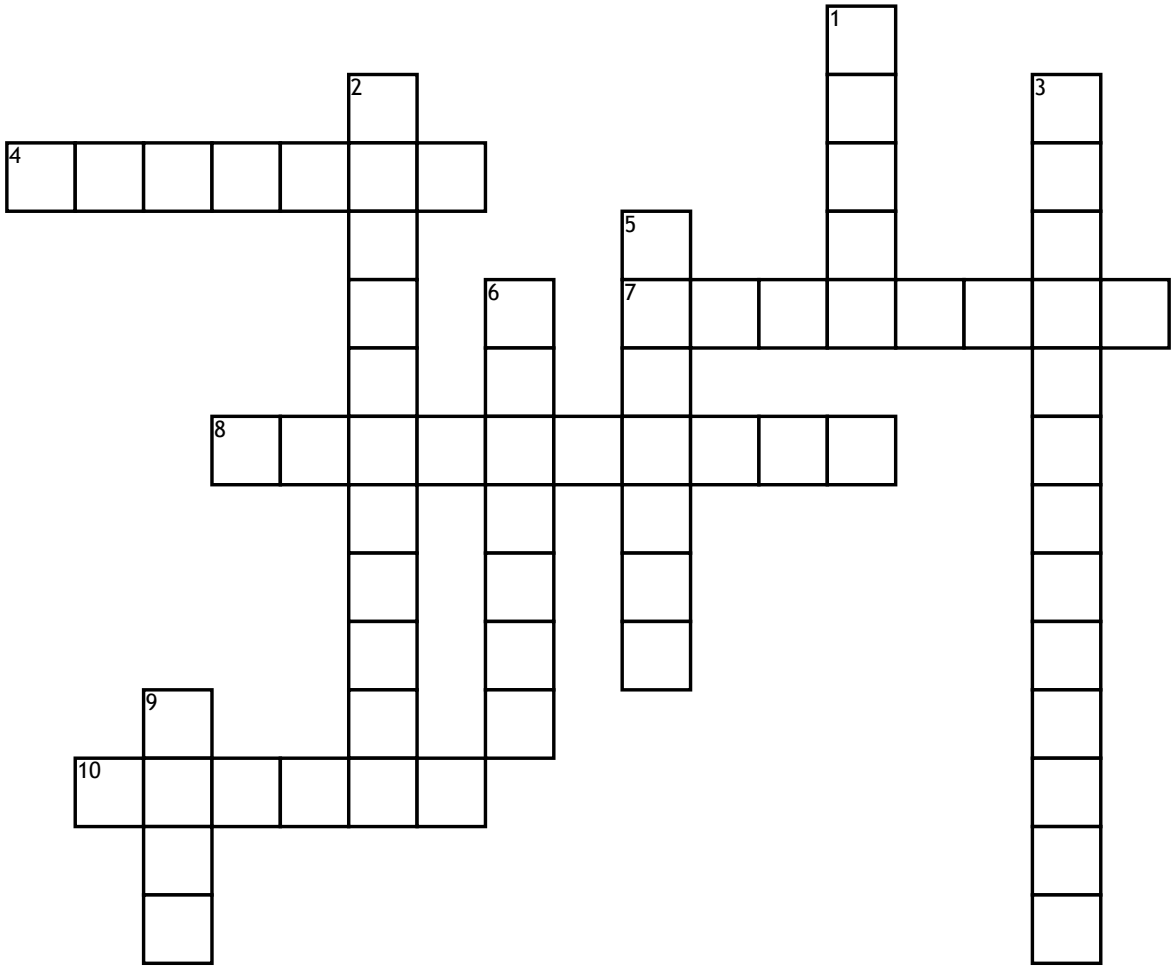
Name: _____ Date: _____

Malware and Viruses



Across

4. An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.
7. A technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.
8. A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.
10. A number of Internet-connected devices, each of which runs one or more bots. They can be used to perform Distributed Denial-of-Service attacks, steal data, send spam, and allow the attacker to access the device and its connection.

Down

1. A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.
2. A piece of malware that often allows a hacker to gain remote access to a computer through a “back door”.
3. A weakness in an information technology infrastructure that makes it susceptible to cyber attacks.
5. A type of malware that functions by spying on user activity without their knowledge. The capabilities include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more.
6. Another kind of malware that allows cybercriminals to remotely control your computer. These are especially damaging because they are hard to detect, making it likely that this type of malware could live on your computer for a long time.
9. A piece of malware that can replicate itself in order to spread the infection to other connected computers.