Type of Attack	Description	Detection
Malware	Software Program designed to damage or do unwanted actions in a computer. Common examples include viruses, worms, Trojan horses, spyware, and ransomware	Annoying pop-up massage on the computer system, system become sluggish at in appropriate time, some files are missing or deleted without the knowledge. Use good antivirus software to detect the malware or virus program.
Phishing	Attack sent via mail and ask a user to click on link and enter their personal data. They include link that direct the user to a dummy site, that will steals a user's information	Look for email address and sender name and make sure it comes from legit user, Check the domain name and URL of the website it should not point to suspicious link. Message do not create sense of urgency, not poorly, containing grammar mistakes.
Password Attack	Involves a third party trying to gain access to potential victim by solving a user's password	High number of authentication attempts, especially failed attempt due to incorrect password within a short period of time.
Denial of Service Attack	Attackers send high volume of data traffic through the network becomes overloaded and can no longer function	Monitor for significant increase in TCP-SYN (initial packet to establish a connection), Monitor DNS activity in case of number of DNS request packet will be considerably higher than the number of DNS response packet should be alerted, Monitor overall throughput and count ICMP packet provide early signs of warnings.
Man in the Middle	Information is obtained from the end user and the entity user is communicating with by impersonating the endpoints in an online information exchange (i.e. connection from smartphone to website)	Checking for proper page authentication and implementing some sort of tamper detection are typically the key methods to detect possible attack, but these procedures might require extra forensic analysis after the fact.
Drive by downloads	A program is downloaded to a user's system just by visiting the site. It does not require any type of action by the user to download.	Sometimes it is difficult to detect this attack easily, but proper monitoring of log , flow data and network packets cyber security expert can find out that system is compromised by drive by download attack.