Computer Threats: What are they, What can they do, and How to Reduce Vulnerabilities

Justyce Countryman
Jefferson Community College

What is a Computer Threat?

Computer threats make computer hardware and software vulnerable to cybercriminals. This may result in endangering one or more computing devices, network connections, and forms of personal information.

Reasons why Computer Threats Occur

- No anti-virus protection
- Not updating regularly
- Opening dubious emails or files
- Downloading hazardous software

Ten Possible Modern Computer Threats

- Malware: Any form of software that intends to take advantage of "any programmable device, service, or network." Internet criminals utilize malware for stealing computer data, files, and information.
- Adware: Software that displays inessential advertisements. Adware may exploit browser activity or take control of a computer.
- Ransomware: Encrypts all files until the user makes a specified payment. Sometimes installs by itself.
- Spyware: Software that could take personal computer information and monitor communication from a device without consent.
- Trojans: Tricks users into installing harmful software that appears to be safe. This may result in trojans watching computer activity, crashing computer systems, and sending more threats.
- Viruses: The portion of malware that executes malicious activity. Once a file with a virus is open, the computer receives the virus almost instantly. Email attachments are primary sources.
- Spam: Inessential messages through the internet with the objective of "advertising, phishing, or releasing malware." Spam is viewable because of bulk emails, instant messages, comments, and posts from social media.
- Worms: Spreads to multiple computers without user interaction and takes advantage of security vulnerabilities within software.
- Bots: Software that performs internet tasks automatically. Some bots aid the computer while others search for websites that contain potential malicious software.

Rootkits: Malware that is difficult for users to discover since it can bypass security protection software. Rootkits give cybercriminals almost full control of a computer. They may find passwords, credit card numbers, banking statements, and other personal information. Rootkits can also keep track of which keys a user types. They could stick around for a long time and continuously produce harm. Dangerous files inside of emails or risky applications are where this threat originates commonly.

Solutions for Computer Prosperity

- Install official or certified anti-virus software
- Enable Windows Defender
- Update all software as soon as possible
- Back up data consistently
- Refrain from installing applications that are not from reliable creators.
- Avoid opening websites or downloadable attachments that are clearly skeptical
- Utilize a firewall
- If there are signs of a rootkit attack, remove everything from the operating system

References

- https://www.monster.com/career-advice/article/computer-threats-protect
- https://www.metacompliance.com/blog/what-is-malware-and-how-to-prevent-against-it/
- https://www.mcafee.com/en-us/antivirus/malware.html
- https://softwarelab.org/what-is-adware/
- https://www.reveantivirus.com/en/computer-security-threats/what-is-spam
- https://www.imperva.com/learn/application-security/what-are-bots/
- https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html
- https://www.cnet.com/hhttps://www.metacompliance.com/blog/what-is-malware-and-how-to-prevent-against-it/
- ow-to/the-best-antivirus-protection-of-2020-for-windows-10/