

Cybersecurity Tips When Working From Home

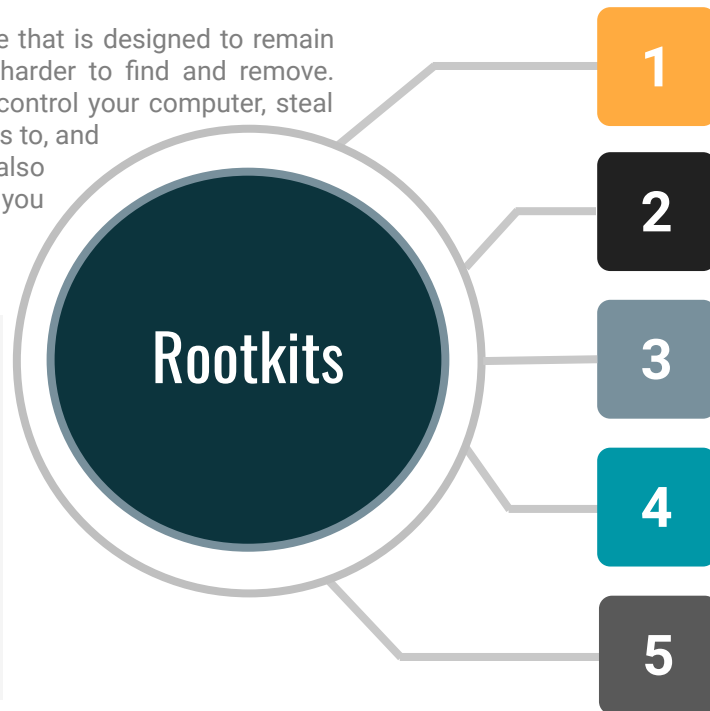
Rootkits

YOUR AWARENESS IS THE BEST DEFENSE

Rootkits are an advanced type of malware that is designed to remain hidden on your computer making them harder to find and remove. These viruses allow hackers to remotely control your computer, steal credentials to any account you have access to, and record your audio and video. Rootkits can also bring down your security software without you knowing.

ROOTKIT FEATURES

- Rootkits are designed to be difficult to detect. This is achieved by being in hard to reach areas of your computer such the system startup process itself.
- Rootkits hide from antivirus software by being in these hard to reach areas where scanners don't usually look.



1

How Rootkits Can Get on My Computer

Rootkits can get on your computer several ways such as via malicious emails or downloaded with seemingly trustworthy software.

2

How Can I Detect Rootkits

Most commercial home antivirus software include a special rootkit scans that require a system reboot. Your normal antivirus scan does not detect rootkits.

3

How Can I Remove Rootkits

Rootkits require specific tools tailored to different types of rootkits. Your antivirus software should recommend options if a rootkit is detected.

4

Keeping Rootkits Off My Computer

Keep software up to date and run occasional antivirus and rootkit scan above what is auto scanned. Do not download unfamiliar email attachments.

5

Backup Your Computer

Keep backups of your computer. By doing so, you can revert to a previous time when the rootkit was not on your computer.

For additional advice or to learn more contact us: info@guardsight.com