How to keep your computer secure in Linux

Making Linux desktop computer more secure involves a combination of best practices, system configuration, and regular maintenance. Here are some key steps to enhance the security of your laptop.

1. **Software Updates**
   Regularly update your system and all installed software to patch security vulnerabilities. Use the following commands to update your system:

   ```
   sudo apt update && sudo apt upgrade    # Debian / Ubuntu
   sudo dnf update                        # Fedora
   sudo yum update                        # CentOS (if applicable)
   ```

2. **Use Strong Passwords**
   Enforce strong password policies for user accounts. Consider using complex passwords with a minimum of 8 characters with at least one capital letter, number, and special character. Set a strong password for your user account and use a password manager to generate and store complex, unique passwords for your various accounts. Change passwords every 60 to 90 days.

3. **Disable root login:**
   Avoid logging in as the root user. Instead, use **sudo** to perform administrative tasks.

4. **Configure a firewall:**
   Use a firewall like ufw (Uncomplicated Firewall) or firewalld to control incoming and outgoing network traffic. Only open necessary ports.

5. **Full disk encryption:**
   Encrypt your entire hard drive using technologies like LUKS (Linux Unified Key Setup) during installation to protect your data in case of theft or physical access.

6. **Use secure boot:**
   Enable Secure Boot if your laptop and Linux distribution support it. This prevents unsigned or unauthorized code from running during boot.

7. **Regular Backups**
   Create and maintain regular backups of your data. Ensure that backups are stored securely and are regularly tested for restoration. Be sure to save work files on the SharePoint and/or OneDrive.

8. **Employ strong authentication:**
   Consider using two-factor authentication (2FA) for your user account, especially for remote login and sudo access.

9. **Lock your screen and change your screensaver settings**
   Set a screensaver and configure your laptop to lock the screen when not in use. Use a strong password or PIN for unlocking.

10. **Install and configure antivirus software:**
    While Linux is generally less prone to malware than some other operating systems, you can still install antivirus software, like **ClamAV,** to scan for threats.

How to keep your computer secure in Linux

11. **Employ a password manager:**
    Use a password manager to store and autofill complex, unique passwords for your accounts. Popular password managers are Bitwarden and LastPass.

12. **SanDisk USB Flash Drive**
    SanDisk USB Flash Drive is a useful tool for saving files and folders. The device is only meant to be used as a temporary storage. Files and folders should be deleted when no longer needed.