How do I best secure my personal computer and data?

Tell Me

1. The following table outlines some computer security tips:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Tip</th>
</tr>
</thead>
</table>
| **Antivirus, Antimalware, Internet security** | 1. Ensure that you are using a good quality antivirus/Internet security program and keep the program up-to-date with the latest upgrades and definition files.  
   a. Windows computers come with Windows Defender installed to help protect your computer. See this [Microsoft page](#) for more information.  
   b. [Sophos Home](#) is free for use on personal computers, Windows and Macs.  
   i. To install on your personal computer you can follow the steps.  
2. Schedule full scans on a regular basis, such as once a week. |
| **Operating System and Application Patches** | 1. Install operating system and application patches as soon as they are available and, if possible, enable automatic installation of patches from the vendor site. |
| **Password Safety** | 1. Create strong passwords to protect access to your accounts. The more characters you use in a password, the stronger it will be.  
   2. Use a combination of upper case letters, lower case letters, numbers and special characters.  
   3. Don't use dictionary words.  
   4. When changing your password make the new password unique and avoid reusing parts of the old password. Do not be tempted to use the same password for all your various accounts – personal computer login, NinerNET account, bank accounts, social network sites, etc. Never share your passwords. Do not store your passwords in plain text and physically protect any written passwords. Do not login to an untrusted computer with your UNC Charlotte NinerNET account credentials. |
| **Lock computer or Log Off** | 1. Lock your computer when you walk away, especially if it is out of view.  
   2. For extra security, set the automatic lock to enable after a short period of time.  
   3. Log off your computer and applications when planning to be away for a longer period of time.  
   4. If your computer is connected to the Internet, you should shut it down when it is not in use for an extended period of time, such as overnight, to avoid being hacked. |
| **Email Links/Attachments** | 1. Do not automatically click on links or open attachments in email messages received from known and unknown senders.  
   2. Hover your mouse over the link to check if the visible URL is an alias for the actual URL. The best practice is to copy and paste the URL into your web browser.  
   3. Check with the sender before opening any unsolicited attachments. Do not assume that because an email is FROM: someone you know that they sent it!  
   4. Disable the auto-preview feature to prevent emails with questionable or malicious content from being opened without your direct action.  
   a. The [IT Service Desk](#) can assist you with these settings. |
| **Phishing Emails** | 1. Do not respond to any email requests for your username, password or personal information.  
   2. UNC Charlotte will never send you an email message requesting your NinerNET username and password.  
   3. Do not provide your username, email address or password on any Internet site to which you linked from an email message.  
   4. Use common sense – if it looks suspicious it is probably malicious. |
| **Sensitive Data** | 1. Do not store sensitive data that is unencrypted (social security number, passwords, credit card numbers or research data) on your computer or digital devices. Mobile devices and storage media are easily stolen and any sensitive data they hold can be used for criminal activities. Make sure sensitive data is encrypted in transit. There are many free useful encryption applications available on the Internet. It is best to choose AES encryption with a high bit number and key size. If you are not required to retain sensitive data, you should purge it from your computer. |
| **Web Browser** | 1. Web browsers are not automatically set for secure browsing and you should secure your browser before surfing the Internet.  
   2. For detailed steps on securing the most popular web browsers visit [Securing Your Web Browser](#) and [Evaluating Your Web Browser's Security Settings](#) for more information. |
### Applications and Services

1. Delete any applications on your computer that you do not use since these are rarely patched and any existing vulnerabilities are susceptible to being exploited.
2. Disable any nonessential services running on your computer.
3. File sharing and print sharing are especially vulnerable to attacks from malware and intruders.

### Backup

1. Perform regular backups of your computer data.
2. Computer hardware is susceptible to physical failure, plus data can be deleted by mistake or maliciously by malware or an intruder.
3. Perform a full system backup followed by regular incremental backups. Best practice is to also perform a backup before making any changes to your computer.

---

### Related FAQs

- What vulnerability management tools are used at UNC Charlotte?
- How do I request an exception from University IT Guidelines for Endpoints, Systems and Applications?
- How does an endpoint device manager configure a device to use secure DNS?
- How does an endpoint administrator use Active Directory for centralized authentication?
- What is Alertus Desktop?