

1 Protect your personal information.

To minimize your risk of identity theft, don't share your personal info. unless you know how it will be used and protected. Use discretion when sharing information on social media sites like Facebook, MySpace and Twitter. Your birth date, address & other personal info. can be used for identity theft.

2 Protect your passwords.

Create easy to remember, hard to guess passwords and never share them with other people. Don't use the same password everywhere. And if you write them down, keep them in a secure location.

3 Protect your computer.

Implement a login password to access your computer. If you leave your computer unattended, lock it or log off – don't rely on it to lock on its own. Never leave your laptop unattended in a public place. If leaving it in a vehicle, hide it.

4 Protect your paper documents.

Limit printing of sensitive data. Lock sensitive documents in a drawer or cabinet. Shred sensitive documents that are no longer needed.

5 Backup your important files.

Backup your important files to external media and store it in a safe place, preferably off-site. Update your backups periodically and be sure to test restoration from backups periodically.

6 Don't open untrusted files and don't install untrusted software.

Only download and install reputable software from authoritative sources. Don't open email attachments if you don't recognize the sender or you weren't expecting an attachment.

7 Keep your operating system and software current.

Configure your operating system to install security patches automatically. Check the websites of other installed software periodically for security patches and updates.

8 Use antivirus, antispyware and firewall software.

Use antivirus software to protect you and your computer against viruses. Use antispyware software to protect against spyware. Use a firewall to protect against intruders and attacks. Since threats are always changing, keep your antivirus, antispyware and firewall software current.

9 Don't store unencrypted sensitive data on portable storage media.

Laptops and portable storage media like USB flash drives are convenient, but are easily lost. Use encryption software to render sensitive data unreadable by an unauthorized person.

10 Report data breaches and missing computers & data storage devices.

Immediately report data breaches and lost or stolen computers & data storage devices (including, but not limited to USB flash drives and CDs). If VCU devices or data are involved or if a loss occurs on a VCU campus, notify VCU Information Security. Otherwise, contact local law enforcement.