Top 10 Best Security Practices

These security recommendations are general guidelines that you should apply to all of your computing practices, whether at home, at school or at work.

1. **Lock your computer whenever you step away.** If you are using a Windows computer, the easiest way to lock it is by pressing the Windows logo key +L
2. **Create a strong password**. Your password should be at least eight characters. Use a mixture of upper and lowercase letters, numbers, and special characters. Try creating a password sentence and use the first letter from every word as your actual password. "Always drink 8 glasses of water each day!" becomes **Ad8gowed!** Never use common words, names, birthdays, or phone numbers.
3. **Never share personal information such as passwords, social security numbers, credit card numbers, and bank account numbers.** Only banks, your employer, and the government can legally require your SSN. Certain scams, known as "phishing," attempt to get this information from you by sending a seemingly legitimate message from a bank or other institution that asks for sensitive information "for verification purposes." Do not give out personal information over the phone, through the mail or over the Internet, unless you have initiated the contact or you are sure you know with whom you are dealing. No one from Information Services will ever ask you for your password.
4. **Never store sensitive data on mobile devices.** One of the easiest ways to compromise sensitive data is when your flash drive, laptop, tablet, or smartphone is lost or stolen.
5. **Use caution when opening e-mail attachments or clicking on email links.** One of the most effective methods of virus delivery is through the use of e-mail attachments. Virus writers use clever and mysterious subject lines and messages to pique the curiosity of users, and they know how to make the sender's address look like it is from someone you already know. You should always approach e-mail attachments with caution. Likewise, links to web sites which download viruses to infect your computer are frequently sent in email as well.
6. **Beware of Spam.** Spam is also known as Unsolicited Commercial E-mail (UCE). When you receive spam, delete it. You should never click on any web links or open attachments associated with spam. Do not respond to spam, including the "Take me off the list" or "Unsubscribe" link. This is usually a way for the sender to verify that your address is still active. Use spam filtering, if available with your email service. Spam filters can help identify unwanted email and lessen your chances of inadvertently clicking on a dangerous link.
7. **Keep your Windows patches up-to-date.** Set up your Windows computer to use "Automatic Updates." By enabling this feature, your computer will regularly check for any updates. Recommended updates will automatically download and install on your computer. Some updates require you to restart your machine before they take effect. Be sure to take this necessary step if prompted to do so!
8. **Install and run a virus scan consistently and regularly.** Install anti-virus software on your computer and keep the signature files current through automatic updates at least once per day. Do not connect to the Internet without first activating an anti-virus program. If you purchased an anti-virus system for your home computer, do not let your subscription lapse.
9. **Back-up files**. Back-up your data on a consistent basis (once a week). For easy back-ups, keep all document files in a central location, such as the "My documents" folder.
10. **Protect shared folders**. If you use a network shared folder, it must always be password protected otherwise you immediately open your computer to virus infection and computer compromises. Shared folders without passwords can be accessed by anybody and, therefore, offer no privacy. When assigning a password to a shared folder, follow the tips for creating strong passwords (See #4).