Public Computers

Protect Your Personal and Confidential Information

Working on confidential and/or personal information in public areas and on public computers is not recommended. Public computers can be used by a variety of individuals throughout the course of a day therefore; security cannot be verified. In order to protect your information and privacy, follow the steps below when working on a public computer:

Privacy Tips

1. **Delete your browsing history**: Use the browser tools available to delete your cookies and history when you're finished using a public computer. This will help to maintain your privacy and keep your information more secure
2. **Log out**: Anyone can access public computers. Be sure to close all browser tabs and log out of your accounts. Some public computers do this automatically but it's always best to confirm.
3. **Remember me NOT**: Be sure to disable the "remember me" function on public computers

The Risks

- Cybercriminals can insert themselves into your data conversations when connected to an unsecured or illicit wireless network.
- Shoulder surfing (people viewing your screen without your consent or knowledge)
- Loss or theft of your computer, smartphone, or tablet
- Malware (viruses, spyware and other unwanted software) installed on a public computer
- Theft of personal information

Be Security Smart

- **Connect to secure websites only:** Make sure the websites you visit are security-enabled. Look for **https://**, which ensures the security of your information. **http://** is not considered secure.
- **Keep Watch:** Don't leave your device unattended
- **Look Around You**: Be aware of your surroundings and ensure no one is shoulder surfing