Best Practice for Wireless BYOD

1. **Operating System and Applications**
    - Record the model number and serial number of your devices (hint - take pictures with your phone and email the pictures to yourself).
    - Enable the inactivity timer and require your password or biometric data to unlock the device.
    - Never leave your BYOD unattended or in your vehicle.
    - Never install unnecessary applications as they can be a means for infection and compromise.
    - Set strong access passwords for OS and applications if possible.
    - Make sure your operating system is current and patched with the most recent patches.
    - Applications can be a means to compromise your system so make sure they are updated as well.
    - Enable the operating system firewall on your device.
    - Disable remote administration and guest accounts if possible.
    - Never open spam mail on your BYOD device.
    - When connecting to a wireless SSID, verify what SSID you are connecting to.
    - Turn off the roaming setting when traveling and stay connected to only trusted SSID's.
    - Turn off wireless and bluetooth services until you are ready to use these services.

2. **Antivirus software**
    - Obtain a current AV product for your device that receives daily updates from the manufacturer.
    - Become familiar with how the antivirus software works.
    - Configure the antivirus software to perform daily updates to the virus definition files.
    - Set the antivirus to scan email attachments and downloads *before* you open them.
    - Perform regular scans of your entire device preferably during off hours. This will require you to leave your system on when you're not using it.

3. **Browsers**
    - Always use secure **HTTPS** browser connections.
    - Change the browser setting to prompt before downloading files.
    - Disable browser autofill settings.
    - Disable the browser setting to cache passwords, addresses, and credit cards numbers.
    - If available, enable the browser setting for protection from dangerous sites.
    - Clear your cache often! Set the browser to clear cache upon exiting when possible.
    - Always verify what website you are on (check the spelling).
    - Before downloading on a desktop or laptop, use the cursor to hover over the download link to confirm what site the download will come from.
    - Check the reputation of the download site using a resource like www.virustotal.com.
    - After downloading, scan the file with your antivirus software or a resource like www.virustotal.com.
    - Never install software from email links. Always use the manufacturer's download site, the App store, or a reputable download site. Check the reputation of the download site using a resource like www.virustotal.com.
    - If you receive an unexpected email file attachment, contact the sender to confirm they meant to send you a downloadable file.
    - After downloading an email attachment, scan the file with your antivirus software or a resource like www.virustotal.com.
    - Use VPN connections when available to attach to corporate resources when you are working off-site.

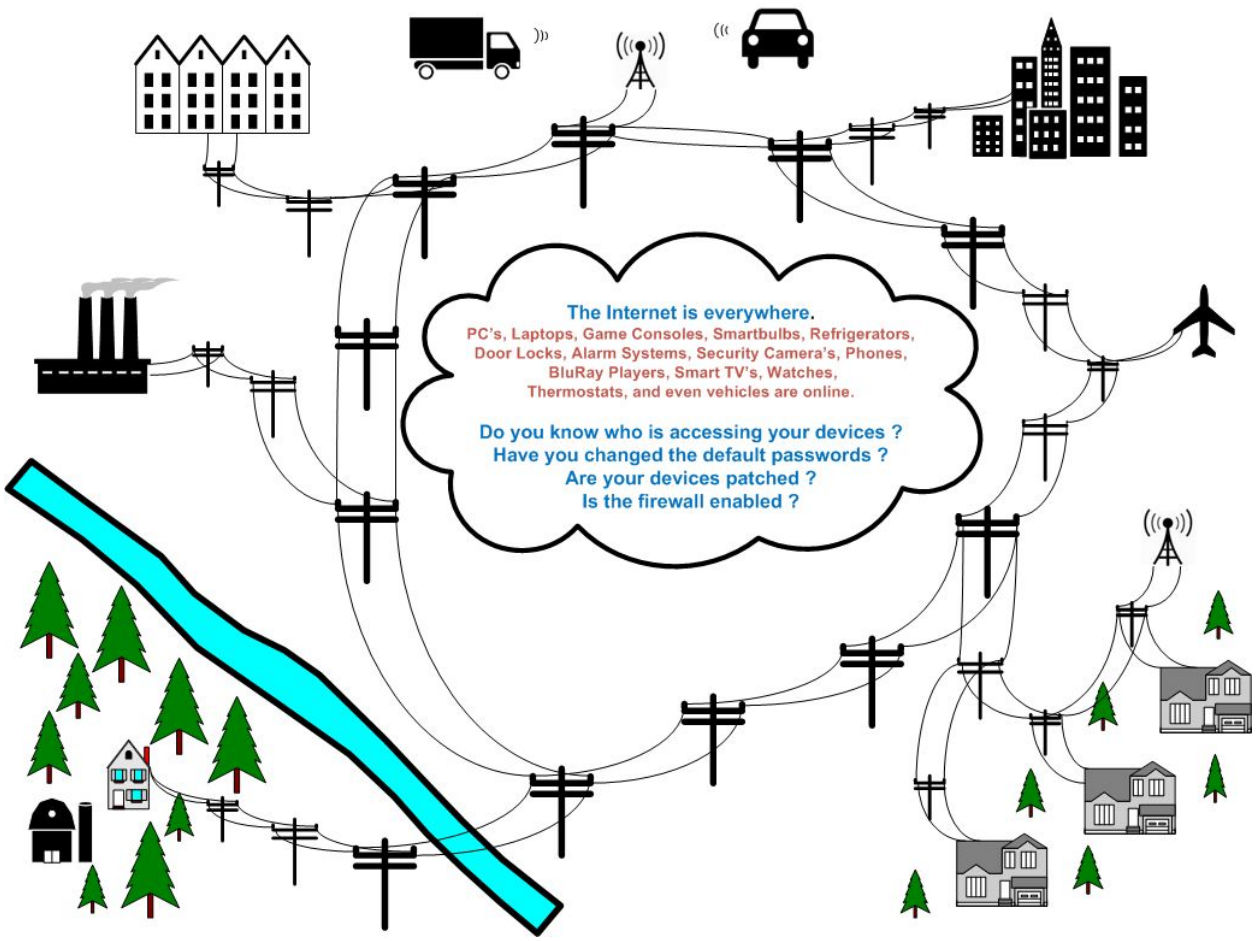
4. **Data**
    - Know where your data is stored and maintain data in an orderly manner (i.e., use appropriate Desktop, Documents, Downloads, Pictures, and Music folders).
    - Remove old files that are no longer needed to prevent unauthorized access and clutter.
    - Store your data in an encrypted format if possible.
    - Backup your personal data often using cloud storage or a USB drive.

- If using a USB drive for personal backups, secure the backup USB drive to prevent unauthorized access.

5. **Wireless information**
   - Everything you need to know to use Baker College Wireless networks is in our Wireless Info document.

6. **Minimum System Requirements**
   - Here are the Minimum Technical Requirements to access Baker College coursework and use our technical services.

Disclaimer: Any antivirus (AV) products or links in this document are for informational use only and not necessarily an endorsement of any specific product or service.




InformationTechnology