# CyberSecurity – Recommendations and Tips

<table>
<thead>
<tr>
<th><strong>Image</strong></th>
<th><strong>Recommendations and Tips</strong></th>
</tr>
</thead>
</table>
| ![Image](image1.png) | - Use complex password (phrase and &%#)  
- Change name if “Smith Family WiFi”  
- Activate guest network and use a different password  
- Router “recommended” WiFi firewall settings are okay to use  
- Attach battery backup to service provider router |
| ![Image](image2.png) | - Have different password and make it complex  
- If using cell phone “app” use different password  
- Do not leave “logged in” |
| ![Image](image3.png) | - Place family members on “guest” network  
- Allow them to share “that” password with friends as appropriate  
- Use router recommended firewall settings for guest network to increase security |
| ![Image](image4.png) | - Do not open unsolicited email and/or attachments  
- If in question, go directly to site versus following in email link  
- Do not use the contact information in the email, Find and contact directly |
| ![Image](image5.png) | - Just because you can connect it to your WiFi does not mean you should  
- Question when family members want to connect a device to your network  
- Remember that connecting friends (or family member friends) to your network means that internet traffic accessed by others will flow through your personal system |
| ![Image](image6.png) | - Lock phone – code/PIN  
- Turn on “find my iPhone” or “Android Device Manager”  
- Do not store PII information on phone  
- Do not “tag” pictures with time/date/location stamp  
- Do not store password on sensitive applications (web cams) |
| **Check for battery backup**  
| **Check connection to company (VOIP or POTS)**  
| **Regularly check system and panic button**  
| **Ensure that family members don’t share access code**  
| | **Exterior lights – automatic timers**  
| **Companies provide home safe assessments**  
| **Keep garage door openers hidden**  
| **Have house look “lived in” when gone**  
| | **Enact privacy settings**  
| **Careful on who you “friend”**  
| **Ask “friends” regarding their privacy**  
| **Complex password**  
| | **Watch for “skimmers”**  
| **Watch surroundings**  
| **Daylight and in an active area is generally the best time to use an ATM machine**  
| | **Check credit reports yearly**  
| **If victim of identity theft – have a plan - notify bank, credit cards, credit agencies, freeze credit accounts**  
| | **Updated anti-virus**  
| **Firewall settings on computer – generally recommended “okay”**  
| **Do not allow someone to “take over” your personal computer**  
| | **Use major company**  
| **Ensure that password is “very” complex**  
| **Look as to where your information is stored (some store overseas)**  
| | **Only join known networks**  
| **Do not join “personal” networks or networks that appear to be spelled funny**  
| **Know that your information will be accessible while using a public network. Always look for HTTPS:// - no banking should be done on free Wi-Fi**  

| **Company provide home safe assessments**  
| **Keep garage door openers hidden**  
| **Have house look “lived in” when gone**  
| **Enact privacy settings**  
| **Careful on who you “friend”**  
| **Ask “friends” regarding their privacy**  
| **Complex password**  
| | **Watch for “skimmers”**  
| **Watch surroundings**  
| **Daylight and in an active area is generally the best time to use an ATM machine**  
| | **Check credit reports yearly**  
| **If victim of identity theft – have a plan - notify bank, credit cards, credit agencies, freeze credit accounts**  
| | **Updated anti-virus**  
| **Firewall settings on computer – generally recommended “okay”**  
| **Do not allow someone to “take over” your personal computer**  
| | **Use major company**  
| **Ensure that password is “very” complex**  
| **Look as to where your information is stored (some store overseas)**  
| | **Only join known networks**  
| **Do not join “personal” networks or networks that appear to be spelled funny**  
| **Know that your information will be accessible while using a public network. Always look for HTTPS:// - no banking should be done on free Wi-Fi**  

| **[Image of a home with exterior lights on](image)**  
| **[Image of a garage door opener](image)**  
| **[Image of a person with a computer](image)**  
| **[Image of a credit card with an identity theft alert](image)**  
| **[Image of a security system](image)**  
| **[Image of a cloud storage system](image)**  
| **[Image of a free Wi-Fi logo](image)**  

---

**Check for battery backup**  
**Check connection to company (VOIP or POTS)**  
**Regularly check system and panic button**  
**Ensure that family members don’t share access code**  

**Exterior lights – automatic timers**  
**Companies provide home safe assessments**  
**Keep garage door openers hidden**  
**Have house look “lived in” when gone**  

**Enact privacy settings**  
**Careful on who you “friend”**  
**Ask “friends” regarding their privacy**  
**Complex password**  

**Watch for “skimmers”**  
**Watch surroundings**  
**Daylight and in an active area is generally the best time to use an ATM machine**  

**Check credit reports yearly**  
**If victim of identity theft – have a plan - notify bank, credit cards, credit agencies, freeze credit accounts**  

**Updated anti-virus**  
**Firewall settings on computer – generally recommended “okay”**  
**Do not allow someone to “take over” your personal computer**  

**Use major company**  
**Ensure that password is “very” complex**  
**Look as to where your information is stored (some store overseas)**  

**Only join known networks**  
**Do not join “personal” networks or networks that appear to be spelled funny**  
**Know that your information will be accessible while using a public network. Always look for HTTPS:// - no banking should be done on free Wi-Fi**