















CyberSecurity – Recommendations and Tips

	<ul style="list-style-type: none">• 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
	<ul style="list-style-type: none">• Have different password and make it complex• If using cell phone “app” use different password• Do not leave “logged in”
	<ul style="list-style-type: none">• 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
	<ul style="list-style-type: none">• 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
	<ul style="list-style-type: none">• 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
	<ul style="list-style-type: none">• 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)

	<ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • Exterior lights – automatic timers • Companies provide home safe assessments • Keep garage door openers hidden • Have house look “lived in” when gone
	<ul style="list-style-type: none"> • Enact privacy settings • Careful on who you “friend” • Ask “friends” regarding their privacy • Complex password
	<ul style="list-style-type: none"> • Watch for “skimmers” • Watch surroundings • Daylight and in an active area is generally the best time to use an ATM machine
	<ul style="list-style-type: none"> • Check credit reports yearly • If victim of identity theft – have a plan - notify bank, credit cards, credit agencies, freeze credit accounts
	<ul style="list-style-type: none"> • Updated anti-virus • Firewall settings on computer – generally recommended “okay” • Do not allow someone to “take over” your personal computer
	<ul style="list-style-type: none"> • Use major company • Ensure that password is “very” complex • Look as to where your information is stored (some store overseas)
	<ul style="list-style-type: none"> • 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