The Church of Jesus Christ of Latter-day Saints
Kansas City Missouri Stake
850 SE Church Road
Lee's Summit, MO 64063

Stake Self-Reliance & Emergency Preparedness

Monthly Newsletter

May, 2021

Personal Cybersecurity

By Jason Bowne
Kansas City Stake Self-Reliance Specialist
VP Information Technology, JE Dunn Construction

What Is Personal Cybersecurity? *(sounds complex)*

Cybersecurity is the act of protecting digital systems (of ALL kinds) and digital assets (like your information or access to your information). Personal Cybersecurity is the application of cybersecurity principles and practices into your daily life to protect your 1) personal information, 2) personal devices, and your 3) Personal Area Network (PAN).

Over the next three months, I will discuss get into each of these, using, easy-to-understand technical interpretations that make sense and are applicable. I will also provide some tips and resources for you to learn more about this and what to do to help you protect those three important areas above and share resources for you to learn more.

Why Is This Important?

I am a huge geek and I love technology. I know I am dating myself some, but I remember when the internet didn't exist and when it first became public to the world. I experienced a text based internet through dial up bulletin boards, ftp, gopher etc.. and then this amazing thing came to the scene called the Mozilla browser, then Netscape Navigator. Yeah, I know a lot of you are smiling with me ;). Cybersecurity wasn't even a term back then, but neither were cell phones that could access bank accounts, send money electronically from phone to phone, and connect with billions of people over social media (because that didn't exist either).

Times have change drastically. We live in a digital economy at a global scale. There are very few areas of our lives that are not touched by technology, providing us an enormous amount of good, like:

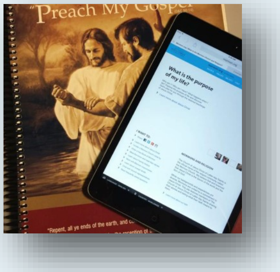
- Ability to connect with family and friends anywhere in the world at any time, share pictures, memories, have multiple person video calls and stay connected. Could you imagine how damaging COVID would have been without the internet if we were all isolated with no way of connecting other than a hardwire telephone line?

(continued on next page...)

Inside this issue

Spiritual Insights

- Preparation, both spiritual and temporal, can dispel fear
- "...if ye are prepared ye shall not fear " (Doctrine and Covenants 38:30).
- "The need for preparation is abundantly clear. The great blessing of being prepared gives us freedom from fear" (Elder L. Tom Perry)



Technology can provide an enormous amount of good

- *Ability to connect with family and friends anywhere in the world at any time, share pictures, memories, have multiple person video calls and stay connected*
- *Digital safety features in vehicles*
- *Artificial Intelligence*
- *Electronically secure paycheck deposits*
- *A watch on your wrist that can make phone calls, receive/ reply to texts and emails, pay for things at stores, and oh… do an EKG !*
- *A device you can carry in your pocket that has more computing power than entire buildings of computers from the 1960's*

- Digital safety features in vehicles. Electric vehicles can drive themselves – and I would even venture to say, in many situations, can drive better than a human can.
- Artificial Intelligence – through machine learning and massive data collection, computers can do things people could never have done in data and decisions etc.
- Electronically secure paycheck deposits going into our bank accounts without the fear of losing a paper check after it was endorsed.
- A watch on your wrist that can make phone calls, receive/reply to texts and emails, pay for things at stores, and oh…do an EKG – now that is Star Trek and Star Wars combined!
- A device you can carry in your pocket that has more computing power than entire buildings of computers from the 1960's.
- The amazing feeling from telling your house to turn the heat up or down, to turn lights on or off, or even your garage door opening when your phone is with you in the car and your 'smart home' sees you are close. Some may think this is a little too much, but I use it as an example.

These are just a few examples as there are many, many more. Now look at that list and think like a criminal. The opportunity to steal, embezzle, destroy, and corrupt is enormous. This is what a 'hacker' is, and this is exactly what they do. There are many methods they employ to get into your PAN (personal area network – like your home Wi-Fi) and find devices that they can 'hack' into (computers, Wi-Fi connected sound systems, Wi-Fi connected smart plugs etc..). Once inside your network, they find computers that have not been patched or have bad software on them and can then install keyloggers to capture your keystrokes when you log into your bank or whatever. That information comes back to them, allowing them to log into your bank online and perform transfers of money out of your account into theirs - and then it is gone. This is only one example – others get much worse than just losing money, but I don't want to scare you too much as, we just read, there is an enormous amount of GOOD that technology brings us.

So why is Personal Cybersecurity important? It protects our ability to do the good things with technology and not be taken advantage of by those that want to do harm to us in a digital way.

Personal Devices

This month, let's dig into personal devices as this is VERY important.

(continued on next page...)

Let’s tackle the biggest one – your cell phone. I know many people that use their phone more than a computer by a mile. Many companies have a ‘mobile first’ approach to their business. Given that mobile phones are in such massive use, the focus from hackers on phones is huge. Here are some things you can do TODAY to better secure your device, the information it can access, and the information it stores.

- **Patch your device** – learn about how to update your phone and set your phone to automatically perform updates at night when connected to wifi and plugged in. In addition to this, manually check to make sure BOTH your phone and apps are updated. I am an iPhone user so here are the steps to do this. Android is similar in practice, and you can go to youtube.com and search for ‘update android phone system and apps’

  - iPhone system update: tap settings (gear icon) > tap General > tap software updates. If your phone is up to date great you are done, if not and an update is shown – update it now if you can - don’t wait.
  - IPhone app update: tap on the app store > tap on the person icon in the top right > pull down the screen to do an update check > tap ‘Update All’ in the middle of the screen (it will show you how many apps are getting updated)

- **Remove un-needed apps from your phone.**

  - In my job, I have a team that manages cell phones and we see phones that have up to 100 apps. The person that uses the phone has no idea what is installed. Most of the time, they installed the app to do one thing or see what it was then just left it. All these apps contribute to what is called ‘an attack surface’ or ways a hacker can get in. If a company that makes an app gets hacked and the hackers can get to your phone through that app – bad things can happen. This doesn’t happen a lot, but it can. Simply removing apps you don’t need will reduce that ‘attack surface’.

- **DON’T click on emails that say anything about urgent need of information or your account will get disabled, or some incredible deal that will only last for the next hour** – review them on your computer with a full browser.

  - You can’t see where emails like this come from, or where the link in the email goes to. You need to get on a computer with a full browser to look at it by ***hovering*** the mouse arrow over (***NOT clicking***) the link, then you can see that the email you got from “Netflix” came from 23ei4ofjwien@netflix.iwillscamyou.com (you get what I mean J). More will be covered next month in the Personal Information portion along with Password Management.

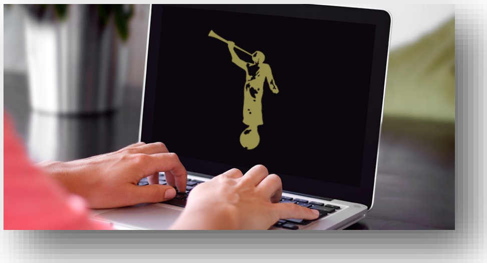
(continued on next page…)

- **Make use of voicemail for unknown calls** – just because your phone rings doesn't mean you need to answer it.

  - Put phone numbers you know in your contacts so that, when they call, your phone shows you the name. Ensure you know how to delete and then clear your voicemail. Block calls that you do not want to call you any longer. Again, if you don't know how, go to YouTube and search for 'how to block calls on iPhone' or android etc..

- **Turn off Wi-Fi and Bluetooth if you are not using it.**

  - When you are away from home, these 2 technologies are always searching for a connection. Hackers will do very tricky things like sit in a Starbucks and create a Wi-Fi network called 'Starbucks-high speed' > you see that and think "oh cool, Starbucks put in a free high speed Wi-Fi network" > you connect your phone to it > they now own your phone and can pull off just about anything they want, including that notes file that has all your passwords in it (shame on you – I will cover password management next month).



- **ONLY use public Wi-Fi if you have a VPN (virtual private network) service.**

  - VPN service will encrypt the data from your phone to where you are going in your app or browser so hackers on the public Wi-Fi can't see it.
  - If you don't want to get or pay for a VPN service – simply just turn off Wi-Fi and use your cell data network. Public Wi-Fi has become a theme park for hackers and your phone is the 'ring toss' game ;)

Now that we have covered cell phone security pretty well, we need to now cover one of the primary ways hackers get information from people and companies – the computer. I will cover Microsoft Windows and Apple Mac computers as they are the most prevalent used in our society.

Microsoft Windows Computers:

Whether you use a desktop computer, laptop computer or a tablet that runs Microsoft Windows, this section will cover some of the basic security things you should be doing to keep them as secure as possible. Here are a few simple actions for you do to:

- Keep Windows UP TO DATE! This is critically important, so much so I would suggest you put a reminder on your calendar to ensure it is up to date.

  - If you are not running Windows 10 – you need to be! All previous versions of windows are not only outdated, but Microsoft no longer patches them – this means that your computer could very, very easily get hacked and there is nothing that you can do to prevent it. So, if you are on Windows 8 or earlier – you should look at doing an upgrade or getting a new computer.
  - In Windows 10 > click the **Start** button > then click the gear for **Settings** > then click on **Updates** in the options

(continued on next page...)

- ◊ In here, click on Advanced Options and ensure you have the top option turned on – which is to install updates for other items. This will pull down other patches for software outside of windows if it is available as well as drivers and other hardware updates for the brand of computer you have.
- ◊ Click the back arrow in the top left to get back to the updates area
- ◊ Now click on 'Check for updates' button > this will contact Microsoft and do a check for anything that you don't have that you should > will download and then install the patches. Be patient as you might be waiting a long time if you have a lot of patches.

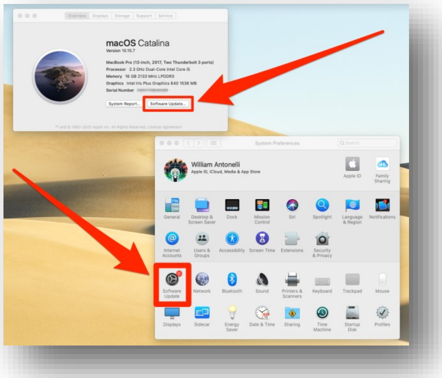
∗ I also recommend running the Windows Store App > then clicking the triple dots in the upper right and select download updates > then click on get updates. This will update any windows native and store apps that are installed

- I also highly recommend that you sign into windows with a Microsoft account – you don't need a new email address to create an account. Simply go to https://account.microsoft.com > and create an account if you don't have one. When prompted what email you would like to create, select the option to use your own email (be it Gmail, Yahoo etc..)
  - ∗ Then in windows, click **Start** > type "**account**" > select to **sign into Windows with your Microsoft account**
  - ∗ This will give you access to OneDrive to protect files / as well as enable you to encrypt your hard drive with BitLocker and save the key within your Microsoft account. This just means that if someone steals your computer they would have to sign in as you to get to your files – if they take the hard drive out, BitLocker will prompt for a very long key to access (which key is in your Microsoft account, so they can't get to it)

Apple Mac (iMac / MacBook etc..)

All the Apple Mac computers run what is called MacOS (similar to a PC running Microsoft Windows). The Mac OS needs updated as well.

- Keep MacOS UP TO DATE!
  - ∗ Click on the gear on your dock 'system preferences'



macOS Catalina
Version 10.15.7
MacBook Pro (13-inch, 2017, Two Thunderbolt 3 ports)
Processor 2.3 GHz Dual-Core Intel Core i5
Memory 16 GB 2133 MHz LPDDR3
Graphics Intel Iris Plus Graphics 640 1536 MB
Serial Number [redacted]

  - ∗ Click on **Software Update**
    - ◊ If there is an update to the macOS – install it
    - ◊ I would highly recommend checking the box to Automatically keep your mac up to date
    - ◊ I also recommend clicking on the Advanced button and checking all the boxes to get all the updates, install them etc..

(continued on next page...)

    - You also need to keep your apps up to date > open the App Store app
        - On the left, click on updates > and update all the apps that need it

- Ensure you are signing into your mac with an AppleID – most do but if you do not, I would recommend you do. The integrations are great and changing your AppleID password will change it on your mac as well as your iPhone etc..
- Turn on your firewall / encrypt your drive with file vault / and check the privacy settings on your mac
    - In system preferences (the gear icon) > open security and privacy

    - Click on firewall tab > unlock the setting in the lower left > then turn it on
    - Click on the FileVault tab > unlock the setting in the lower left > **you need to have your password or filevault key to get to data – if you lose both of these your mac basically turns into a paperweight and your data is gone – so do this carefully**
    - Click on the privacy tab > review all the settings and change the ones you don't need
        - This is where things are like giving zoom access to the microphone and speakers etc. are found.

Other devices connected to your network:

This is where we address all other things like smart plugs, google homes, amazon echo etc.. Think of all these things as tiny little computers in themselves. They all need to be secured, updated, and properly configured to not provide an entrance into your network to then poke around.

I won't be covering all the kinds of devices as there are literally hundreds - if not thousands - of types of devices that connect to your network, so I will give some overarching mindset and thinking that you should be doing with each device.

Does the device have an app?

- Many devices have an app that you install on your phone to manage the device – install it / learn it / configure the device the way you want and check for updates
- Put a reminder in your calendar 1x a month to check for updates
- Only give the device the access it needs on your network, just because it can connect to everything doesn't mean it needs to

A word on Google Home and Amazon Echos:

- Ensure you dig into the privacy settings of these devices and turn off anything that you don't need – like promotions and sales emails based on data it collects and sends to Amazon or Google
- Option out of any configuration that wants to send information back to the mothership – they don't need it, they already have enough

*****NEXT MONTH: Personal Information & Password Management*****

~Bowne

Emergency Preparedness—Lesson #5

Shelter in Place

“. . . Our homes can be, and should be, a refuge and a sanctuary from the troubled world we live in.” Eran A. Call of the Seventy. October 1997

Here in the Midwest we are all familiar with weather warnings such as this:

“The National Weather Service has issued a Winter Weather Advisory. Snow expected to fall throughout the day and into the evening hours. Limited visibility due to blowing snow. Roadways will be slippery and hazardous. Unnecessary travel should be avoided.”

In addition to weather emergencies, other situations require us to stay put. A recent example of this happened in Atchison, Kansas when a chemical plant spill sent dangerous fumes into the air. Residents were cautioned to shelter in place for several hours.

Read: Many incidents give us fair warning of their onset. Whether they are quick moving or slow behemoths, the earlier the warning signs, the better prepared you can be for their eventuality. Staying-put is the most likely thing you will do in the face of danger. Sheltering-in-place, especially when well prepared, will help you stay in a safe, secured location until the threat passes.

With most identified hazards, your reaction should be to Shelter-in-Place. Sheltering in place means that you will maintain your current location until it is safe for you to venture out again. Incidents may only last a few moments, where more long-term and severe events may last weeks. It is an unfortunate fact that most fast-paced incidents will see you sheltering in place outside of your home - whether on the road, a store, or (in many scenarios) your work or office. Keeping supplies on-hand outside of the home in your car or at your place of work is highly recommended.

Your home should be your safest refuge. Sheltering at home should be the gold standard for any hazard or threat. Please note, that this means dedicating resources and time to not only safeguarding your home, but also assuring that you have sheltering capabilities at your home. For instance, a house located on the coast may be a poor shelter from a hurricane. Likewise, a home in tornado alley without a basement or cellar will often be an inferior protection. Be sure to note whether you will shelter at home or move to a safer location prior to imminent threats. Do not leave a location after a threat or hazardous incident has begun - this may kill you!

(continued on next page…)

What is “sheltering in place”?

Sheltering in place means that you will maintain your current location until it is safe for you to venture out again. Incidents may only last a few moments, where more long-term and severe events may last weeks. It is an unfortunate fact that most fast-paced incidents will see you sheltering in place outside of your home - whether on the road, a store, or (in many scenarios) your work or office. Keeping supplies on-hand outside of the home in your car or at your place of work is highly recommended.

Ponder: Is my home a shelter from the physical and spiritual storms in the world?

Read: Sheltering at home is almost entirely a subject of having enough supplies on-hand to outlast an incident. The most likely scenarios to keep you sheltering at home (rather than evacuating) are weather related. Staying inside until all danger has passed is the first step.

Stockpiling the emergency supplies you will need to shelter in your home requires auditing what storage you already have on-hand. Sheltering supplies requires more than just a minimal supply for eating, drinking, and washing. Hygienic items (toilet paper!) are some of the more overlooked items for extended stays at home. Supplies should be kept in a safe, long-term location for access in an emergency.

TORNADOES AND ROAD SAFETY

WHAT TO DO

Get off the road. The best option is to drive to a designated shelter, basement or safe room.

OR

The next best option is a small, windowless room or hallway on the lowest floor of a sturdy building.

WHAT NOT TO DO

Do not seek refuge in a vehicle, outside or under an overpass. A highway overpass does not provide safety from a tornado.

DO NOT seek shelter under an overpass or a tree. This puts you at greater risk of being killed or seriously injured by flying debris from the powerful tornadic winds.

Discuss: What can you do within your home to make it a place that is comfortable for an extended sheltering situation?

Read: "All members of the Church can make efforts to ensure that their place of residence provides a place of sanctuary from the world. Every home in the Church, large or small, can be a "house of prayer, a house of fasting, a house of faith, a house of learning, a house of glory, a house of order, a house of God" (D&C 88:119). Church Handbook, Families and the Church in God's Plan.

1. Sheltering at Work

Read: Sheltering at the office is much more difficult; having supplies stockpiled at work will help you weather an incident. Storage can be limited in space and permission in office environments. Storing supplies should be enough to last you for 72 hours. Many workplaces store a certain amount of supplies on hand as well. While 3 days may seem like a lot of time to stay at your office, keep in mind that communication and transportation infrastructure may be damaged. Having back-up options readily available will help to assist you and others in getting to help after an incident occurs, or help you sustain your current location until help arrives or you're able to make it home again.

2. Sheltering on the Road

Read: Incidents may occur while you are in transit. When the unexpected occurs while you are driving, you will need to plan to spend an extensive amount of time in your vehicle. You may even find yourself stranded far from help. Your car emergency kit should feature enough food, water, and emergency supplies to keep you safe for up to 72 hours. Be sure to note that you may require weather related items- fuel in your car may not be reliable or needed strictly for travel, so idling your vehicle for air conditioning or heat would possibly be detrimental. Pack cold weather gear and know how to shelter from the sun in these conditions. Hydration is extremely important - remember to keep your water stored properly in your vehicle.

(continued on next page…)

Read: Things to do in preparation:

- Keep a supply of signaling items in your car. This can include road flares, glow sticks, flashlights, etc.

- To increase your odds of being found, predefine your roadways and paths, and share them with loved ones. Preplanning your route and letting others know will help rescue workers know where to search in order to find you, if you fail to show up at your coordinated area.

- Staying put until help arrives. In most minor incidents, staying put is your best bet for survival. If it is not dangerous at your current location, sheltering-in-place wherever you may be is a good solution. Unknown damage to infrastructure and secondary and tertiary threats will make the way treacherous.

- When sheltering at a safe location, make sure that you can be easily found, or others know where you are. For large-scale disaster and emergencies, or small incidents which may require immediate response and survival tactics, preplanning your travel and locations is necessary, as well as having the proper supplies.

Ponder: Consider how you can safeguard your home to be a place of sanctuary from both physical and spiritual calamities.

Activity: Do a quick exercise to assess your home & work placed for safety in different weather emergencies. Consider the following emergencies: heat wave, thunderstorm and lightning, tornado, and winter storm.

Ask yourselves the following two questions:

- Is our home & workplaces a good location for sheltering in place?

- If not, where else could we go during those emergencies?

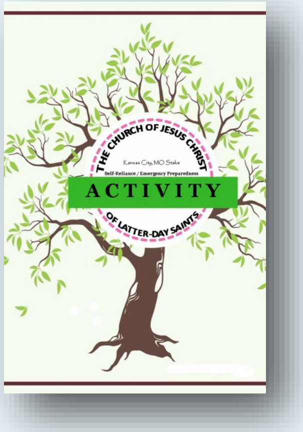
Commitment: I will prepare a shelter in place plan for my home and work.

Resources:

- CDC - https://www.emergency.cdc.gov/shelterinplace.asp

- Red-Cross (home, work, school and vehicle) shelterinplace.pdf (redcross.org)

- Ready.gov- https://www.ready.gov/shelter


THE CHURCH OF JESUS CHRIST
Kansas City, MO Stake
Self-Reliance / Emergency Preparedness
ACTIVITY
OF LATTER-DAY SAINTS

ACTIVITY

Do a quick exercise to assess your home & work placed for safety in different weather emergencies. Consider the following emergencies: heat wave, thunderstorm and lightning, tornado, and winter storm.

Ask yourselves the following two questions:

- Is our home & workplaces a good location for sheltering in place?

- If not, where else could we go during those emergencies?

Commitment

I will prepare a shelter in place plan for my home and work.

12 Principles of Self-Reliance

The Lord has declared, “It is my purpose to provide for my saints” (D&C 104:15). This revelation is a promise that the Lord will provide temporal blessings and open the door of self-reliance. He has also declared that “it must needs be done in [His] way” (D&C 104:16). To receive the blessings of self-reliance, we must accept and live the principles of self-reliance, which include the following:

- Exercise Faith in Jesus Christ (D&C 104:15)
- Use Time Wisely (Alma 34:32)
- Be Obedient (D&C 130:20–21)
- Manage Money (D&C 104:78)
- Work: Take Responsibility (D&C 42:42; 2 Nephi 2:16, 26)
- Solve Problems (Ether 2:18–19, 23; 3:1, 4)
- Become One, Work Together (Moses 7:18; D&C 104:15–17)
- Communicate: Petition and Listen (D&C 8:2)
- Persevere (Hebrews 12:1; D&C 58:4)
- Show Integrity (Mosiah 4:28; Job 27:5; Articles of Faith 1:13)
- Seek Learning and Education (D&C 88:118–119)
- Stay On Task, Receive Ordinances (D&C 84:20; D&C 136:4; 1 Nephi 18:2–3)

Self-Reliance Services

What is Self-Reliance?

“Self-reliance is the ability, commitment, and effort to provide the spiritual and temporal necessities of life for self and family” (Handbook 2: Administering the Church[2010], 6.1.1).

President Thomas S. Monson has counseled, “[Self-reliance] is an essential element in our spiritual as well as our temporal well-being.” (“Guiding Principles of Personal and Family Welfare,” Ensign, Sept. 1986, 3)

Kansas City Stake Self-Reliance Committee Members

President Martin Cooper

Brother Bryant Staples

Brother Gary Arnett

Brother Jason Bowne

Sister Karen O’Riley

Brother Arlen Tanner

Sister Patty Tanner

Sister Michelle Truman

Sister Tammi Iba

Brother Brent Ellibee

Brother Todd Hendrickson

Sister Rebecca Hendrickson

Brother Van Celaya II