Security Best Practices (December 2023)

ThePeopleOfTheBook.Org

It is good to establish and maintain a culture of security to protect ourselves and our missionaries.

1 Always use antivirus software on your personal devices: There are several free ones and multiple subscription services to keep your computer virus free. Download and use one. Upgrade your device if you think the antivirus program slows it down. iPhones are pretty secure and probably do not need an antivirus app unless you are visiting questionable/bad websites. Malwarebytes for iPhone might be good to alert you if you start to visit a bad website.

2 Always use a device firewall: A firewall is an excellent line of defense against malicious software that attempts to connect out to its home server. You'll receive a warning when an attempt is made, and you can optionally block the communication. Blocking the communication won't remove the infection, but it will render it mostly harmless, especially if it is one of the many "logger" infections that grabs your data as you type it into websites or client software.

3 Keep your operating system and software up to date and make regular backups: Yes, it's a pain to keep your apps and operating systems up to date because doing so often requires a reboot. However, it's for your own good. Keep everything backed up regularly or you may find that you have lost it all.

4 Never download pirated or cracked software: This type of software almost always includes some type of malware. Plus, it's illegal to steal software, so there's that aspect of it. Use a modern, secure browser from a reputable company. Downloading apps, movies, or songs without paying is illegal anyway.

5 Don't click on popup windows or install apps that tell you that your computer is infected with a virus or promises to clean up your system: Antivirus software doesn't work that way. Those popups install malware onto your computer, with your permission.

6 Be careful with email attachments and phishing: Not all email attachments are harmful, but unless you're expecting an attachment from someone you know, don't download or open it until you're sure it's OK to do so. If it's from someone you don't know, delete the email or identify it as spam. Do not download or open the attachment. Be careful about plugging in someone else's flash memory stick to your device.

7 Don't use public wi-fi hotspots without using a VPN (secure) connection and maintain control of your physical devices: Do not connect to a public wi-fi unless you do so through a VPN. A VPN will encrypt your communications to and from the internet so that anyone who might be eavesdropping can't steal your information. Your device should have a password to access it and it should never be out of your site. (Except where there is no one around who could possibly mess with it.)

8 **Use passwords on everything and be sure that they're strong passwords:** Do not use the same password for everything. Do not use easy-to-guess passwords. Use strong passwords that are at least eight characters in length and include capitals, numbers, and alternate characters. You can also use phrases. Passwords should be used to protect everything: Devices, email, VPN, anything that you don't want shared with others. Use a good password manager. It is not necessary to change them too frequently. ***Passwords are now starting to be replaced with fingerprint software, iris recognition, facial recognition, and some other technologies.***

9 **Beware of what kind of information you share on social media sites:** A lot of people love Facebook and place photos on it, have conversations on it, play games on it and attach all kinds of other apps to it. If you do this, it puts your privacy at risk! There are companies that scan these sites and collect data on you. They collect data on you from public records sites, social media sites and from sites that deliver malicious payloads to your devices. Keep private information private. Be careful what you share about missionaries online. Once you put somethiing on the internet, it will remain there pretty much forever somewhere, even if you think you erased it.

10 **Review your online accounts and credit report:** You should review your bank accounts, credit card accounts, and mobile phone accounts for signs of fraud or charges that you didn't make.

11 **Be aware of Stingray type devices:** There are devices that will spoof a cell tower and route your cell phone signal through them before connecting to a regular cell tower. They can capture all your activity.

Bonus Guidelines:

– Use discretion when answering questions via phone calls or face to face. People are very nice and clever about the way they ask questions of you. They ask deeper and deeper personal questions because people love to talk about themselves. Doing so puts you at risk of identity theft.

– Do not install an extension on your browser unless you know exactly what it does and you need it.

– Encrypt your device. Consider using secure, encrypted email like protonmail (https://protonmail.com).

– Understand that your cellphone gives your exact location and can be monitored unless you put it in a faraday case. It is possible to listen to your conversations through the microphone if your phone is close by, even if it is turned off! Even your camera can be used to watch you without your knowledge. There are many reputable companies where you can purchase these protective cases so that you cannot be tracked temporarily (https://mosequipment.com).

– Go to https://haveibeenpwned.com and put in your email address. It will tell you if your email has been compromised.

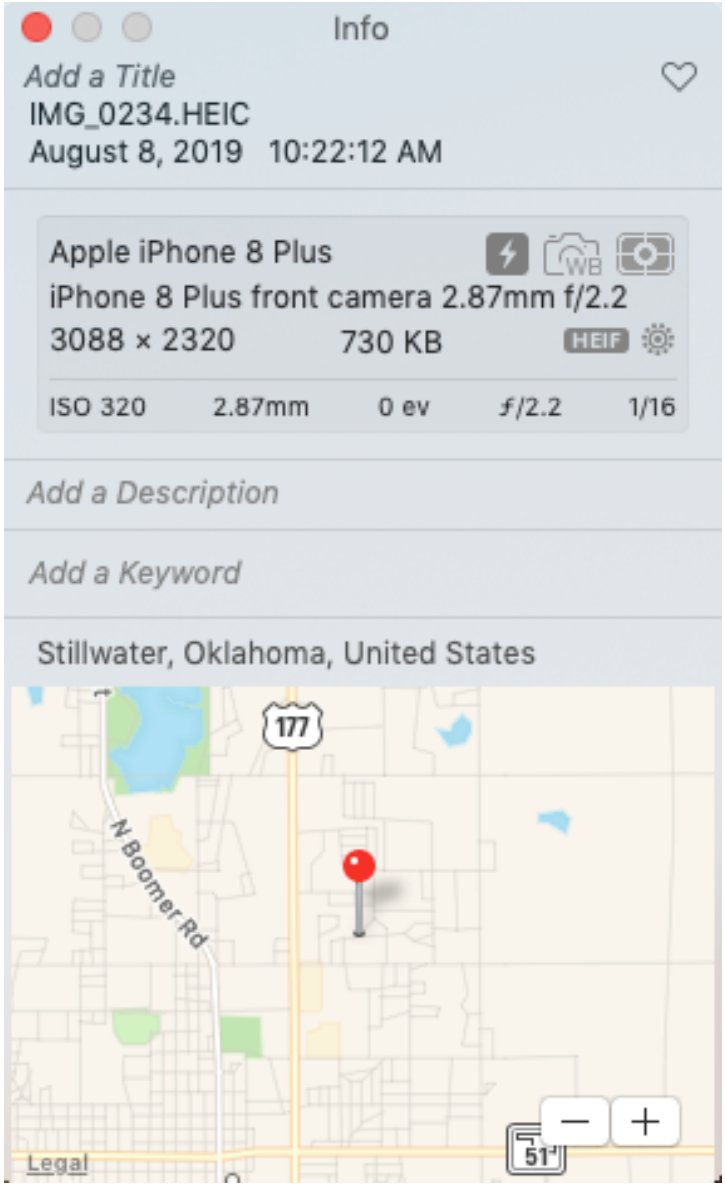
– Consider using a more secure OS, like TAILS or Qubes, for added security (https://tails.boum.org or https://www.qubes-os.org/)

I think I have pretty good  **security!**

But from a different view it does not look so good:

Hey, here we are in a secret place visiting our missionary friends.

(But I was not aware that the meta data on the picture says exactly where we are!)



PLEASE DO NOT CLICK ON THE LINK BELOW!

You are receiving this because you are on our list.
Click on the link to go to our secure portal:

Click here

[hover over the link for the answer]