Protecting your medical information is just one important step to assuring that you have a strong personal cybersecurity plan in place. No one wants to learn they are a victim of medical identify fraud. Here are a few tips to follow to help you keep your medical and personal information secure.

* Purchase and regularly run a credible anti-virus product on your PC, iPad, or laptop. This will assist in keeping malware off your system.
* Turn on automatic updates to maintain the latest software, operating and browser updates for your computer, iPad or laptop. Many of these updates will includes security features you need to avoid malware infections.
* Avoid clicking on link or opening any attachment in unsolicited emails or text messages. If you know the person check to make sure their spelling is correct and that it is really coming from them and not from a spam account. Spammers can look like someone you know but they often will misspell the name or be off by one letter. Opening these can infect your system.
* When sitting in the doctor’s office, a clinic or any public locations, avoid public Wi-Fi hotspots. Whenever possible, use your mobile phone’s personal hotspot. If you must use public Wi-Fi, use a Virtual Private Network (VPN) so you can protect your communications and information.
* Bring your own charging system wherever you go and use it. Avoid using any public form of charging cords or USB ports with your devices. These can deliver malware onto your phone or silently Don’t use publicly available charging cords or USB ports with your devices. These can be used to deliver malware onto your phone.
* Do not share any personal identifiable information over the phone, in a text or in an email. Remember, credible sources do not ask for this type of information in this manner. If you have a question about whether it is a credible source, contact them by phone. Do not use any links provided in a text or email. Call the medical office, consumer office, or bank using a secured and reliable number.
* Change your home Wi-Fi network router’s factory-default password and username and doing this as soon as it is installed will help keep you secure. Select a password that is not easily identifiable and one you do not use for other secured sites. Consider using the first letter of a phrase or sentence such as, “I love fried chicken and mashed potatoes for dinner.” Your password would then be, “ILFCAMPFD.”
* When downloading applications be cautious to not give permissions to them to have access to your location, contacts, photos, camera and data. This permission leaves you vulnerable and less secure.
* Use credible downloading sources such as Google or Apple and avoid any reliable sources because these can attach malware to your system.
* Be careful about what you share on social media. Avoid providing your location, sharing when you are on vacation, traveling or providing other private details. Even when you think you are only sharing to friends, once you hit post, your information is out there for anyone to see. There are no guarantees as to who will read your post.
* Purchase a shredder and use it daily or weekly to shred document, mail and all-important information. This will keep your information private and secured. Medical records, office visit summaries, insurance statements are included in documents that need to be shredded.
* Be cautious when keeping notes or documents on your phone to use only reliable back-up services. Often patients will place important medical information from a doctor visit on their phone in order to remember details and not have secure back-up in place.
* Review all your Explanation of Medical Benefits to make sure that the information on them is accurate and it applies to services and visits that you had. Assuring this information is accurate can help you avoid medical identify fraud.
* Keep your insurance cards in a safe place and when you hand them over to a medical office make sure they are returned before you leave the building.
* Ask your health care team if and how they may share your health information. Learning this information will help you know who might have access to your health records.
* Openly discuss with your health care team how you like to communicate with them. If you do not want to have text conversations or emails, then share this information and ask to be contacted only by the telephone. Ask who the individuals who could be contacting are so you will be prepared for their calls.
* If you decide to store any medical records on-line select passwords that you have never used before, ones that contain no specific sequence of letters or numbers and can’t be easily traced to your personal information. Again, consider a phrase or sentence that has only meaning to you and add numbers to it or characters to make it complex and not identifiable.
* Check your credit history once a year to see if you have any unpaid medical bills in your name and if they are not related to your medical treatment, make reports to all the credit bureaus and follow up with the medical centers.

Creating a cybersecurity plan for you and your loved one’s call be the first step in keeping your data and medical records secured. Take the time to make the necessary changes in your life to obtain security and peace of mind.

Diagram

Description automatically generated