STN computers www.stncomputers.com

Vonore, TN 37885 (865) 556-4714 1stncomputer@gmail.com

REDUCE YOUR DIGITAL FOOTPRINT-NOW!

Ideas to minimize your online footprint and safeguard your data from cyber thieves. Getting hacked is often our own fault. Limit the availability of your personal information. Only you can Protect yourself!

Credit Cards: Remove your credit card number/info from all of the websites that you have made purchases. Make sure when you purchase something the website does NOT save your credit card info. When you purchase something, you do NOT need to "create an account." Set up a PAYPAL account-many sites (not all) now accepts PayPal as a way to pay. PayPal does NOT share your credit card info with the seller. Do not use "auto-pay" from your credit card. Each website that has your credit card number is just one more server that can be hacked. The less servers that have your info, the better. Don't use payment type "apps" (Zell, Cash App, Google Pay, Venmo, Facebook Messenger, Stripe, Samsung/Apple Pay, etc).....again too much info in places that you don't need to be. Yes, this is more work for you to put your credit card number in for each purchase, or to pay by cash or check, but it can protect you from a potential MESS! If you get an email that there's a problem with your credit card-DO NOT respond or click on anything! Get your credit card out and call the number that is printed on the back of the card.

Social Media: Limit your social media accounts and what info you give them. For instance, go to your Facebook account and remove personal info that is not necessary…your location, your schooling, email address, workplace, hometown, etc. The less info you put out, the better. Do not accept friend requests from people you don't know. Stop signing up for accounts you don't need/may not use…TikTok, WhatsApp, Instagram, Twitter (X), LinkedIn, Snapchat, etc. …and if you don't use them, delete them. Avoid oversharing on any social media websites or on public forums. Do not share information that could be linked to you, like your home address, phone number, and date of birth.

Telephones: Get all of your financial info off of your cell phone. Clear the browsing/search history/cache/cookies from your phone, often. If the phone is lost, all of that info is available to the finder. A cell phone is not a computer. STOP answering calls that do not show up on caller ID. If it's someone you know, they will leave a message. If it's a scammer you can block the number and they didn't waste your time by answering it…and you didn't get scammed. To be extra safe, always dial the number on your utility bill, bank statement, health insurance card – or whatever the official source may be – instead of relying on the callback number left from an unidentified caller. Turn off the location setting on your phone, check with your cell provider to make sure the 911 location stays on. Uninstall apps that you don't need. Don't use public wi-fi.

Social Security Number: STOP giving it out. NO ONE needs your SSN including…and especially doctors/medical facilities. Make sure to get your SSN removed from all of your medical providers. Your health plan has an ID number, that is ALL they need. Medical facilities are the most often hacked….let the hackers have your medical info, but NOT your SSN.

Passwords: Do not use the same password for your accounts. Each account should have a unique password. Do not always capitalize the first letter. Passwords should be at least 12 characters utilizing multiple lower case & uppercase letters, numbers and symbols.

Computers: Stop signing into things that you don't need or want. Just because a site "requires" you to sign in, doesn't mean you have to do it! This includes Microsoft and Apple. If a pop-up comes up, red, and maybe screaming at you to call Windows or Microsoft NOW, it is a scam web page. **DO NOT CALL THE NUMBER POSTED!!!!!** Turn off your computer. First, there is no such company as Windows, it is an Operating System. Second, this is a pop-up web page that is embedded in the website you were on, at that time. 1) Shut the computer off or unplug it. 2) Wait a few minutes 3) Plug in or turn on the computer. 4) Run the Ccleaner it will remove that website (the pop-up) from the history in your browser. Stay away from the website you were on when this happened, there is obviously an issue on that site. Close old or unused email accounts. Create a new email account that does NOT include you name….this in itself, gives a hacker a great starting point into your life. Keep your computer programs and Operating System updated and make sure your privacy settings are set for YOUR privacy. Run your Ccleaner once per month.

Spam Emails:

Don't reply to them, use your email providers spam filter AND if you are using the PROGRAM Outlook, use the Outlook spam settings in addition to your email providers, report spam, UNSUBSCRIBE from legitimate email lists that you don't want anymore, and don't give out your email address on sites you just want to look at once.

These days, you cannot completely prevent personal information from ending up in the hands of the public or advertisers, but the above steps can reduce your exposure and thus reduce the availability of information to scammers, the amount of email spam and cold calls you get. They can also help protect you from identity theft, which can result in major emotional and financial difficulties. Protect Yourself!