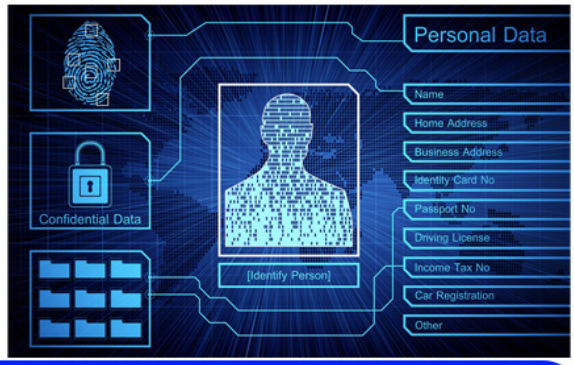
# FREE TIPS From a US Air Force Veteran To Protect Your Digital Privacy




abilityclinical.com 407-844-0859

All of these are suggestions, based on recommendations of military personnel, medical clients, C-level business professionals and Business Continuity experts. Ability Clinical, LLC makes no guarantees for any of these products.

EMAIL: For sending the most-secured-encrypted messages, get a FREE email account with ProtonMail (www.protonmail.com). Its servers are located in Switzerland in a practically nuclear-proof location. It encrypts the messages end-to-end between protonmail users. Be SURE to remember your password! Since it has the highest encryption, protonmail doesn't even have access to it to recover your account.

The Free account allows up to 150 emails/day and 500MB storage.
The $4/month version allows up to 1000 emails and 5GB storage. The pricing goes up from there. However the site is not for bulk email sending.

TEXT MESSENGING: SIGNAL www.Signal.org – Free SMS/Texting app that works like any other texting app, except that it encrypts messages between Signal users. It imports your contacts list from your current texting app, so you're ready to go. It's trusted by CEO's and other most concerned about the information they send.

SECURE WEB BROWSERS: Google watches everything you look for, everything you buy, everywhere you go and everyone you connect with, selling that information to the highest bidders. And they sell it globally!

We recommend Firefox (https://www.mozilla.org/en-US/firefox/new/) for your desktop computers.

For mobile devices, download the free DuckDuckGo app from the Apple or Android store.

For the highest encrypted privacy (which also causes slower performance), use TOR (https://www.torproject.org).

For a very family-oriented browsing experience (filters out violence, porn, etc), consider using SwissCows (www.swisscows.com). SwissCows is also heavily protected in the Swiss Alps. We especially recommend its use on public-use computers in your business as well as any computers used by children.

MICROSOFT WINDOWS – Shut off the automatic updates, since you'll never know if some "enhancement" is installed giving access to microphones and/or cameras. You might need to go into your "services" and disable the Windows Updates service. When in doubt, contact your IT professionals at Ability Clinical (https://abilityclinical.com)

AUTOMATED LISTENING-DEVICES (Amazon Dot's "Alexa", "Hey Google", etc) – They have ultra-sensitive microphones active 24/7 listening for your next command. Doesn't it surprise you that something you were "just talking about the other day..." mysteriously pops up on your browser? Unless you have 100% faith in them protecting your privacy, disconnect them. We gave up the convenience of speaking to turn on the stereo or get weather reports, to take back a lot of privacy.

FACEBOOK – As long as you're on FB, get F.B. Purity www.fbpurity.com and install the Facebook Purity add-in. It allows you to customize everything, including shutting off ads, games, stories, suggested connections, etc. as well as it notifies you whenever anyone unfriends you.

SOCIAL MEDIA – Although MeWe.com and Gab.com allow free speech for the moment, I don't have enough info yet to make a decision here.

We'll be researching safer alternatives to Twitter, Instgram, Tik-Tok and more, so stay tuned and stay safe! Sign up today for our newsletter and stay informed!

**Click Here to Subscribe to our Newsletter for the Latest, Breaking Technology News!**