Basic Computer Security

Besides the obvious use of antivirus scanners and malware removers, Preppers need to have other security features in place.

General Use:

Preppers need to communicate by email, just like everyone else. Unfortunately, using email is like walking through the woods dripping fluorescent orange paint from your back pocket - It leaves a highly visible trail all the way back to you.

Seriously consider the following information.
Obtain a generic, relatively unknown email mail provider. They are all over the web, do a search for ‘free email accounts’.
Avoid the bigger name ones like Gmail or Yahoo.
Ideally you want one that automatically deactivates your account if it is not used at least once in a few weeks. Hotmail used to do this, not sure if it still does, (and it’s a well known name besides), but there are plenty of others.

For maximum security, open the account in an avatar name, not giving any of your actual information. How to do this is covered in another discussion.

Do not link this account to your ‘standard’ email program for automatic retrieval. This means if you use Microsoft Outlook, or a similar email program, do not enable it to download your email from your new account.

This is inconvenient, I know, but since when has security been convenient?

The security comes from having to access the account from the web, and sending email from the web. Once it is downloaded to your desktop program, copies of emails are distributed throughout your computer, and are much harder to find and control.

Also avoid using email encryption programs. The general thought here is that watchdog agencies will assume you have something to hide if you do, and will concentrate their efforts on you. This goes against being ‘gray’, (a discussion elsewhere).

If emails must contain ‘sensitive’ information, utilize some code phrases or words rather than the words themselves. Remember, ALL email is run through scanners, looking for ‘trigger’ words. Not using these words is just common sense.
Your email should be as plain vanilla as possible, so it doesn’t stand out from any other.

Keep in mind, you cannot ‘mask’ an email by using an unusual or homemade font either, (or making letters ‘white-on-white’. The digital data is all converted to ASCII code, so the type of font is irrelevant.

Communication is safer in forums as well, which utilize their own ‘internal’ messaging systems, thus avoiding some net traffic. Usually the retention time of these messages is short also, so in a sense, they are ‘disposable.’

There are also internet chat rooms, set up with secure zones and instant erasures.
See https://project.crypto.cat
This provides a secure chat room for meetings and discussions. While not perfect, it is really very good. Used in conjunction with the other advice given here, it should be damn near bulletproof.

Also in the general use category – make sure your browser settings are maximized for security. The ideal case is to use a separate browser, for example MS Internet Explorer for normal use, but use JonDoFox or Tor equipped browsers for other uses.

Admittedly they are not convenient, but they are secure, take your pick.

Obviously in both cases, turn off ‘third party cookies’, Use ‘Do Not Track’, use ‘private’ browsing modes, and clear ‘history’ on closing.

In Microsoft Outlook, uncheck the following options:
“save forwarded messages”
“save copies of messages in Sent Items Folder”

Check and set the following option:
“empty Deleted Items folder upon exit”

Under “Archive options”
Check and set “Clean out items older than ___”, (the shorter the better)
Check “Archive or Delete old items”
Check “Permanently delete old items”

Notice while you are in there, Outlook stores emails in several places –
Current email (up to your archive date) goes to a file called “outlook.pst”
Archive material goes to a file called “archive.pst”

I suggest copying off your email on a regular schedule. You can copy these files on to a thumbdrive or a CD or DVD data disc. After the copy, erase the contents of both.

Make it a habit to regularly visit and delete all email from your web account as well.

Convenience comes into play here to. Do not allow Outlook, or any other email program to “automatically add names to the address book”. In fact, do not use the address book at all. This does two important things, it prevents your computer from spamming all of your contacts if malware does sneak in, and it protects your contacts.

Emergencies:

In the event of a major disaster, it is highly possible that along with weapons and food, computers will be collected as well.

If you travel, this is far more likely, numerous examples already abound, but it would be a logical step in a disaster as well.

With that in mind, keep all critical information on your computer in one place. I keep a folder on my desktop where everything of this nature goes. Periodically I burn off the contents on a CD.
Lately I have taken to using a thumbdrive which is encrypted. This is the best way to go for now.

As for internet sites, keep all bookmarks in one folder that could be seen as 'suspect'. In an emergency – delete this folder.

Here is the 'emergency' delete list –

Bookmarks or Favorite places – delete the one container folder
Find and delete - outlook.pst (if you use outlook) and archive.pst (know where to find these)
Delete cookies, history, and recent
Delete (uninstall) any encryption program on the computer
Empty recycle bin

THEN

Defragment the hard drive (this will cover over 'tracks' left by deletions)
Defragment the registry (this is fairly quick, use Tweak-now)

This all assumes you have some idea of whats coming, which, if you are reading this, now you do, so time should not be a constraint at this point.

Don't you wish there was a one button solution to all this?
There used to be.
It was called "DeCaf". This was supposed to be a joke, since the forensic tools the Feds used were by Microsoft, and called "COFFEE".
DeCaf used to be freely available, but since the writers of the program used some MicroSoft proprietary code, they had to withdraw the product, but not before thousands of people got the download.
To stop the program from working any longer, the authors had written in a "call home" feature when the program started. If the program called in and got no answer, it would simply shut down.
When the product was pulled, the "call home" number was deactivated, and the program would no longer work.
Fortunately computer people do not give up quite so easily, and there are reactivated versions on the market, as well as versions that use the original program and call home number, which can be easily fooled into calling your own computer instead.

If you proceed down this road, be warned.
This is not a program to play with.
It will erase virtually all areas of concern, as well as deactivate your flashdrive, your CD drive, and numerous other critical areas.
It will not kill your computer, but you will have a lot of restoring to do, from already backed up CD discs...
I have tested it, it was not fatal, but my computer required CPR for about 2 weeks.
It does what it is supposed to do though, and that’s what counts.

Well, those are the basics, and everyone should be aware of these issues and practice some form of “safe-text”, by doing so we protect not only ourselves, but each other.