Under the radar

In this age of increasing snooping on the generic activities of the populace there are a few things that can be done to minimize your profile.

I do not agree with those who believe that “if you have done nothing wrong, who cares if someone spies on you”.

Lately we have seen many examples of abuses of these powers among all agencies and it is clear they do not have our best interests at heart.

It is wrong to use information to “build a case” where there has been no suspicion of a criminal act, and this is the sole purpose of these spying and data retention programs.

We do have a Constitution that is supposed to prevent ‘case-building’.

I also do not agree that it is “too late to do much about it now”. I hear this all the time, and from people who really should know better.

I am pretty sure most of you have had the opportunity to deal with governmental agencies, whether Social Security, the local DMV, the Post Office, or other such groups. What do think of the divisions’ competence as a whole? I am not going after individuals here, let’s be clear. There are plenty of smart, capable people working in these areas, but as a whole, how effective are they?
How bureaucratic are they?

What I am getting at here, is that these organizations operate very inefficiently, lots of wasted motion, wasted paper, and poor management in general.

Why should organizations such as the NSA and the DHS and TSA be any different?
They are not.
Which is good. For us.

Like the DMV and the Post Office, information that these agencies rely on can become confused and irrelevant.
And all it takes is to feed them some confusing and irrelevant information.

That being said, what are specific actions you can take to muddle your information trail, since we acknowledge that it already exists.

Rule #1 – All email from any source, whether encrypted or not, is read, scored, and stored.

Mitigation –

Your email address – create a new one. Not just a made up one. A made up sounding legit one. You probably have gotten spam mail for Viagra pills or 'Russian women' , look at the email address. It is almost always a personal name. Let me check my spam folder right now –

Yup, sure enough. One from "Baruch D" (hot stock tips). Do you see my point yet? Don't just create some name, create an avatar.
Create an entire resume for your avatar – where they live, birthdates, married or not, spouse name, mothers name, password, everything. Write it all down and store it on paper where you will not lose it. Do NOT store it on your computer with the rest of your info.
That's just step one.
Now go to a search engine (not google),(I suggest Startpage or DuckDuckGo), and type in your avatars name. You will likely get a long list of results. Find where one of these names lives. This is not hard, Facebook users, LinkedIn users, and many other sites have hometown data for those names on file.
Even the whitepages.
Once you settle on one, adopt that as your new hometown. Go back and change the info on your avatar, school info, first job, etc.
Now you have a 'real' avatar, which if followed up superficially, will match up with a real person.

Next step, open an email account. This should be an account on a lower level site such as 'inbox.com' or some other relatively unknown free email. TIP – do not use Outlook to download email, if you need desktop accessibility, use Thunderbird.

Switch to using this email address for all sites you are registered with. If they hold home locations, change that also. Leave your current 'real' address active and continue using it, but now you have another address you can use as an alias.

I know encrypted mail can be broken as well, but just to make it more difficult, I use a 'hushmail' encrypted account (using the avatar of course). Thunderbird will encrypt mail as well. ‘Hushmail’ will automatically ‘burn’ messages that you have read, you can set the time delay. There are many other sites similar on the web. For live chat – see “cryptochat”. It has a burn feature as well, so nothing is left behind anywhere in storage.

Keep in mind – all of these messages and chats will still be recorded. The real question is will they bother to try to decrypt them if there is no reason to.

For a quick disposable email – consider “MaskMe”, which generates a fully usable email good for a very short duration. It can also generate a temporary phone number for you as well. These temporary addresses forward to your real account so you get the advantage of the address without the worry of where it will end up. This is an addon for Firefox.

Rule #2 – IP addresses are exactly like return addresses on mail, except harder to fake…

Okay, I will try not to make this technical, since it is VERY important to understand this concept. Your computer is assigned an address, just like your house number and street. Your Internet provider allows access to the internet from your computers address (IP) to its address (another IP) and then to whatever site you want to visit (the destination IP address).
Just like mail.
Your ‘return address’ is attached to every site you visit on the internet. The method of delivering the mail is also there (your providers address).

This is important, because if you change to your avatar, your computers address will not change. So even though you have ‘written’ a different name on your return address, the ‘street address’ (your IP) is still the same.

There are several programs that can ‘reroute’ this address, so that it actually appears to be coming from somewhere else. Some are fairly easy to use, some are more technical, (but better). Avoid being lazy, and learn how to use them.

TOR – stands for ‘the onion router’, and in German means ‘a gate’.

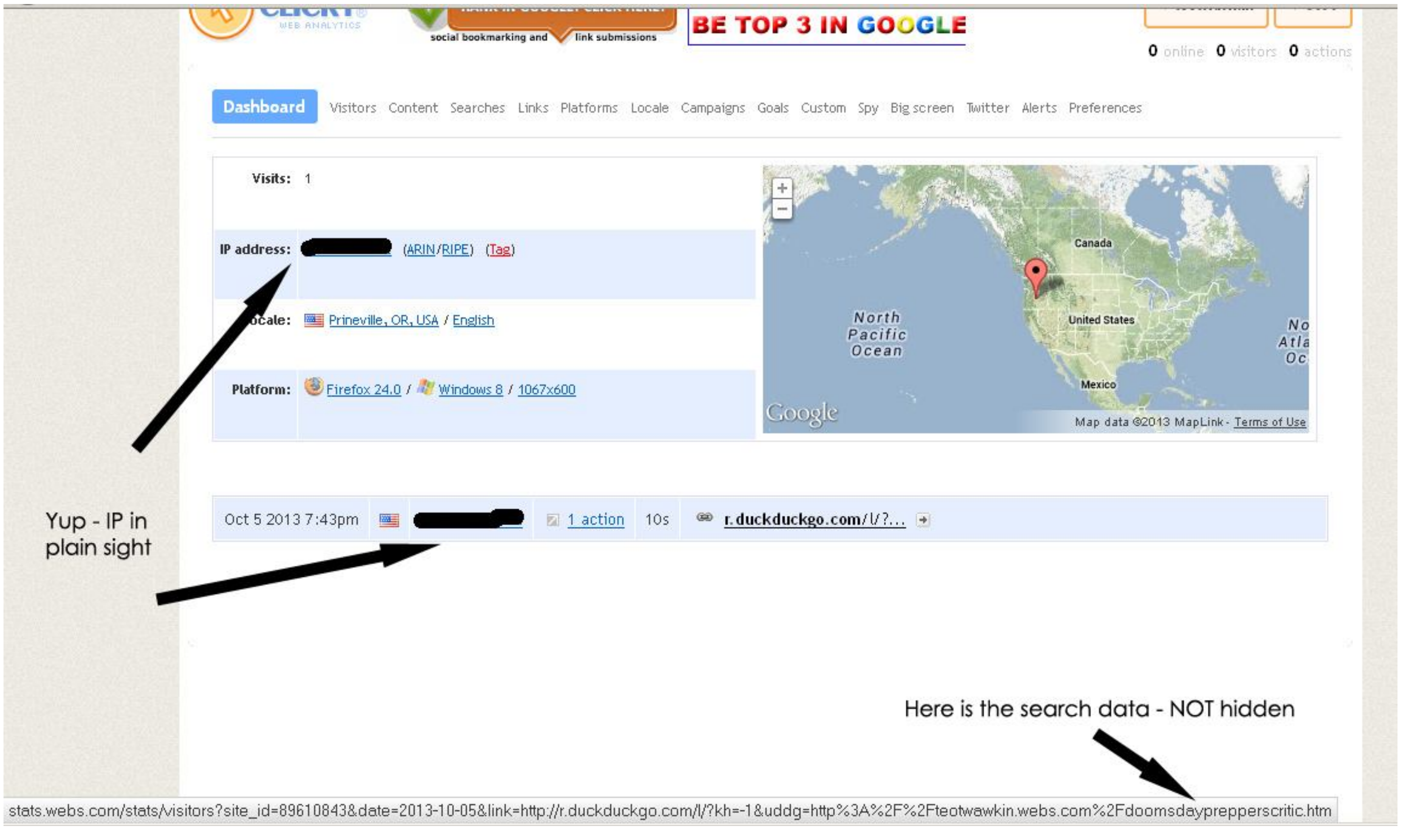
A ‘Gate’ describes it nicely. TOR takes your ‘mail’ (and that includes your site surfing requests) from your internet providers address, and then randomly ships parts of it around the world. The computers receiving it only know the address of the computer that sent it, and they only know the address of the computer it is sending it to. This way, after several jumps around the world, the tracking becomes extremely difficult, as one would have to go to each computer in the ‘jump’ to find out which was the next one back. Finally, after numerous jumps, it hits an “exit node” which makes the final connect to the website you wanted to visit. The process is repeated all the back in reverse, except that a new set of jumps occurs, with the ‘exit node’ finally contacting you again.

This doesn’t take as long as it sounds, but it does take noticeably longer than going directly to the site you want to see.
TOR can be turned off when you don’t require it, and that’s probably the way most people use it.

Other programs are similar.
JonDo Fox is a Firefox add-on that allows two intermediate jumps for the free version, and three jumps for the paid version. In the paid version, you can select the countries you want the jumps to occur in. I have used this, and while easier to use than TOR, it is not as fully featured. Like TOR, it can be turned off when not being used, and regular surfing can continue.

HotSpot Shield was another system using a Virtual Private Network to mask the original IP address, however this is also adware and can be quite annoying. It does work and it is free though. This program only allows one jump off point “exit node”, which you can choose in the paid version, but is preassigned in the free version. I ran into conflicts with this and my AVG scanner, so I no longer run this.

Search Engines – Both StartPage and DuckDuckGo use proxies to do your searching, and both do not retain any records, so these operate like a remote TOR connection for your search use, but IP records will show that you connected to these search engines, even if they don’t know where you went from there.
Note – On my website I have noticed that searches conducted with Duck-Duck-Go are fully visible, as well as your IP address, so this appears not to be secure.



Visits: 1

IP address: [redacted] (ARIN/RIPE) (Tag)

Locale: Prineville, OR, USA / English

Platform: Firefox 24.0 / Windows 8 / 1067x600

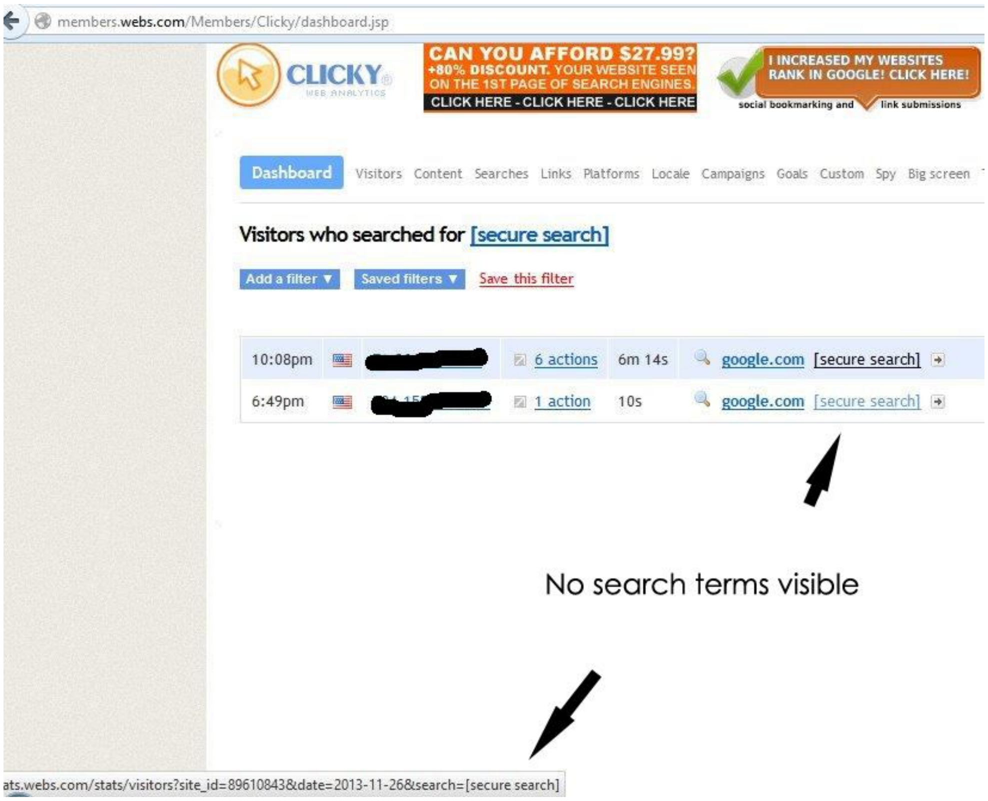
Oct 5 2013 7:43pm [redacted] 1 action 10s r.duckduckgo.com/l/?...

Yup - IP in plain sight

Here is the search data - NOT hidden

stats.webs.com/stats/visitors?site_id=89610843&date=2013-10-05&link=http://r.duckduckgo.com/l/?kh=-1&uddg=http%3A%2F%2Fteotwawkin.webs.com%2Fdoomsdayprepperscritic.htm

Even Googles' "secure search" appears to be better than Duck-Duck-Go in that no search terms can be seen -
(See below)


CLICKY
WEB ANALYTICS
CAN YOU AFFORD $27.99?
+80% DISCOUNT. YOUR WEBSITE SEEN ON THE 1ST PAGE OF SEARCH ENGINES.
CLICK HERE - CLICK HERE - CLICK HERE
I INCREASED MY WEBSITES RANK IN GOOGLE! CLICK HERE!
social bookmarking and link submissions
Dashboard
Visitors
Content
Searches
Links
Platforms
Locale
Campaigns
Goals
Custom
Spy
Big screen
Add a filter ▼
Saved filters ▼
Save this filter

members.webs.com/Members/Clicky/dashboard.jsp

Visitors who searched for [secure search]

```
10:08pm  [redacted]  6 actions  6m 14s  google.com  [secure search]
6:49pm   [redacted]  1 action   10s     google.com  [secure search]
```

No search terms visible

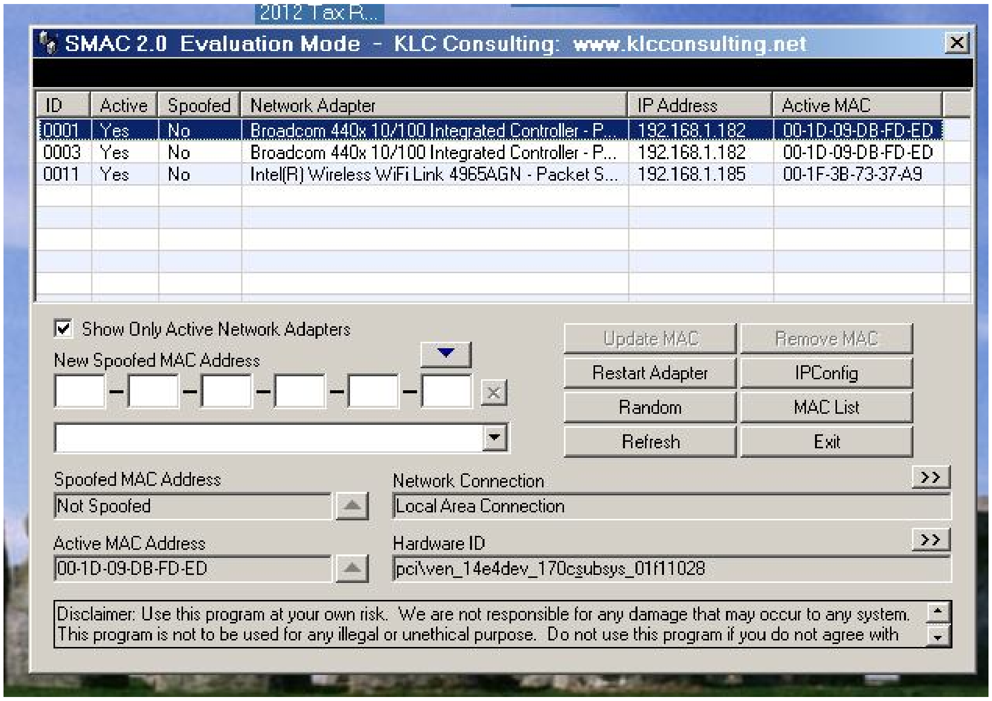
ats.webs.com/stats/visitors?site_id=89610843&date=2013-11-26&search=[secure search]

MAC Addresses

– Besides having an IP address, every device has a hard coded MAC address as well. This is because IP addresses can change, by changing providers, or you may have a 'dynamic' IP address, which just means it takes an available address when you connect from a list of available ones.

There is software that can alter your MAC address too, and if you are going to stay on line in this digital world, you must learn how to use these tools.

Example – This one is called "Smac", and it allows you to assign your own fake "called spoofed", MAC addresses to your equipment.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0001	Yes	No	Broadcom 440x 10/100 Integrated Controller - P...	192.168.1.182	00-1D-09-DB-FD-ED
0003	Yes	No	Broadcom 440x 10/100 Integrated Controller - P...	192.168.1.182	00-1D-09-DB-FD-ED
0011	Yes	No	Intel(R) Wireless WiFi Link 4965AGN - Packet S...	192.168.1.185	00-1F-3B-73-37-A9

☑ Show Only Active Network Adapters

New Spoofed MAC Address

Spoofed MAC Address: Not Spoofed

Network Connection: Local Area Connection

Active MAC Address: 00-1D-09-DB-FD-ED

Hardware ID: pci\ven_14e4dev_170csubsys_01f11028

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

RULE #3 - SEARCH ENGINES are data carnivores !

Some are worse than others, but by and large, figure all search engines, even those mentioned above, are insecure by nature.
On the other hand, the bigger ones are notoriously bad.

Avoid all use of the following:

Bing, Yahoo, Google, AltaVista, Cuil, Go, HotBot, All the web, live search, AOL search, Alexa, Bloglines, Blogperfect, Microsoft Sharepoint , Rollyo, and many others.

Almost every one of those mentioned above are owned by three entities, Google, Yahoo, or Microsoft.

If you must use a search engine, research it carefully, find out who owns it, and what it does with the search data. To get an idea of a ‘good’ policy, read the one on the StartPage site.

As a related item – “Google Earth” is another security risk. Never type in an address of where you are or where you want to look on any of these. It will never forget. Mapquest is not much better, but by nature you have to put in origins and destinations.

Rule #4 – Facebook knows all –

Don’t get me wrong, I am not advocating that you drop all your social media accounts, give up the cell phone, and hide in the woods.

What I am saying is that if the powers that be are looking at certain things, why not provide them those things, just not in your name or in a traceable way.

Facebook unfortunately is a major security risk by itself, but it can be minimized. If you follow these simple points, you can still be interactive on facebook without as much risk.

- Register with your avatar (this is the best solution, but is not that practical for people who have been on a long time).

- Never post, or allow someone else to post a picture of you. The national database for facial recognition is being conducted through Facebook. Do not become a part of it.

- Put very little personal information on the page, that which you do put on should be from your avatar.

- Delete all past posts containing your name, pictures of you, or political comments from the page and your history. (Note that Facebook does not delete them, just hides them from your timeline).

Linked In –

This is a different animal, no less dangerous, but it needs a different approach. Some of the concepts can carry over from Facebook though.

- Never post, or allow someone else to post a picture of you.
- Post only the information that is needed.
- Hide the visibility tag on any groups you join.
- Do not join any political or religious groups, keep it strictly professional.
- Avoid making connections with people in ‘areas of interest’, this may be the Mideast, China, Egypt, etc. This will automatically flag you as ‘communicating’ with possible terrorists.

Rule #5 – make cleanup a snap with a little planning !

Simple rules –

1. In your bookmarks section, create a folder named “Burn” – all ‘questionable’ (religious, political, etc) stored sites should be in here. A one button click can delete all, (followed by emptying the bin and a defrag...)

2. On your desktop, create a folder marked “XFER”. All critical docs , pics, etc should go in here. They can be easily erased in one shot, like above, or preferably burned off on some other media and buried. This should be done on a regular basis. To do this properly, use a file encryption program like “Truecrypt”, and encrypt a flashdrive. Burn off your data to here. Store the flashdrive in a hidden location. Get

another cheap, small flashdrive and encode it as well. Use it to store tax return data, scans of important papers, etc. and leave it close by. This is your ‘decoy’. It gives you reason to have encrypted the contents, and you can decrypt it if asked. Your ‘other’ drive uses another password and is safe.

3. Clean up Windows debris regularly. Use “Tweaknow” or something similar to vacuum cookies, erase history, temp files and downloads. Defrag the drive after all cleanup.

4. Set your browser setting to maximum security levels. TOR and JonDo Fox will do this for you automatically. If you are not using those, you will have to set the options yourself.

5. Regularly run an antivirus and a spybot program. Let’s just say if your computer gets hacked, and the hacker uses it to funnel a suspicious download through your machine, guess whose IP or MAC address Big Brother sees?
Yup – Yours.

So far, we have been talking about digital communications, mostly computer related, but there are other things as well.

Public information exists where you don’t really think about it.

Change your voter registration card. Sooner or later this will be critical, get a jump on it.
“Independent” is a good neutral choice.
Don’t take this advice too lightly, Libertarians are already listed as “Domestic terrorists” on the FBI’s VGTOF list. (Violent Gang and Terrorist Organization File).
So are “The Family Center”, Evangelical Churches, and Tea Party groups.
Forget the bumper stickers, and take a “non political” stance in public.

Watch out publicizing your religious views. Conservative Christian groups and Zionist Groups are already being targeted. Ease off on the bumper stickers and make your donations in cash.

Other groups and associations need to be watched as well.
Hunting Clubs as well as animal rights groups are both on the list.

Some other problem associations: Concealed carry permits, attending gun shows and sales, or taking part in a public demonstration of any kind. Also beware of online forums and meetup groups, never use any traceable information.

Be aware that driving on highways is fully monitored. EZ Pass systems track your vehicle at all major crossings, microwave radar scans passing vehicles from the side of the road, and paying for gas with that credit or debit card makes you easy to follow too.

Then there is your cell phone. We love to have the latest and greatest, but it comes at a terrible price. It was leaked in 2011 that these phones can be ‘turned on’ for full listening remotely. The cameras can also be activated remotely.
Up until now the only defense was to take the battery out, but to counter this, the newest phones do not allow access to the battery.
Needless to say, if it is GPS equipped, you are being tracked there as well. Even if it isn’t, triangulating the cell towers will pinpoint your location pretty well.

The new Windows 8 operating system contains a chip (TPM 2.0) which allows remote operation of the computer through a backdoor access. The government of Germany has released a memo to officials stressing not to use these machines.

The new Microsoft Xbox is equipped with infrared cameras and microphones, and blatantly advertises that it will target ads to you based on what it ***sees and hears***. (And people willingly buy this stuff!)

The information age has been co-opted under the guise of ‘convenience’, and it is the biggest data collector there is.

While it is almost impossible to hide your data, you can provide the other extreme, ‘too much confusing data’, and that is what we advocate here.

RULE # 6
SEARCH YOURSELF -

Preferably using a ‘safe’ search engine, conduct regular searches of yourself by name, email address, and physical address. You will be amazed at how much data is out there, and probably a bit weirded out too!
Some you may be able to fix, most you will not.
But it helps to know what is there.

Since Gmail saves all emails, I have been able to find emails by typing in a Gmail account. You should try this on yourself if you use Gmail. People cut and paste portions of emails that are received, and these become locked in stone. Reviews (like on Amazon, Edmunds, Yelp) are all available this way.
Craiglist complaints are a great source for these searches….

“Gmail member parkmo001 is a scam artist. He replies to postings on Craigslist, saying he is interested but does not have the time to come see the item, but he will send you a check or money order for the purchase, you call him after it is cashed, and then you send the "extra" money to a third person (a "shipper"). Then a month down the road the check is seen to be a fake, you are responsible for the money lost by the bank, and the people get away because they don't use real names. I do not know if these "shippers" actually pick up the items or not. If they do you are out of the item too.”

Never assume your emails will not show up on the net, regardless of what system you use.

So what can be done?

Never post your picture or pictures of relatives on any site on the web.

Never tag any picture.

Erase metadata which is stored on most pictures – this may include your location encoded in the data.
Use a program such as “Hidden Data Detector” or “Batch Purifier” to look at this data and erase it. Windows 8 has a “Properties” function which does the same thing.

Don’t forget to look at the properties of documents, pdfs, and spreadsheets, this data is there as well.

Use a proxy when surfing the web.

Use the most secure email you can find. Use more than one.

Use an Avatar - see www.fakenamegenerator.com for examples of where to start.

Compile a complex and realistic avatar – use this avatar to create email accounts.

Use a MAC address generator.

Burn off identifying information from your computer on an encrypted flashdrive. (Use Truecrypt for this.)

Search your personal data on the web and remove everything you can. Be aware of what you cannot remove.

Use good virus scanners that include rootkit detection.

Cover your computers’ internal camera unless it is needed.

Tighten all of your security and privacy settings on social media and other websites.

Remember, nothing is secure.
Even the thoughts inside your head will be monitored someday.