NORTHPORT SECURITY

## ELECTRONIC PRIVACY CHECKLIST

No one should live with the fear that they are being spied on. Based on our experiences and those of the clients we have helped, we've put together a list of things you can do to help protect yourself and your privacy.

The list is certainly not all-inclusive. If you have any proposed additions, deletions, or questions, please get in touch with **info@northportsecurity.com**.

While we suggest changing passwords, this list is not meant to address cyber/hacking threats, as that is not our area of expertise. Similarly, we do not do forensic examinations of computers or cellphones for malware, but we've included some suggestions for securing those devices.

### PHYSICAL SECURITY:

Protect yourself from physical harm first, and then secure your residence and vehicle to prevent someone from getting inside and installing eavesdropping devices. There is little value in having a bug sweep done if someone can get access to your home immediately afterward and install something.

- Change your door locks-including electronic locks that use a combination.
- Change the codes for your garage door openers.
- Change safe combinations
- Account for all vehicle keys
- Ask your dealership to confirm in writing that you are the only one authorized to have keys made.
- Restrict access to bank safety deposit boxes
- Consider installing cameras and alarm systems to monitor your residence while you are gone.

### PASSWORD CHANGES AND ONLINE RECOMMENDATIONS:

You should regularly change joint/known passwords to prevent spying and harassment. Avoid passwords that are easily guessed by someone who knows you. Listed below are accounts and devices that should be secured with new passwords and utilize two-factor authentication when possible.

**Financial**

- Bank accounts
- Credit cards
- Online shopping sites
- Utilities

**Email and social media**

- Be careful what you post and whom you accept as a friend
- Restrict sharing of locational data

**Cellphones**

- Lock code
- Apple ID
- Google Play
- Carrier account-Verizon, Sprint, ATT, etc.
- *Prevent SIM swapping-require a PIN
- from your carrier for account changes

**Laptops, Computers, iPads, etc.** - yours and your family members

- Cover camera lenses when not in use.
- Router and Wifi-make sure you have the latest firmware and use a password
- Security systems-Change your PIN and safe word
- Thermostats-Nest, Ecobee, etc. that are connected to the internet

**Security cameras**

- Including Wifi dash cams and vehicle cameras (e.g., Tesla)
- Baby Monitors

**Tracking Systems**

- Lojack, Onstar, etc.-prevent tracking or remote unlocking
- Child trackers - including via cellphone apps
- Pet trackers
- Fitness apps that post your location data

**Entertainment**

- Netflix, Amazon Prime, and other streaming services
- Devices such as Amazon Alexa, etc.

### INDICATORS THAT YOUR CELLPHONE IS SPYING ON YOU

A compromised cellphone is the ideal surveillance device as it can provide audio, video, GPS location, browsing history, text messages, and email messages. Your cellphone might have an issue if it is always hot and the battery drains quickly.

- Go into your phone settings to see what programs are using the battery
- There might be a hidden spy app

**FOR IPHONES:**

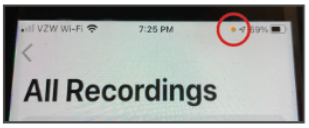
- An orange dot near the upper right corner indicates
- an app is using the microphone on your phone. **(ex. 1)**
- A green dot near the upper right corner indicates that the camera or the
- camera and microphone are being used by an app on your phone. **(ex. 2)**

**FOR ANDROIDS:**

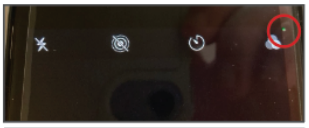
- Android phones show a camera or microphone at the top of the screen
- when they are active. **(ex. 3)**

You can also try a factory reset to remove malicious programs. You can have a forensic examiner check your phone, but it may be cheaper to buy a new one.

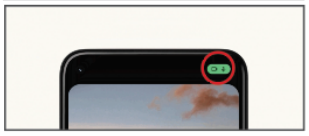
ex. 1




ex. 2



ex. 3



**VEHICLE TRACKERS:**

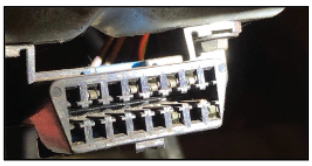
- These are cheap and widely available and are usually battery-powered.
- Check the bottom of your vehicle for a small black box that is magnetically attached and looks something like this.
- Waterproof enclosure with magnet on Left / GPS on the Right

*You can ask a mechanic at a dealership to check the underside of your vehicle while your oil is being changed and the car is on a lift.*

Check the OBD port (a black plug usually under the steering wheel) that looks like this (there are different variations). **(ex. 4)**

- See if there is anything plugged into it. Some widely available trackers plug into this port and receive power from the vehicle.

ex. 4



**Note:** Some insurance companies use trackers that plug into this port to monitor your driving habits in exchange for lower rates; however, they should be labeled with the insurance company name. Likewise, some lenders require that GPS trackers be installed on the vehicles of high-risk borrowers.

- Look under the seats, in door and seat pockets, under the dash, in wheel wells, the trunk, and any other place where it may be possible to hide something in your vehicle.
- Check for extra wires going to your fuse box or your battery. See your owner's manual for the location of your fuse box.

**AIRTAG TRACKERS:**

These cheap tracker devices sold by Apple are about the size of a quarter dollar but thicker. They rely on nearby iPhones to connect via Bluetooth and report their location. If you have an iPhone and an AirTag is accompanying you for an extended time, you will get a popup message that says, "Unknown Accessory Detected. This item has been moving with you for a while. The owner can see its location." Apple has released an Android app called Tracker Detect that will provide the same function for Android phones. You will have to open this app and run it periodically. It does not automatically scan.

To locate the Air Tag.

- Tap the alert on your phone, tap Play Sound, and listen for beeping.
- If the AirTag has been placed inside an enclosure, it may be difficult to hear.

If you find an AirTag, you can either remove the battery by twisting the two halves and pulling them apart or notify law enforcement to have them assist you in determining the owner.

For a complete explanation of what you can do if you find an Air Tag, see the following article from Apple: **https://support.apple.com/en-us/HT212227.**

**TILE TRACKERS:**


These trackers are similar to AirTags, in that they use Bluetooth to report their location, and they have also been used to stalk unsuspecting victims. They must be near a cellphone running the Tile app to work.

Tile has released apps for both Apple and Android phones, which allow you to see if there is a Tile nearby. The app, called Scan and Secure, must be manually started to scan for Tile devices and requires that you leave the suspect area before returning and running the app for at least 10 minutes to find out if there are devices nearby.

**HIDDEN CAMERAS:**

Cheap small cameras that can look like everyday household items are widely available. These are just some examples. If you search for “hidden cameras” or “nanny cameras” on Amazon or eBay, you will find many other ordinary-looking items with cameras hidden inside them. To find these cameras, look for items new to the area, including things plugged into outlets. Concentrate on rooms where your privacy is most important. Check heating vents, smoke detectors, bathroom vents, and clocks. Weatherproof cameras placed outside your residence can also be used to spy on you. Check trees for trail cams and look for large rocks near your exterior doors or driveway.

You may also encounter small wireless security cameras, such as those made by Arlo and Blink, hidden inside or outside the home. Unless the camera has a cellular connection, such as the Arlo Go, it will need to communicate with a box or “hub” inside the home, that is connected to your computer or router.

You can go to your phone’s settings and check wifi networks for unusual names to detect wifi cameras. You can also download a network scanning app such as Fing to see what devices are connected to your wifi network.

Try turning out the lights in a dark room and shining a flashlight to look for a reflection of the camera lens. Hidden camera detectors on the internet use flashing LEDs and a filtered viewer to make viewing lenses easier.

**A NOTE OF CAUTION:**

You may see relatively cheap devices on the internet called “Anti Spy Bug Detectors” or a similar name. These are strong signal detectors that detect radio signals. These can be effective in areas where there are no other radio signals other than the transmitter you are trying to find; however, we have seen many situations where persons have used these devices and found what appears to be a strong signal coming from inside their home, when in fact they are detecting wifi, cellphones, Bluetooth, or other innocuous signals in the vicinity. These are not professional detectors and will not identify the signal’s frequency to allow identification of the transmitter.

Furthermore, these devices are only capable of locating active wifi cameras which are emitting a signal. Many hidden cameras record directly to an SD card, and there is no wireless component that can be detected.

These detectors often cause alarm and result in a call to private investigators for a bug sweep. You may encounter investigators who use these cheap devices to conduct so-called “professional” bug sweeps. If you contact a professional, ensure they have the proper equipment and training to do a bug sweep, or you will just be throwing your money away.

We have also run into several situations where we have been asked to do a bug sweep after an ex indicates that they have planted a device in the house when they have not. Consider that this may be an attempt at a “mind game” to confuse you and cause paranoia.

**A NOTE TO OTHER SECURITY PROVIDERS:**

This list is a free resource and should not be used for financial gain. Please don’t try to resell or cut and paste it onto your site.

We have heard of many examples of private investigators and “bug sweep” providers taking advantage of persons going through highly stressful situations, such as a divorce, by exaggerating potential threats and offering over-priced and ineffective services. Please don’t be that person. Put integrity before making a quick buck.

We believe that suggestions such as those listed above should be provided to victims first so they can make an informed decision on whether they need professional assistance.

The latest version of this list can be found at www.northportsecurity.com. Please pass this along to anyone you know who you believe might find it of value.

Marty Vander Vliet
Northport Security