19 Clues Your Smartphone is Infected with Spyware and 15 Prevention Tips

by Kevin D. Murray, CPP, CISM, CFE, MPSC

Cell phones have secret lives.

When we are not using them, they chitchat with their masters at cell phone central, periodically transmitting messages like, "I'm here! I'm ready to accept a call."

They also download e-mail and news, adjust their transmitter power settings, and switch cell sites automatically. Depending upon the make, model, and type of apps loaded onto the phone, the phone may be handling other chores as well. In short, your phone transmits when you are not using it, and this is perfectly normal.

A number of other types of transmissions, however, are not normal. They may indicate that someone is receiving private information directly from your phone.

Many of the following clues have one thing in common: They indicate that your phone is transmitting when you are not using it.

19 Clues Your Phone is Bugged

1. Your phone's battery life suddenly decreases.
2. Your phone periodically lights up for no apparent reason.
3. Your phone is unusually warm when you are not using it.
4. Your phone bill shows a spike in SMS (short message service), text, or data usage.
5. Odd background noises or clicking can be heard during calls.
6. Friends often say your phone was busy or jumped straight to voice mail, when you know you were not using it.
7. Your phone beeps for no apparent reason.
8. Your Call Duration log shows entries that don't make sense to you.
9. Features of your phone that you didn't activate, such as call forwarding, are on.
10. Your phone frequently displays error messages such as "App Closed: Main" (or similar).
11. Your phone frequently displays "Message stuck in outbox" errors.

19 Clues Your Smartphone is Infected with Spyware and 15 Prevention Tips

by Kevin D. Murray, CPP, CISM, CFE, MPSC

12. Your phone is slow to respond to keypad entries.

13. "No SMS credit" messages appear on the screen.

14. Your phone is receiving odd text messages (example: <*#83><2125551212><d>).

15. The Web icon appears for no apparent reason.

16. You notice weird additions in your phone's Applications menu.

17. Your phone does not turn off as quickly as it once did.

18. Specific details of your calls are being mentioned to you by others.

19. Your phone shows frequent phone transmissions when you are not using your phone.

Detecting an increase in transmissions is the biggest clue that your cell phone is infected with spyware. The phone *must* transmit when it sends information back to the spy, such as: your texts, your e-mails, and data about who you called, when, and for how long.

The phone will also be transmitting when your spy has called your phone and has silently turned on the microphone and/or camera to covertly discover what you are doing.

Dealing with a spyware privacy invasion on your mobile communications device is a draining experience, both emotionally and time-wise. You don't want to go through this again.

Following a few simple rules will help prevent future spyware attacks. The following is also a good list to share with friends to help keep them safe.

15 Spyware Prevention Tips

1. **Do not jailbreak your phone's operating system software.** This is your first line of defense against spyware attacks.

2. **Do not let your new phone out of your possession.** It takes a snoop only minutes to activate spyware on your phone or pull your SIM card to read the information stored on it (contacts, etc.).

3. **Do not put a new SIM card into your old phone.** This will not solve the problem. Some spyware has the capability to detect new SIM cards and will report the new phone number to the spy immediately, thus continuing your privacy problems.

19 Clues Your Smartphone is Infected with Spyware and 15 Prevention Tips

by Kevin D. Murray, CPP, CISM, CFE, MPSC

4. **Do not sync a new device with the old device's contacts/apps backup file.** Syncing could bring your problem back to life. You may have backed up the spyware. Delete the backup. Start fresh.

5. **Use your mobile device's password feature.**

6. **Set your device to lock after the shortest *time of inactivity.***

7. **Use your SIM card's password PIN feature to prevent unauthorized access to stored information.** Here is how this security feature works: If your PIN is entered incorrectly three times, the SIM card is blocked. You can then unblock it only by entering a personal unblocking code (PUC) provided by the service operator. If the PUC is entered incorrectly ten times, your SIM card will be permanently blocked and you will have to buy a new SIM card.

8. **Do not store any confidential information on your mobile device that you cannot afford to lose.** Assume there is a possibility your phone will be stolen, lost, hacked, or infected with spyware.

9. **Never use any wireless device to access your bank and credit card accounts.** This includes your wireless laptop and iPad devices as well.

10. **Keep current on your software updates.** They frequently include security-related improvements.

11. **Download e-mail attachments only if you trust the source.** Your basic policy should be "Unknown? Leave it alone." Free ring tones, songs, and games fall into this category. Even if your source is a trusted friend, he or she may unknowingly be passing along spyware or other forms of malware. Ask yourself, "Do I really need this?"

12. **Never install pirated software on your cell phone.**

13. **Monitor the Usage Log built into your device.** Write down the usage at the beginning and end of the day. Keep an eye out for unexplained spikes in usage (both text and voice). This chore may be made easier with a utility usage app that logs and charts usage for you. Search your app store's Utility section using the search term "usage." Some apps will automatically notify you when a threshold limit is exceeded.

14. **Turn off your mobile devices when you are not using them.** It sounds simple, but surprisingly, most people leave their devices on. If you can remove the battery, do that too.

15. **Consider purchasing a second phone that no one else knows about.** Keep it hidden,

19 Clues Your Smartphone is Infected with Spyware and 15 Prevention Tips

by Kevin D. Murray, CPP, CISM, CFE, MPSC

and use it only for your most important calls. Remember to turn off the Caller ID function. Giving out a temporary number out can also keep your real phone number private.[1]

Bonus

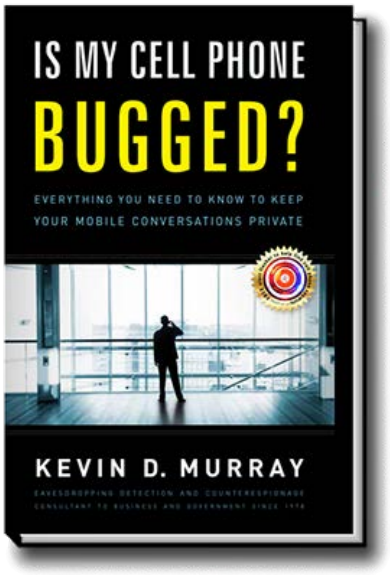
These security tips will also help protect you from the many non-spyware, but still harmful, mobile device viruses and Trojans out there.

Some are known for sending mass SMS texts and expensive MMS (multimedia) messages; manipulating your desktop; adding weird icons; or opening up your Contacts file for harvesting.

All this can dramatically drain your battery, your phone bill, and your patience!

Other viruses and Trojans are just malicious—they have no purpose other than to disrupt your life. Called "malware," these programs attack the phone's operating system and can shut the phone down completely.

For additional in-depth information on this topic, pick up a copy of, Is My Cell Phone Bugged - Everything you need to know to keep your mobile conversations private.[2]



Kevin D. Murray CPP, CISM, CFE, MPSC[3] is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[4] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

---

[1] https://www.burnerapp.com/

[2] https://amzn.to/36qvWon

[3] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/

[4] https://counterespionage.com