Are your devices spying on you?

Is it a surprise to anyone that the *CIA* has the capability to spy on people? Isn't that one of their main functions? Haven't we all seen *James Bond* movies? In every *Bond* movie, there is always a scene where James visits Q to get a tour of the latest gadgets, some of which included spy gadgets.

- "Electric shaver detector (*A View To A Kill*) - Contains an electronic eavesdropping detector. Once they arrive at Zorin's château, Tibbett uses this bug detector to scour the room. Eventually he finds a bug hidden within the lamp on the bedside table."

- "Bug and earpiece (*Casino Royale*) - Bond plants a bug in Le Chifré's benzedrine inhaler in order to eavesdrop on his conversations."

- "Tape-recorder camera (*From Russia with Love*) - A small reel-to-reel tape recorder disguised as a camera. Bond uses it to interrogate Tatiana and sends the tape back to MI6, where M and other officials play it back to listen to the technical specifications of the Lektor."

Anyway, back to reality. Unfortunately, the answer is yes, any gadget that has a microphone and/or a camera has the potential to spy on us.

- Computers
  - Almost all laptops have microphones and cameras built-in for making video calls with *Skype* and *FaceTime*.
  - Almost no desktop computers have microphones and cameras built-in. You have to attach them separately.
  - All-in-one computers have microphones and cameras built-in.

- Cell phones and tablets

    - All smartphones and most flip phones have microphones and cameras.
    - Almost all tablets have microphones and cameras.

- TVs
    - Very few TVs have microphones and cameras built-in (check your owner's manual).

- Vehicles
    - More and more new vehicles have entertainment systems that have microphones, and some have cameras.
    - *OnStar* has a microphone.

- Amazon Echo
    - It has a microphone and is constantly listening for commands.

- Google Home
    - It has a microphone and is constantly listening for commands.

- Baby monitors
    - They have microphones and maybe cameras to monitor your baby.

- Surveillance systems
    - Have video cameras and maybe microphones to record what is happening.

Is this a problem? Probably not. Just because a device has the potential does not mean that we are in immediate danger of being spied on. For one thing the *CIA* is not supposed to spy on American citizens inside the country. But of course, if the *CIA* has the tool you can bet the *FBI* has it also. For another thing, most of us would be extremely boring to spy on so who is going to do it? There is a certain amount of safety in obscurity.

But the problem is that once the capability is discovered and tools are developed, then criminals and other under world people could get their hands on them and use the capability for all sorts of nefarious purposes. Again, the likelihood is very small but the potential is there.

Is there anything we can do to prevent our devices from spying on us?

- "The bad news is that platform exploits are very powerful," Blaze tweeted. "The good news is that they have to target you in order to read your messages."

- Q: "I'm not a high-value target. But I still want to protect myself. How?"
  A: "It may sound boring, but it's vital: Keep all your operating systems
  patched and up-to-date, and don't click links or open email

attachments
unless you are sure they are safe."

- "There will always be exploits of which antivirus companies are not aware until it's too late. These are known as zero-day exploits because no patches are available and victims have zero time to prepare. The *CIA*, *National Security Agency* and plenty of other intelligence agencies purchase and develop them. But they don't come cheap. And most of us are hardly worth it."

So if you are worried about spying is there anything that you can do about it?Not really, but here are a few things that might help:

- Don't purchase the device in the first place. An *Amazon Echo* is a neat toy but the built-in microphone is always on listening for a command. Do you really need that new TV with a built-in microphone?

- Turn off the device when not in use or when you need some privacy. Better yet, unplug it.

- Cover the camera when you want some privacy. Many people cover the camera on their laptops all the time with a piece of paper or tape.

- Turn off your cellphone or tablet, or better yet, remove the battery if you can, when you must have privacy.

- Always update/upgrade your device when a software update or upgrade becomes available. Many times these updates include new features and security patches. (Note: If your computer is five years old or older be warned that an operating system upgrade may slow it down so much that you will be forced to buy a new computer. So when a computer gets to be older you have to balance the risk of security with the potential of slowing it down.)

- Always change the default password for configuring the device, if it has one.

- Use a VPN service. (See my January 2016 newsletter.)

- Don't click on links in email if you don't have to, and definitely don't if the email looks suspicious in any way, even if it looks like it came from someone you know. You never know if their computer was hacked.

- Don't open email attachments unless it is necessary. Even if the email looks like it came from someone you know if you aren't expecting an attachment it could be trouble.

- Be very careful and suspicious when searching the Internet. An

innocent *Google* search can turn into a nightmare if you don't pay attention to what you are clicking on.

- Don't be tricked into thinking there is anything wrong with your computer just because you see some random message of gloom and doom. They are all fake messages trying to trick you.

The reality is that the devices around us have had the ability to spy on us for a long time (see articles below dating back to 2003), but the likelihood that anyone is actually doing it is pretty small. But if you are at all concerned about it then by all means take some simple steps outlined above to keep your private life private.

- "Switching on the shower while you talk in the bathroom - a favored method of celluloid spies - is also unlikely to work, as constant volume noise can easily be filtered out. In fact, the only way to truly guarantee privacy, according to most security experts, is to take a walk in the park. Charles Shoebridge says: "It remains the case today as it has always been, that probably the best way to avoid being eavesdropped is to pass information during a long, unpredictable and unannounced walk in the big outdoors."

More information

NY Times - With WikiLeaks Claims of C.I.A. Hacking, How Vulnerable Is Your Smartphone?

cNet - WikiLeaks and the CIA's hacking secrets, explained

NY Times - In a Global Market for Hacking Talent, Argentines Stand Out

CBS News - WikiLeaks aftermath: Can you protect your phone or TV from spying?

cNet - Court to FBI: No spying on in-car computers (November 19, 2003)

BBC News - This goes no further... (March 2, 2004)

cNet - FBI taps cell phone mic as eavesdropping tool (December 4, 2006)

Wired - Hackers Remotely Kill a Jeep on the Highway-With Me in It (July 21, 2015)

Newsletter Archives

Click here to read some of my past newsletters.

Some of my clients do not realize that my business has expanded to all mobile devices. In fact, any consumer electronic product that you can purchase I can help you with. So if you would like help setting up or syncing your new smartphone or tablet or connecting your new WiFi TV to

the Internet, just let me know.

Claude Kerno
Computer & Consumer Electronics Consultant
719.650.9916
claude@kerno.biz - www.kerno.biz