LEXINGTON™
FINANCIAL/LIFE MANAGEMENT

Expert Tips: Protect Yourself from 'Stalkerware'

Add "stalkerware," a nasty form of spyware, to your list of worries in the digital age.

What is it? Often marketed as a tool to monitor potentially cheating spouses or partners, stalkerware essentially tracks individuals without their knowledge or permission. It can compromise data on mobile phones via keylogging and screenshots. Companies that make the creepy software design it to operate in stealth mode, in which the app is invisible in the victim's list of installed programs.

If there's any good news, it's this: Recent publicity around stalkerware has caused widespread outrage, causing a backlash that has, for example, prompted Google to pull ads.

What you can do

Actually, there is more good news regarding stalkerware; you can reduce your risk by following many of the same precautions that eliminate other forms of phone-centric malware. Here are tips from the pros:

- Look for unusual cellphone behavior, such as your battery dying more quickly than usual. This could indicate there's a spyware (including stalkerware) app running in the background without your knowledge.
- Scan your personal devices with a highly regarded tool such as MalwareBytes, Certo, NortonLifeLock, or Lookout.
- Check your phone's app settings to see if other devices have access to them.
- Change passwords and PINs often, and don't use the same password on multiple accounts.
- Wherever possible—and it's growing more and more common—enable twofactor authentication. This will prevent others from accessing your device even if they learn your password.
- Regularly update your apps and other software to ensure you've got the latest security patches.

LEXINGTON™
FINANCIAL/LIFE MANAGEMENT

Security FAQ: Killware

This up-and-coming cyber-menace is just as ugly as it sounds. To give you an early heads-up, here are answers to some common questions:

Q: With a name like that, it sounds terrible. What is killware?

A: Killware occurs when technology is weaponized to cause physical security incidents in critical national infrastructure targets that could lead to loss of life—targets like oil and gas manufacturing; other facets of the energy sector; water and chemical systems; and transportation, aviation, and dams. Unlike most cyber-incidents of the past, which caused loss of money and nuisance, killware gets its name because people could actually die.

Q: Are there any recent examples?

A: Not long ago, hackers nearly caused a Florida town's water treatment facility to distribute contaminated water to residents. That incident got the attention of officials nationwide. Additionally, a recent spike in ransomware targeted at hospitals is considered killware because patients have died as a result of crippled IT systems.

Q: Why is killware on the rise?

A: The Internet of Things is essentially the reason. The IoT has connected everyday devices such as refrigerators and doorbells to the global network, and industry has seen similar innovations. The Industrial IoT, or IIoT, opens all manner of devices to tampering.

Q: Who is committing killware attacks?

A: That is difficult to answer due to the nature of contemporary cyberattacks; often, nations hostile to the U.S. fund or approve hacks committed by private groups. So while national security officials will not come out and say that some killware attacks are carried out by nation-states, analysts believe this is the case.