Staying Safe Doesn’t Get Any Easier

Beware the “wares”.

Malware, or malicious software, is a term for computer software with malicious intent. And, remember, your smartphone is really a computer.

There are many well known and some less well known threats. There’s *Grayware*, *Hijackware*, *Crimeware* and probably some newly minted “wares” discovered since this article was written.

Grayware is software, and while not as malicious as some, that is still unwelcome. Think of it as the annoying relative of malware. It can track your browsing, bombard you with ads, and hog resources, but it won't steal your data or wreck your system. A component of this are "Potentially Unwanted Programs" (PUPs). Downloading free software is the most common way to get this nuisance. Included in this category is **Adware**. Yes, it’s just what it sounds like. The more of these unwanted ads you get, the slower your device will be.

Hijackware, also known as browser hijacking, is malicious software that specifically targets your web browser. It takes control of your browser's settings to control your browsing experience. Now you’re directed to what *they* want you to see, not what *you* want to see.

Crimeware is a term for malware designed to commit cybercrimes. Unlike Grayware that might cause annoyance, e.g. adware or viruses to disrupt systems, crimeware has a more sinister goal which is to steal something from you, like your money, your identity or your financial data.

How it Works: Crimeware comes in many forms. Some of the most common include:

- **Trojans:** Much like the mythical *Trojan Horse*, you invite the scammers in. Disguised as legitimate software, they trick users into installing their brand of malware, granting criminals unlimited access to your device.
- **Keyloggers:** These record every keystroke you type, capturing passwords and other sensitive information.
- **Spyware:** Steals data from your device and transmits it to the attacker.
- **Ransomware:** Encrypts your files, making them inaccessible, and demands a ransom payment for decryption.
- **Bots:** These turn your device into a server or host that is now controlled by criminals to launch large-scale attacks. You might even become part of an illicit crypto currency mining operation.

Targets: Crimeware can target individuals, businesses, and even critical infrastructure.

How to protect yourself?

- **Be cautious with downloads:** Only download software from trusted sources and pay close attention during the installation process to avoid accidentally installing unwanted programs. Inspect those “Check boxes”.
- **Beware of phishing scams:** Don't click on suspicious links or attachments in emails or texts, even if they appear to be from legitimate sources.
- **Keep your software updated:** Regularly update your operating system, web browser, and other software to benefit from the latest security patches.
- **Use strong passwords:** Implement complex and unique passwords for all your accounts, and consider using a password manager.

And, remember. **Don’t talk to strangers!**

Any comments, clarifications or questions should be directed to the author at jgf6217@gmail.com.
Written by Joe Fitzpatrick