GIBRALTAR REGULATORY AUTHORITY

Malware

What is Malware?

Malware – or malicious software, is an umbrella term for any kind of software designed to harm or exploit your devices or even your home or business network. Malware often invades, and/or disables computer systems by taking partial control of its operations and therefore having a negative impact on its function. Think of it as the same way the human flu interferes with the normal functioning of the body.

Malware is wide-ranging and its capabilities are quite extensive; it can crack weak passwords, lock up files, spam you with ads, and spread through networks. Malware attacks can lead to data theft and the destruction of entire computer systems. In most cases, cybercriminals use malware to extract personal data – therefore you are vulnerable to malware whenever you are online, and your vulnerability has a lot to do with the sites you visit, the links you click on, and the files you download, although it's still possible to get infected when taking the right precautions.

Does malware also affect mobile devices?

Any device with an internet connection can pick up malware, including your mobile phone or tablet. With the ever-increasing use of smartphones worldwide today, cyber attackers are poised to take advantage of this growing mobile market. Think about it: your phone is a highly sophisticated handheld personal computer that follows you everywhere; it holds troves of valuable and personal data; it's got a camera and a microphone that can record what you say, and a GPS that tracks your every move. Now imagine these capabilities in the wrong hands.

Most mobile users don't protect their phones as well as their computers; they don't install security software or update their operating systems, making their mobile devices easy targets. While iOS is a more malware resistant operating system than Android, Apple devices aren't impervious to threats. You can still infect your device by, say, downloading a questionable app.

8 Common types of malware

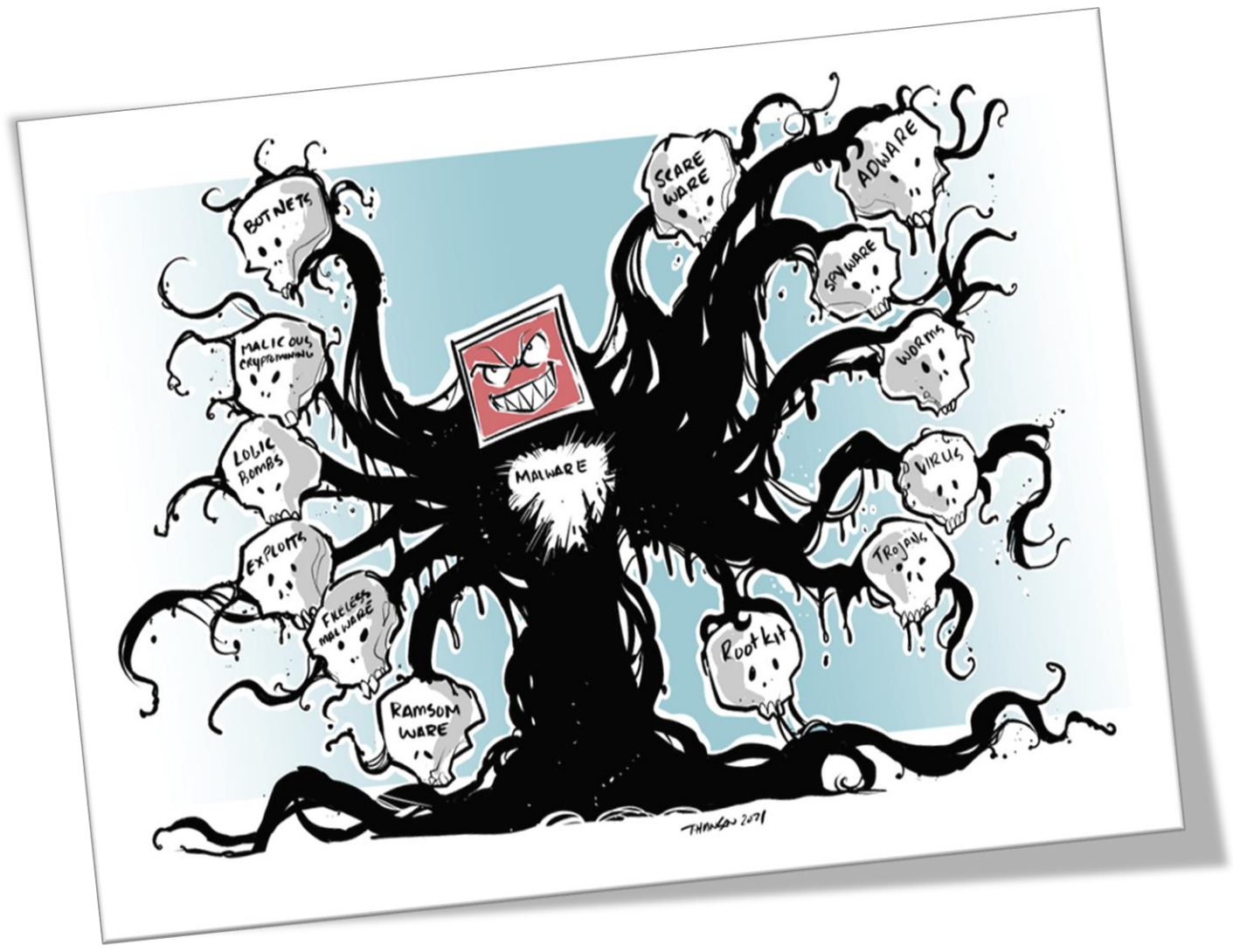
Different forms of malware impact computer systems differently, and some are easier to detect than others. Here are some of the most common types of malware that you should be aware of:

1) **Spyware** - runs in your system's background and observes your activity without your knowledge or permission. It then reports sensitive or personal data back to the spyware's author. Spyware can collect everything from your browsing history, usernames and passwords, location, and financial information. It certain cases it can even engage your camera and microphone, record your communications, and access your messages—more than enough to imitate your identity. The goal of spyware is to infiltrate your device, capture and send data, then remove itself, all while avoiding detection, meaning spyware is usually designed not to cause obvious system disruptions and other infection warning signs.

2) **Keyloggers** - are a specific form of spyware that hide on your device to record your keystrokes on the keyboard, which can reveal personal information, like login credentials, passwords, or credit card details, all of which is then sent back to the keylogger's author.

3) **Adware** – is designed to spam you with ads—usually pop ups within your web browser—to generate revenue for the attacker or to collect data on your activity. It's often installed in exchange for another service, like the right to use another program for free. Adware also gives other types of malware an easy way into your system; it can direct your browser to unsafe sites and contain other, more dangerous malware, like trojans or spyware.

4) **Viruses** - perhaps the most well-known form of malware, are designed to disrupt a computer system's operation. These usually come attached to a host file or program, commonly via email attachments. Once downloaded and opened—often inadvertently—the virus can spread uncontrollably, replicating itself by infecting other files and programs with its code. Computer viruses can damage your system's core functionality, as well as cause significant operational issues and data loss.



5) **Trojans** - are one of the most dangerous types of malware. A trojan masquerades as harmless, legitimate software, tricking you into downloading and opening it. Once installed, the trojan's authors gain unauthorised access to your device. They can modify, delete, or steal your personal data, including financial information, spy on your activities, crash your system, or install other forms of malware, usually ransomware.

6) **Ransomware** - is one of today's most pressing malware threats. It locks you out of your device and damages, encrypts or renders your sensitive files otherwise inaccessible, then demands a ransom and threatens to destroy your data unless you pay (usually in untraceable cryptocurrency). Ransomware attacks are profitable and hard to trace, making them cybercriminals' weapon of choice.

7) **Rootkits** - burrow deep into your device to provide the attacker with full administrative privileges on your infected system, known as 'root access' to your hard drive—i.e. the ability to control your personal computer.

8) **Scareware** - uses fake security alerts - a tactic known as social engineering—to trick you into thinking your device is infected, and to get you to download rogue apps, like scam security software, which tends to be additional malware.

Common signs of malware infection & how to tell if someone is spying on you

Malware is often designed to stay hidden, but that doesn't mean it's completely undetectable and can reveal itself in a variety of ways. If you notice your device working abnormally, it may be infected. The more of these common symptoms you observe, the more likely it is your device has malware. Here are a few signs to look for on your device:

1) **Poor system performance** - Malware can occupy a good deal of your device's processing power, causing its operation system to slow down. You may notice with considerable lags or delays when using apps, programs or when browsing the internet.

2) **Frequent crashes and freezing** - Malware can cause your device to freeze, crash, or encounter a fatal error. Some do this by consuming too much RAM or CPU power.

3) **Your device may be running hot** - A whirring fan in your computer is another indication that usage of your system's resources are abnormally high.

4) **Poorly functioning autocorrect** - A type of spyware called a keylogger, which records your keystrokes and interferes with autocorrect.

5) **Frequent pop-up ads** - The purpose of some malware, notably adware, is to inundate you with invasive ads, even when you're not using your web browser. Some redirect you to undesirable pages, others might pretend to be security software. These ads typically carry other malware threats—**don't click on them.**

6) **Deleted or corrupted files** - Types of malware that seek to damage your data or hold it for ransom might delete or corrupt your files.

7) **Loss of disk space** - Malware can hide in your hard drive and take up space, sometimes considerable amounts.