PREVENTION AND REMOVAL

Even though it is possible to clean an infected computer and completely remove malware from a system, the damage caused by some forms of malware, such as ransomware, cannot be undone. If a malware has encrypted your files and you have not backed them up, the damage has already happened. So your best defence is to prevent malware infections in the first place! And the biggest single factor in preventing malware infection on your PC is you. You don't need to be an expert. All you need is alertness to avoid downloading and installing something you don't understand or trust, no matter how tempting.

UPDATE YOUR SOFTWARE

Your best bet in securing your system against malware threats is to update it regularly. Don’t forget to do the same with your browsers, antivirus and anti-malware programs, firewall, and spam filters. Whenever prompted to download a security update for your phone or tablet, just do it without second thoughts.

SECURE YOUR HARDWARE

History remembers countless cases where companies’ or private users’ information has been stolen due to lack of security of electronic devices. Keeping your hardware protected will save you from a lot of trouble.

ENCRYPT YOUR DATA

It’s a good company practice to encrypt data as a security measure. This way, even if a breach occurs, a hacker would only gain access to a bunch of mumbo-jumbo they cannot decipher. Although encryption is a useful tool, remember that it only works if an unknown user tries to log in without the proper user credentials. So, make sure all company systems automatically log out after five to ten minutes of inactivity.

EDUCATE YOURSELF

Make sure all your employees are aware of and use good security practices, such as:

- ✓ Setting up unique and strong passwords.
- ✓ Staying alert for messages with poor grammar, as well as senders with numerous full stops in the email address.
- ✓ Always checking which URL they are being sent/directed to. For security measures, sensitive information should not beshared on websites that do not begin with “https”.
- ✓ Only downloading files from trusted sources.
- ✓ Confidential or sensitive data (mother’s maiden name, pet’s name, birthday, etc.) is kept away from social media,blogs or other places online.
- ✓ Excel macros should not be enabled unless necessary.

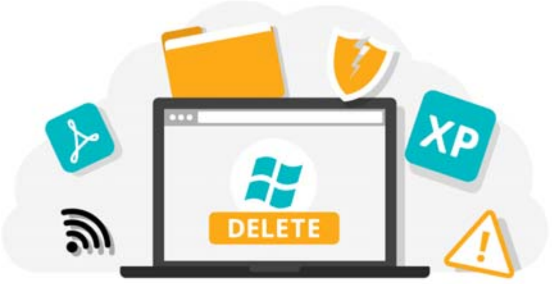
- Never pick up and plug in any devices that come from an unknown source. Always scan external drives prior to opening.

BACKUP YOUR DATA

Your data should never exist in just one copy. Make sure you back it up; daily, if possible. In addition to cloud storage, it’s a good idea to have a hardware copy of your files. The former can still be cracked, but the latter can be kept safe so you won’t have to pay a ransom if an attacker steals your files.

REMOVE SOFTWARE YOU DON’T USE

Keep your software up to date. If your system is outdated (such as Windows XP or Windows 7/8.1) and doesn’t offer security updates, it’s best to mark it redundant and invest in an upgrade. Otherwise, your security can be easily compromised. The same goes for old versions of programs such as Adobe Reader, multimedia players etc. If you don’t use them, remove them. If you do use them, upgrade to the latest available versions.



INSTALL ONLY FROM TRUSTED SOURCES

If you need a new app for your mobile device, use the Google Play Store for Android, or the Apple App Store (or F-droid, a FOSS app store for Android). Malware can easily be added into otherwise normal apps, and you will be none the wiser that your device is infected. When you download files or documents to any of your devices, make sure you trust the source. Otherwise, your system can be infected by a virus or other malware.

USE SECURITY SOFTWARE

Security software exists to keep you safe from cybercriminals. Your firewall, for instance, detects and blocks some of the known agents. Malwarebytes offers great multi-layer products that work to defend your system from sophisticated attacks from unknown sources. They also stop many malware and ransomware assaults in real time, continuously working to protect your vulnerable programs from breaches.

PRACTICE SAFE BROWSING

Whenever you’re online, there are certain policies you should keep for your own privacy and security.

- Strong passwords are a must. You can’t write them down or reuse them and have to change them often. Obviously, not everyone is keen on keeping that kind of information in their memory. If that’s true for you, use a password manager to keep your encrypted passwords in one place.
- Whenever you access the Web, make sure you’re on a secure connection (hint: look for the padlock icon in front of theURL.
- Websites that request login should begin with “https”.

COMMON SENSE

No means of protection will ever be enough for a user who fails to use their common sense. And the best tactic when it comes to malware is to make sure you never have to deal with it. So, stay skeptical of any new apps and odd downloads (until proven safe), and you will most likely escape potential disasters.