Have you ever wondered what’s all the hype about ransomware? You may have read it in the news or heard about it at your office. The truth is, that ransomware has gained popularity due to a gradual but steady increase in ransomware attacks over recent years. In the first quarter of the financial year of 2020, ransomware attacks were reported to increase tremendously due to the work-from-home culture resulting from COVID-19 pandemic. The reason behind it was the lack of remote work cybersecurity practices and policies for employees by the organizations. Hence, cybercriminals have been using this opportunity to exploit vulnerabilities in small and big businesses running remotely.

Let’s have a brief look at what is ransomware attack, how it works, and how it can be removed from an infected system.

**What is Ransomware?**

Ransomware is an advanced malware program that encrypts and locks the files of a victim’s computer system. Afterwards, the cyber attacker demands a ransom amount from the target to restore their access to the files after receiving payment.

The victim of the ransomware attack is given payment instructions to get the decryption key. Usually the payment has to be made in cryptocurrency, preferably bitcoin, since it’s not possible to trace the receiver.

Some types of ransomware attacks can even stop your entire computer system from working till the ransom is paid. It can affect both organizations and individuals alike, and cause serious financial damages to a business in addition to downtime and recovery costs.

**How Ransomware Works**

Ransomware can enter your computer in a number of ways, the most common of which is a phishing scam – an email posing as a person or organization you trust and asking you to download an attachment. Once the target opens and downloads the attachment, the attacker takes over their computer. Other sophisticated strains of ransomware such as [NotPetya](https://www.csoonline.com/article/3233210/ransomware/petya-and-notpetya-the-basics.html) exploit vulnerabilities in computer systems and infect without the need to trick a user.

There are many things ransomware can do once it infects a victim’s computer, but the most common action is to encrypt the user’s files. Once encrypted, it’s not possible for the files to be decrypted without a key known only to the attacker.

[In some instances](https://www.computerworld.com/article/2507340/security0/ransomware-squeezes-users-with-bogus-windows-activation-demand.html), the attackers pretend to be from law enforcement agency and claim to shut down the victim’s computer because of pornographic material or pirated software. They then demand the victim to pay a “fine” to make them less likely to file a report against the attack.

Another variation, called doxware or leakware, threatens publicizing the victim’s sensitive data. However, since finding this kind of information is not easy, encryption ransomware is still the most commonly preferred method by hackers.

**How to Protect Yourself from Ransomware**

Following are some of the defenses you can use to prevent yourself from potential ransomware infections. These are general security best practices, and following them can protect you against all cyber-attacks.

* Conduct regular penetration testing and vulnerability assessments to look for potential vulnerabilities in your system. Take help from [professional vulnerability assessment services](https://kmtech.com.au/book-a-cyber-assessment/) for detailed accurate results.
* Don’t install unknown software programs or give administrative privilege to any software unless you are sure of its authenticity
* Always update your operating system and install all latest patches to ensure least vulnerabilities in your system
* Install antivirus and whitelisting software to detect malware and prevent unauthorized apps from running in your system
* Keep an automatic backup of your files and perform the backup regularly. This step cannot stop ransomware attack but it can help you recover your data without paying huge ransom amounts
* Follow [best practices for keeping passwords](https://www.cyber.gov.au/acsc/view-all-content/advice/passwords-pins-and-passphrases) including strong passwords, keeping different password for every account, and preferably using a password management tool.
* Train your employees about safe online behavior such as using the web and email safely. Also teach them about phishing scams and why they should never click on links or download attachments received in email from unknown addresses, even if they seem very appealing
* Disable Macros in Microsoft office. Macros are useful for making simple MS Office tasks automatic but can also be used for malicious purposes
* Stay up to date about [latest threats](https://www.cyber.gov.au/node/1601)

**What to Do in Case of a Ransomware Attack?**

If your computer is already infected with ransomware and you don’t have a backup while also being locked out of your machine, here are some steps you can try taking to regain control of your system on windows 10 operating systems.

* Reboot your windows to safe mode
* Install antimalware program in your windows
* Scan your system to locate the ransomware
* Restore your machine to a previous date

While these steps will help you get back control of your machine and remove the ransomware, it will not help you decrypt the already encrypted files. The files have already become unreadable and the decryption key only lies with the attacker. In fact, you should take this step only if you plan on not paying the ransom to the attackers, since by removing the malware you exclude the probability of restoring your files.

**Some Facts and Figures about Ransomware**

Ransomware is a big market with a lot of money and started rapidly expanded since early 2010s. In year 2017 alone, ransomware attacks caused [$5 billion](https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/) losses to different businesses as a result of paid ransom amount and recovery costs. This was approximately 15 times more than 2015. Some industries, such as healthcare, are more prone to ransomware attacks since they have critical patient data to recover, and are more likely to pay the ransom amount. According to an estimate, about [85 percent of malware infections](https://enterprise.verizon.com/resources/reports/dbir/) in healthcare sector are ransomware attacks. Similarly, financial industry is another desirable target of cybercriminals, with an estimate of [90 percent of financial institutions](https://betanews.com/2018/05/22/financial-institutions-ransomware/) being a target of ransomware attacks in 2017.

One of the most noteworthy ransomware attacks affecting Australia in 2020 was Mailto attack in February, that affected a shipping and logistics company named Toll Group. The ransomware infected at least a thousand servers of Toll Group and forced them to take down their customer-facing apps.

**Maintaining a Good Cyber Hygiene**

The best approach towards maintaining a good cyber hygiene and preventing ransomware attacks is to have a proactive approach towards them. KMTech’s vulnerability assessment is designed to evaluate your organization’s vulnerability to potential ransomware attacks. [Book a free Cyber Security Vulnerability Assessment](Dionach’s%20ransomware%20readiness%20review%20is%20designed%20to%20assess%20your%20organization’s%20specific%20vulnerability%20to%20ransomware%20attacks.%20The%20review%20will%20determine%20the%20likelihood%20of%20an%20incident,%20the%20potential%20impact%20on%20your%20wider%20organization,%20and%20how%20quickly%20you%20could%20recover.) with us today to determine the likelihood of a ransomware incident, its potential impact on your organization, and how quickly you are likely to recover.