A decade-old form of malicious software known as ransomware has been making headlines after cybercriminals hijacked hundreds of thousands of computers worldwide.

Ransomware usually transmitted by email or web pop-ups, involves locking up people's data and threatening to destroy it if a ransom is not paid. More than 150 countries, including China, Japan, South Korea, Germany and Britain has been affected 200,000 Windows computers.

This cyber crime activities have generally targeted hospitals, academic institutions, blue-chip companies and businesses like movie theater chains. The attacks highlight the challenges that organizations face with consistently applying security safeguards on a large scale.

These 5 steps can help businesses and individuals to protect themselves from ransomware :

TIP 1 : Update your software

Security experts believe the malware called WannaCry, may have initially infected machines by getting people to download it through email. After that, the malicious code was able to easily travel to a wider network of computers that were linked together through the Windows file-sharing system.

The most disheartening revelation from the cyberattack was that there was a fix available for the ransomware before the attack. Microsoft, which makes Windows, released a patch for the WannaCry vulnerability eight weeks ago, said Chris Wysopal, the chief technology officer of Veracode, an application security company.

In other words, if people had simply stayed on top of security updates, their machines would not have been infected.

Consumers can remedy this by configuring their Windows machines to automatically install the latest software updates.

TIP 2 : Install antivirus software

An up-to-date antivirus software can prevent malware from infecting your computer. An expert, Mr. Kamden of NordVPN said 30% of popular antivirus systems were capable of detecting and neutralizing the ransomware.

Make sure to keep the antivirus app up-to-date, too, so it blocks the latest emerging malware. Also, download antivirus apps only from reputable vendors like Kaspersky Lab, Bitdefender or Malwarebytes.

TIP 3 : Be wary of suspicious emails and pop-ups

Security experts believe WannaCry malware may have initially infected machines via email attachments. To prevent your computer from the ransomware attack, avoid clicking links inside fishy emails.

How do you spot a fishy email? Carefully look at the sender's email address to see if it is coming from a legal address. Also, look for obvious typos and grammatical errors in the body. Check the hyperlinks (without clicking on them) inside emails to see whether the link direct you to suspicious web pages. If an email appears to have come from your bank, credit card company or internet service provider, keep in mind that they will never ask for sensitive information like your password or social security number.

In addition, ransomware developers often use pop-up windows that advertise software products that remove malware. Do not click on anything through these pop-ups, then safely close the windows.

TIP 4 : Create backups of your data

Whenever a hacker successfully hijacks your computer, you could rescue yourself with a backup of your data stored somewhere, like on a physical hard drive. In this way, if a hacker locked down your computer, you could simply erase all the data from the machine and restore it from the backup.

In other words, you should first create a copy of your data, in case your computer fails or is lost. After backing up your data onto an external drive, unplug the drive from the computer and put it in different location.

TIP 5 : Create a security plan for your business

For larger businesses with 100 or 1000 of employees, applying security updates organization wide can be difficult. If one staff's machine is not up to date to the latest security software, it can infect other machines across the company network.

An expert, Mr. Wysopal said businesses could learn from how WannaCry malware spread through the Windows file-sharing system by developing a strict schedule for when computers companywide should automatically install the latest software updates. Businesses should know and plan when is the best time to apply these security updates to office computers without interrupting productivity.

IT personel in your organization should also regularly educate and test employees on spotting suspicious emails.

What to do if already infected ??

If you are already a victim of ransomware, the first thing you can do is to disconnect your computer from the internet so it does not infect other machines. Then report the crime to law enforcement and seek help from a technology professional who specializes in data recovery to see what your options might be. There may be new security tools to unlock your files in the future.

With WannaCry malware, people definitely should not pay the ransom. That's because the hackers are apparently overloaded with requests from victims asking for their data to be released and many who have paid the ransom are not hearing back.