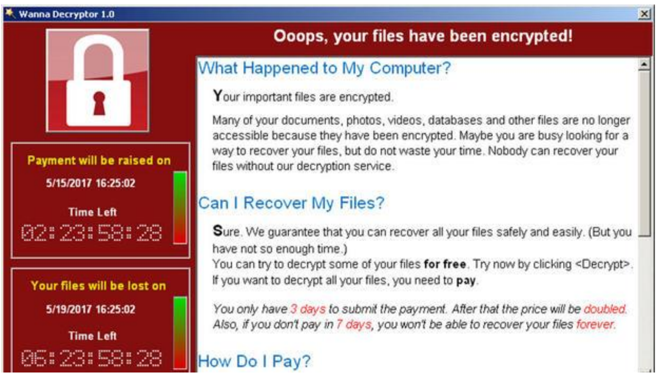
Ransomware

Ransomware is a type of malware that encrypts your files so you cannot read them. It then asks you for money to decrypt them. If you do not pay, they will remain unreadable forever or be deleted. Sometimes the infection will claim to be the work of law enforcement agencies, but this is always a lie designed to make it look more convincing.



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Figure 1: Ransomware Example

How Do You Get It?

Most victims are tricked into installing it. Sometimes it gets in by exploiting security holes in your web browser or operating system. Fortunately, such instances are rare.

How Can I Avoid It?

Delete emails from people, organisations or business that you have do not know or do not deal with immediately. Never open any attachments or follow any links contained in such messages under any circumstances, no matter how important the message claims it is that you do or how dire the consequences will be if you do not. If you get a message from a person, organisation or business you do know that contains an unexpected link or attachment, regard it with caution. Reply and ask them to confirm what it is and that they intended to send it. A very common tactic is to make a message from a business or organisation you are likely to have dealings with (such as a bank) and claim that some kind of problem has been detected with your account or something needs to be verified. No organisation or business will ever send such a message. Analysing the language of the message can help. Does it have spelling and grammar errors uncharacteristic of the sender? Does it just not "sound" like they normally would? Always be suspicious of advertising on websites. Never believe any ad that tries to tell you that your computer has problems or viruses. It is beyond the capability of websites to diagnose such issues. If you follow the link and install the app they say will fix the problem, it could turn out to be ransomware. If in doubt, call your local technician for help.

Keep your software up to date as many ransomware infections take advantage of security holes. If you see a message saying an update is available for an app you use, apply it. Updates sometimes cause problems, but this is rare. It is a small risk to take for keeping yourself protected. And finally, keep good up to date backups of your files. If you are not sure how to backup, ask for help.

What to Do If You Get Attacked

Do not pay the ransom. You have no guarantee that your files will be decrypted. Cut the power to your computer or device as soon as you see the message saying your files are locked. Desktop computers can be turned off at the wall. Laptops can be turned off by holding down the power button for several seconds until you hear the power cut out. For smartphones and tablets, hold the power button until you see the prompt to shut it down. You do not want your well intentioned automatic backup to copy the encrypted files over your good copies. Leave it turned off, disconnect your backup device (if any) and take it all to your local technician for assessment. Most likely, they will save your files if they can and then recommend the device be reformatted or reset. Having your device reset or reformatted will most likely be considerably cheaper than paying the ransom and will allow you to regain control.