What is Ransomware:

Ransomware is a malware that stealthily gets installed in your PC or mobile device and holds your files or operating system functions for ransom. It restricts you from using your PC or mobile device, and fromaccessing your files (files are sometimes locked or encrypted), unless you pay the ransom (in exchange for file decryption).

Paying the ransom (either through credit card or Bitcoins) however, does not guarantee that you'll get your files back. Prevention is still way better than allowing yourself to be infected and then trying to find a cure.

Type of Ransomware:

There are two types of ransomware – lockscreen ransomware and encryption ransomware.

Lockscreen ransomware shows a full-screen message that prevents you from accessing your PC or files. It says you have to pay money (a "ransom") to get access to your PC again.

Encryption ransomware changes your files so you can't open them. It does this by encrypting the files, These encrypted files are not decrypted because of the non-availability of decrypting keys and thus cannot be recovered to original form.

How it enters into the system:

Ransomware can get on your PC from nearly any source that any other malware (including viruses) can come from. This includes:

- Visiting unsafe, suspicious, or fake websites.
- Opening emails and email attachments from people you don't know, or that you weren't expecting.
- Clicking on malicious or bad links in emails, Facebook, Twitter, and other social media posts, instant messenger chats, like Skype.

It can be very difficult to restore your PC after a ransomware attack – especially if it's infected by encryption ransomware. That's why the best solution to ransomware is to be safe on the Internet and with emails and online chat.

Do's and Don'ts

Protecting endpoints against ransomware :

Do's

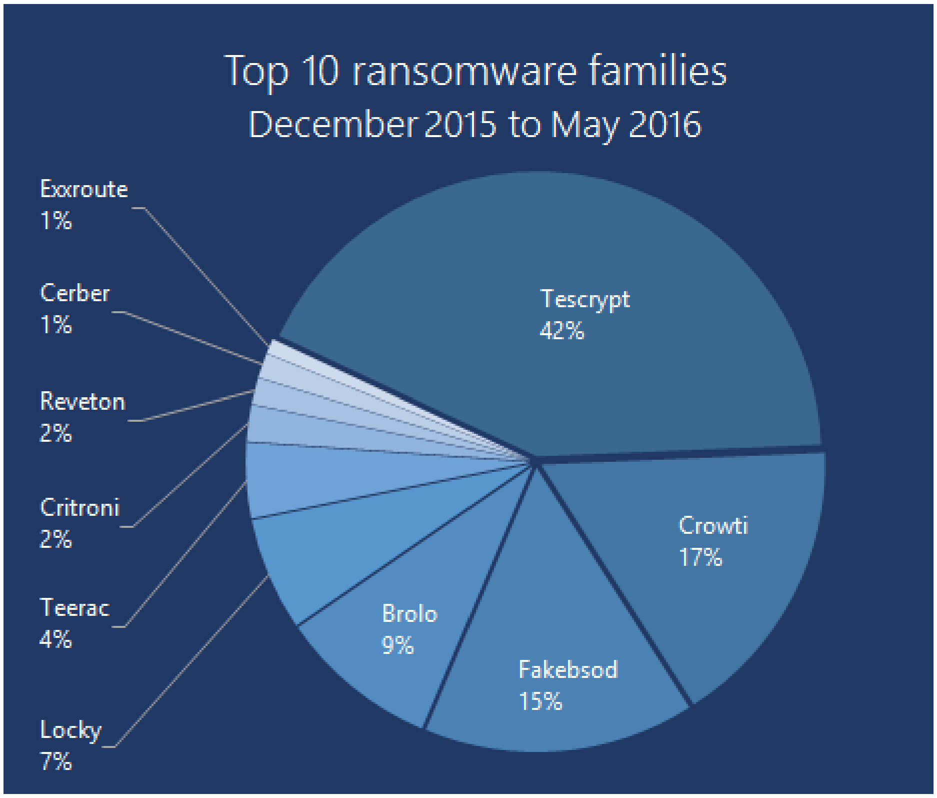
- Regularly backup your important files.
- Install and use an up-to-date antivirus solution.
- Make sure your software is up-to-date (OS,Database, Microsoft Office, 3rd Party software etc). Apply patches regularly when issued by the OEM's using windows AutoUpdate enabling on your system.
- Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
- Ensure you have smart screen (in Internet Explorer) turned on.

- Have a pop-up blocker running in your web browser.

Don’ts

- Don’t click on a link on a webpage, in an email, or in a chat message unless you absolutely trust the page or sender.
- Do not browse randomly results in drive-by-download attack.
- If you’re ever unsure – don’t click it!
- Often fake emails and web pages have bad spelling, or just look unusual. Look out for strange spellings of company names (like “PayePal” instead of “PayPal”) or unusual spaces, symbols, or punctuation (like “iTunesCustomer Service” instead of “iTunes Customer Service”).

Top 10 Ransomwares:



How to recover encrypted files without decrypting:

Here are some of the few that are applicable for a home user or those in the information industry like you:

1. Make sure you have backed-up your files.
2. Recover the files in your device. If you have previously turned **File History** on in Windows 10 and Windows 8.1 devices or System Protection in Windows 7 and Windows Vista devices, you can (in some cases) recover your local files and folders.

To restore your files or folders in Windows 10 and Windows 8.1:

- Swipe in from the right edge of the screen, tap **Search** (or if you're using a mouse, point to the upper-right corner of the screen, move the mouse pointer down, and then click Search). Enter "*restore your files*" in the search box, and then tap or click **Restore your files with File History**.
- Enter the name of file you're looking for in the search box, or use the left and right arrows to browse through different versions of your folders and files.
- Select what you want to restore to its original location, and then tap or click the **Restore** button. If you want to restore your files onto a different location than the original, press and hold, or right-click the **Restore** button, tap or click **Restore To**, and then choose a new location.

To restore your files in Windows 7 and Windows Vista

- Right-click the file or folder, and then click **Restore** previous versions. You'll see a list of available previous versions of the file or folder. The list will include files saved on a backup (if you're using Windows Backup to back up your files) as well as restore points. Note: To restore a previous version of a file or folder that's included in a library, right-click the file or folder in the location where it's saved, rather than in the library. For example, to restore a previous version of a picture that's included in the Pictures library but is stored in the **My Pictures** folder, right-click the **My Pictures** folder, and then click **Restore previous versions**. For more information about libraries, see Include folders in a library.
- Before restoring a previous version of a file or folder, select the previous version, and then click **Open** to view it to make sure it's the version you want. Note: You can't open or copy previous versions of files that were created by Windows Backup, but you can restore them.
- To restore a previous version, select the previous version, and then click **Restore**.

Warning: The file or folder will replace the current version on your computer, and the replacement cannot be undone. Note: If the **Restore** button isn’t available, you can’t restore a previous version of the file or folder to its original location. However, you might be able to open it or save it to a different location.

Important: Some ransomware will also encrypt or delete the backup versions and will not allow you to do the actions described before.