Here is a list of Do's and Don'ts which you should follow to keep your computer safe:

1. You need to immediately install the May Windows Update bundles. Microsoft has released a patch for Windows XP and other versions of windows.
Click bellow link to download patches
https://www.catalog.update.microsoft.com/Search.aspx?q=kb4012598

2. In order to prevent the infection, users and organisations should apply relevant patches to Windows systems as mentioned in the Microsoft Security Bulletin MS17-010. The malware has been targeting commonly used office file extensions such as .ppt (PowerPoint), .doc and .docx (Word), .xlsx (Excel), and image file extensions such as .tiff, .raw, among various other common file types for archiving, emails, databases, etc.

3. This attack type may evolve over time, so any additional defense-in-depth strategies will provide additional protections. (For example, to further protect against SMBv1 attacks, customers should consider blocking legacy protocols on their networks).

4. As part of the best practices to prevent ransomware attacks, users should maintain an updated antivirus software, regularly check for integrity of the information stored on databases, to not open attachments in unsolicited e-mails, restrict users' ability to install and run unwanted software applications, among various others.

5. Individuals or organisations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and law enforcement agencies.

6. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

7. CERT-In advisory: Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1. http://support.microsoft.com/en-us/help/2696547

8. Don’t open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organisation’s website directly through browser

9. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

10. USE THESE TOOLS:
1. Tool (NoMoreCry) to prevent Wannacry Ransomware by CCN-CERT:
2. Sophos: Hitman.Pro
3. Malwarebytes Anti-Ransomware(formally Crypto Monitor)
4. Trendmicro Ransomware Screen Unlocker tool
5. Microsoft Enhanced mitigation and experience toolkit(EMET)