1-) Security cautions could be increased to prevent the attack.

2-)More software updates needed to installed to prevent ransomware attack.

Computer users became victims of the WannaCry attack because they had not updated their Microsoft Windows operating system.

Had they updated their operating systems regularly, they would have benefited from the security patch that Microsoft released before the attack.

This patch removed the vulnerability that was exploited by EternalBlue to infect computers with WannaCry ransomware.

3-)Untrusted email attachments should not be opened

Avoid opening any email attachments unless you are sure they are safe. Do you know and trust the sender? Is it clear what the attachment is? Were you expecting to receive the attached file?

If the attachment asked you to enable macros to view it, stay well clear. Do not enable macros or open the attachment as this is a common way ransomware and other types of malware are spread.

4-)Do not download from untrusted websites

Downloading files from unknown sites increases the risk of downloading ransomware. Only download files from websites you trust.

5-)Avoid using unknown USBs

Do not insert USBs or other removal storage devices into your computer, if you do not know where they came from. They could be infected with ransomware.

6-)Update your internet security software

To ensure you receive the maximum protection your internet security has to offer (including all the latest patches) keep it updated.

7-)Backup your data

Be sure to back up your data regularly using an external hard drive or cloud storage. Should you become victimized by ransomware hackers, your data will be safe if it is backed up. Just remember to disconnect your external storage device from your computer once you've backed up your data.