What is ransomware?

Ransomware is a type of malware that infects your computer and prevents you from accessing files, at times it may even encrypt your files. There's no fool proof way to completely prevent any type of malware from infecting your computer.

Below, we outline some precautionary steps you can take to avoid ransomware from infecting your system:

- Always ensure your antivirus software is up-to-date. This provides another layer of security against many attacks.
- Backup important data. There are no known tools to decrypt files that have been encrypted by ransomware. One good safe computing practice to develop is to ensure that you regularly back up your files. The 3-2-1 principle is a good rule of thumb: have three copies, two different media, and one separate location for your backed up files. Windows has a feature called Volume Shadow Copy that allows you to restore files to their previous state, and this is enabled by default.
- Always verify the email sender. If you receive an email from someone claiming to be a bank representative, call the bank directly to verify that the message is legitimate. If you receive a suspicious email from a personal contact, contact that person directly to confirm that they sent you the message. Do not reply to the email you received. Do not reply solely on trust by virtue of relationships, as your friend or family member may be a victim of a cybercriminal as well. Avoid opening emails from an unknown source.
- Double-check the content of the message. There are obvious errors or discrepancies that you can spot in illegitimate emails. For example, if your bank or a friend claims that they have received something from you that you don't remember sending, try to go to your recently sent items to double-check if you really did send the items they are referencing. There are lots of tactics that spammers and phishers use to lure you, so take some time to learn about the different types of techniques that social engineers use.
- Refrain from clicking links in email. In general, clicking on links in email should be avoided. It is safer to visit any site mentioned in email directly. If you have to click on a link in email, make sure your browser uses web reputation to check the link, or use free services such as Trend Micro Site Safety Center (https://global safety.trendmicro.com/).