KAZMAREK
TECHNOLOGY SOLUTIONS, Inc.
www.kazmarek.com

Basic Security Practices

1.) Back up your data.
The importance of a reliable data backup is imperative. There are a number of factors to consider but your backup system should support file revisions as well as offsite data storage.

2.) Run effective Antivirus software.
All computers should be protected by an up to date antivirus client.

3.) Do not open attached files via email.
Many viruses will attempt to convince you that a file attachment containing the virus is something you really want to read.

> ******Do not click on links within emails you were not expecting. For example: FedEx package, BBB complaint, domain expiring, etc.***

4.) Use a spam filtering service.
More than 80% of the email traffic on a daily basis is unwanted Spam email. A spam filtering service can prevent the vast majority of spam email making it to your inbox and can be particularly helpful in preventing the spread of viruses via infected attachments.

5.) Additional software solutions. These can include web content filtering, Firewall security services and software restriction policies put in place on your network. Limiting your exposure to security threats is the key and there are many options available in the type layered approach that KTS recommends to our clients.

For any more information on safeguards please feel free to contact our team direct by
emailing support@kazmarek.com or calling (858) 952 - 5400.