Basic Email Security

Office365 uses a sophisticated AntiSpam engine to help keep users safe and inboxes from dangerous viruses. However, due to regular spam outbreaks, some unwanted or dangerous messages may potentially get through to your inbox or be diverted to your Junk Mail folder, so please use caution.

Here are a few good reminders about email:

- Messages that do not include an attachment are generally safe to open, even if you do not know the sender.
- If the message does include an attachment be very suspicious of it especially if the text of the message is in any way peculiar (poor grammar or spelling, odd subject matter). If it is uncharacteristically peculiar do not open it until you have verified that it is safe.
- If the message is from a known and trusted person but the text or subject matter does not resemble his or her usual patterns be very suspicious, especially if the message includes an attachment.
- Common sense rules! If the email is from an unknown sender with an attachment, don’t open it.
- Avoid phishing attacks. Phishing scams are designed to steal users’ personal information. They often use doctored and fraudulent e-mail messages and websites to trick recipients into divulging private information, such as credit card numbers, account usernames, passwords, and even social security numbers.

If you happen to receive a message that appear to be spam or if you receive an alert that you’re sending infected emails, close the message immediately and delete.