If you receive an email that you suspect is SPAM please do the following:

1. **NEVER open attachments or click on links** that you think are suspicious as this could be malicious and cause further issues
2. Screenshot it and send to Nemsys as suspicious SPAM (**DO NOT forward a suspicious email**) (see directions on how to use snipping tool)
3. Block the sender and mark as Junk or Phishing
4. Delete it permanently



**What are the key signs of a phishing email?**

* An unfamiliar greeting.
* Grammar errors and misspelled words.
* Email addresses and domain names that don't match
* Unusual content or request – these often involve a transfer of funds or requests for login credentials.
* Urgency – ACT NOW, IMMEDIATE ACTION REQUIRED.

**IF YOU'RE EVER IN DOUBT..... SEND IT TO NEMSYS and they can verify if it's legit or not. 🙂**