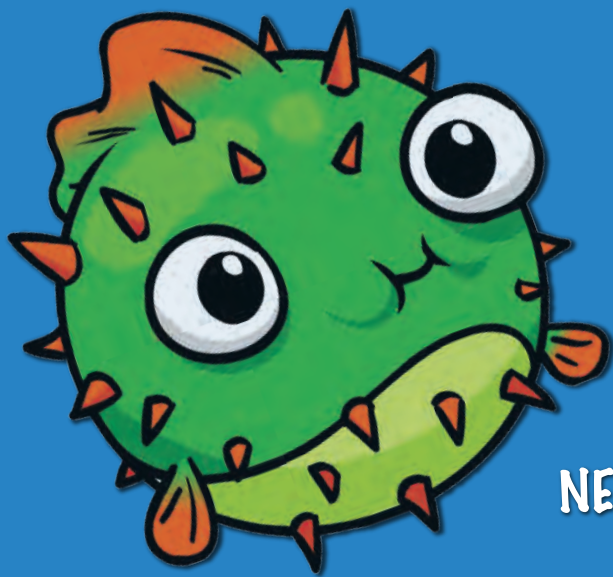


LOOK FOR THAT HOOK!

Signs that an email might actually be a
phishing scam



Is someone asking you to click on a link and log in with your password? Real banks and retailers would NEVER ask you to provide private information through an email!

Is there a lot of bad grammar? Maybe some misspelled words?

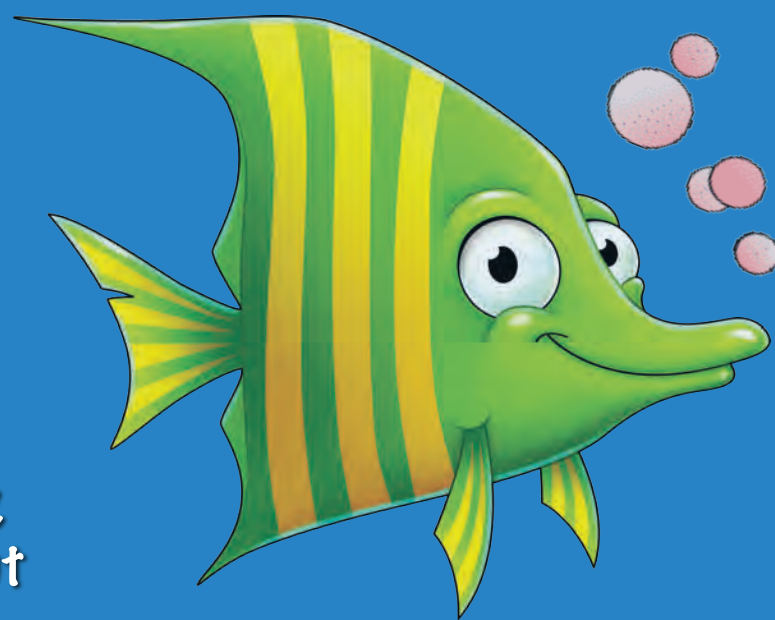
These are very common signs that the sender isn't who you think it is.

Does the domain name in the sender's address or any links not match up?

If the message claims to be from Amazon, but the From: address doesn't have "amazon.com" in it, it's probably a phishing scam!

Are you being asked to send money?




Whether the message is from a (supposed) retailer, bank, friend, family or even your boss, verify by some other method (pick up that phone!) that the request is legitimate.



Is the message trying to appeal to your emotions? Cyber criminals often use urgency, fear or even greed to get you to respond without thinking.



What to do:

-  **DON'T** Reply!
-  **DON'T** click on any links!
-  **DO** delete the message - and contact your IT department right away if you actually did reply or click on a link that took you somewhere unexpected!