Phishing scam detection flowchart

# Apply these steps to some sample emails

1. **Start**
2. **Check sender's email address**
   * If the sender's email address does not match the official domain, go to Step 3.
   * If the sender's email address matches the official domain, go to Step 4.
3. **Identify as phishing scam**
   * Flag the email as a phishing scam.
   * End.
4. **Check for email spoofing (a way of deceiving the recipient into believing that the email is from a legitimate sender)**
   * If there are signs of email spoofing, go to Step 3.
   * If there are no signs of email spoofing, go to Step 5.
5. **Check for grammar and spelling errors**
   * If there are grammar or spelling errors, go to Step 3.
   * If there are no grammar or spelling errors, go to Step 6.
6. **Check for urgency and threats**
   * If the email contains urgent requests or threats, go to Step 3.
   * If the email does not contain urgent requests or threats, go to Step 7.
7. **Identify as legitimate email**
   * Flag the email as a legitimate email.
   * End.
8. **End**