Identifying Phishing Emails

A few tips to help identify phishing emails:

1. The message is sent from a public email domain (A couple of public domain examples: @gmail.com, @yahoo.com)
No legitimate organization will send emails from an address that ends '@gmail.com'.

2. The domain name is misspelled
Another clue hidden in domain names that provide a strong indication of phishing scams is misspelling of the domain name – and it unfortunately complicates our previous clue. The problem is that anyone can buy a domain name from a registrar. Although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that's being spoofed.

3. The email is poorly written
You can often tell if an email is a scam if it contains poor spelling and grammar.

4. It includes suspicious attachments or links
Phishing emails come in many forms. But no matter how phishing emails are delivered, they all contain a payload. This will either be an infected attachment that you're asked to download or a link to a bogus website. The purpose of these payloads is to capture sensitive information, such as login credentials, credit card details, and phone numbers and account numbers or to download malware.

5. The message creates a sense of urgency
Scammers know that most of us procrastinate. When we receive an email giving us important news we need to act upon, most will decide to deal with it later. But the longer you think about something, the more likely you are to notice things that don't seem right. Scammers what to present the urgency to do it now before you have time to think.