# How To Spot Legitimate Emails from Fake Ones: Protecting Your Computer Against Cyber Attacks

In this presentation, we're going to help you determine what an email should look like when it's legitimate versus one that is fake. Of course, a cybercriminal's favorite vector is none other than an email message that looks legitimate to the untrained eye. But if you look closely, you will notice some subtle red flags that people may not even notice.

So, with this in mind, we are going to discuss how you can spot a legitimate email and what to look out for when there's a fake one right in front of you. So, here we go.

## The Risks of Phishing Emails

So, to kick things off, let's talk about phishing emails. These are deceptive messages that cybercriminals put together. They pose as a legitimate source, so for example, it could be Amazon, Apple, or any recognizable brand that you might have done business with. The goal here is for them to steal credentials like your login name, password, credit card number, or any data that is linked to you personally.

Keep in mind that these phishing emails can lead to identity theft and financial loss, and, of course, your computer may be infected with malware. This can escalate quickly, so you need to know the difference between a legitimate email and one that is fake.

## Characteristics of Legitimate Emails

Now, let's take a look at how you can determine whether or not an email is legitimate. You'll have to look out for the following characteristics:

* **Clear sender information:** First, you want to make sure that the sender information is clear. It matches the company's domain name, and it is from a known and trusted source. So, if it's from Amazon, look for Amazon.com as the domain.
* **Proper grammar and spelling:** All legitimate emails should be professionally written, which means grammar and spelling need to be correct.
* **Professional tone and appearance:** The email must be professional in tone and appearance.
* **Secure links and attachments:** A legitimate email will rarely, if ever, ask you to click on any links or download attachments. Avoid clicking on any suspicious links or downloading any unexpected attachments.

## Identifying Signs of Fake Emails

So, now that you know the legitimate characteristics, let's go into the signs of a fake email. Here’s what to look for:

* **Suspicious sender information:** Check the sender information and look for the email address. For example, in Amazon, the "O" might be replaced with a zero instead of the letter "O," or a clever cybercriminal might replace a lowercase "a" in Amazon with a Cyrillic lowercase "a." Remember, Cyrillic and lowercase "a"s have subtle differences but look similar.
* **Language that is urgent and threatening:** Legitimate organizations would never send a threatening or urgent message. Fake emails may use urgency to pressure you into taking immediate action. This is where verifying the message with the company in question comes into play.
* **Unexpected attachments or links:** As mentioned before, avoid unexpected attachments and links. This includes anything that requests your login credentials or any sensitive information such as your bank account number, credit card number, and so on.
* **Requests for personal information:** A legitimate company will rarely, if ever, ask for sensitive information via email. Ignore such emails.

## Final Thoughts

This will conclude the presentation. Before we finish up, let's remind you to always be on the lookout for any of these signs to determine if an email is legitimate or fake. Check the sender's information, read through the email to spot any grammatical or spelling errors, ignore any attachments or links, and never give out any personal information unless you are verified to do so. Thank you for taking part in this presentation today. Take care.