Phishing Emails: What are phishing emails and how can you spot them?

What is a Phishing Email?

Cybercriminals send what we call ‘Phishing emails’ to pose as someone else in an attempt to gain access to personal data. People sending phishing emails will often present themselves as established organisations to try and immediately gain trust from the recipient and make them think that the email is legitimate. The end goal being to lead the recipient to unsafe websites, to take personal data or attack users’ machines with malware.

How to Spot a Phishing Email

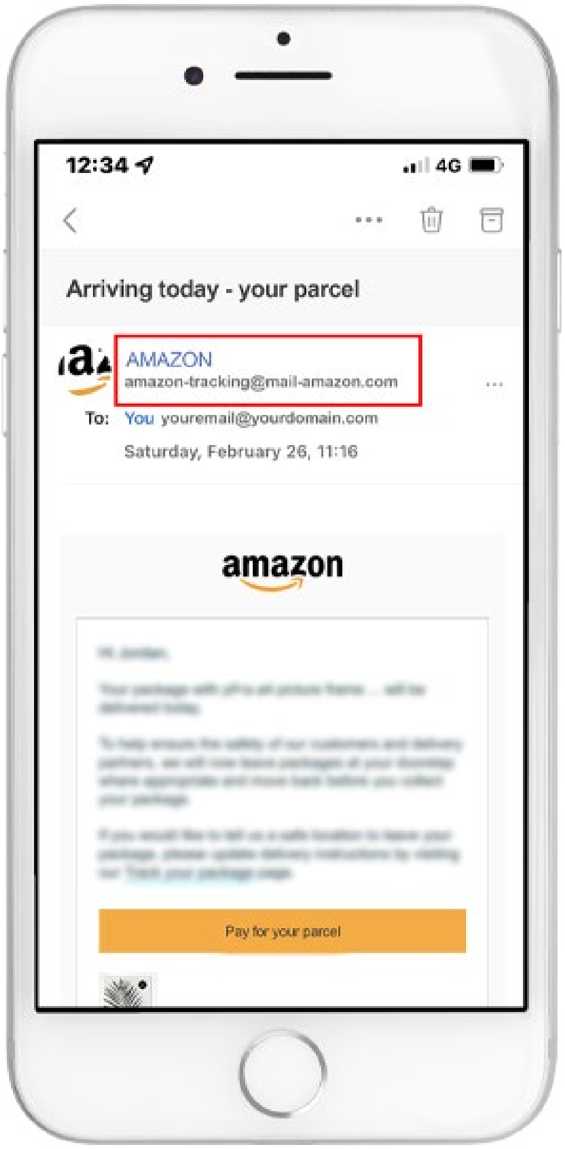
Phishing has become a common method for cybercriminals to target individuals and businesses. Why? Because its an easy, low technical way of trying to scam people but can yield great results for the criminal. Here are some useful tips on how you can spot a phishing email and avoid being caught out by cybercriminals.

Unrecognised Sender Address

Any user who owns an email address can change their display name to almost whatever they want. So when an email comes through that may look like its from a genuine business, or even someone you know personally, the display name alone cannot be trusted to suggest that the email is from that person.

In this example, you can see that the display name is being shown as 'AMAZON', but the email address alongside is amazon-tracking@mail-amazon.com, which is a tell-tale sign that it is a phishing attempt. Looking out for legitimate domain email addresses is key in spotting a phishing attempt, for example an email from LinkedIn will be from an email address such as example@linkedin.com, but a phishing attempt could have an email address such as example@mail.linked-in.com.

To make it easier for end-users, Office 365 have the Outlook with Defender product which will automatically highlight these unrecognised sender addresses.



Arriving today - your parcel

AMAZON
amazon-tracking@mail-amazon.com

To: You youremail@yourdomain.com

Saturday, February 26, 11:16

[illegible]

Requesting Sensitive Information

Over 75% of organisations around the world experienced a form of phishing attack in 2020 with 60% of them losing data as a result.

Legitimate companies will never ask you without warning to send over sensitive information such as bank details or passwords through an email, and as a rule of thumb, many banks now make it clear from the outset that they do not communicate with their customers through email.

If you receive an email that looks legitimate but were not expecting to be asked for sensitive data, it should still be treated with the same level of caution as an obvious phishing email.

Insecure Links and Attachments

Another popular method that cybercriminals opt for is directing users to unsafe websites using a phishing email.

Similarly, to the sender address domains, its usually easy to tell if this link is illegitimate. For example, if a cybercriminal posing as The Royal Mail telling you that you must pay for your parcel to be delivered, but they're directing you to a link that is not at the domain of royalmail.com. This is a big red flag and a sign that the email is an attempt to gain information or take payment from a user. Additionally, the link shown in the email can mask what the real website is, however, by hovering over the link it will allow you to see the real website.

Incorrect Grammar

Companies that send genuine emails will take the time to ensure their emails are grammatically correct. As many phishing emails come from foreign cybercriminals, its often evident from the amount of spelling and grammar issues that the email is not from a legitimate person or company. In some instances, bad spelling and grammar is evident deliberately as it can highlight easy targets if end-users do not pick up on it.

What to do with phishing emails?

There are some simple baseline rules to follow when you receive a phishing email.

1. **Do not click on any links**. In some cases, clicking on an unsafe link can lead to having malware downloaded onto your machine to cause chaos on individual devices.
2. **Do not reply**. Even if you're on the fence about an email and think it could be legitimate, replying to a potential phishing email could end up giving the attackers more leverage to work with other methods of cybercrime.
3. **Report the email**. Find out how you can report phishing emails to the National Cyber Security Centre here.
4. **Block the sender.** By blocking the sender, they will not be able to send you more emails from the same domain.
5. **Do not open attachments.** Similarly, to web links, this can lead to malicious malware making its way onto your device to do damage.
6. **Secure your device with Anti-Virus.** This is very important, and we recommend that all devices have some form of Anti-Virus to ensure that extra level of protection against malware.
7. **Share Knowledge and information.** If you have found out something new surrounding the protection against phishing emails, we advise to share with your colleagues. The more people within your company that are cyber-aware, the less chance there is of your company being a victim of cyber-crime.

Vinters