Tips for Spotting Phishing Emails

Make sure the sender information and the email address match. You would generally expect the sender email address to have the name of the sending organization in it. In this example you might expect the email to be notice@usps.com.

Check the legitimacy of the company

It is often the case that phishing emails will be sent from what appears to be a legitimate entity. However, there are often mistakes that reveal this is not the case. In these examples, the name of the company is spelled incorrectly. A quick internet search reveals these types of mistakes.

Check the email salutation and closing

In phishing emails, the salutation and closing of emails is often absent or not appropriate.

Generally, directed emails like this example would be addressed to a specific individual rather than a generic greeting like ‘Hi there!’

The closing of a legitimate email would generally have information about the sending company, a means to make contact, or to unsubscribe from future emails.
Tips for Spotting Phishing Emails

Check for spelling / grammar errors

Phishing emails often contain spelling and grammar errors. It would be very unusual to see mistakes in a legitimate email. If you notice these types of errors, you should definitely proceed with caution.

Be aware when there is an urgent call to action

Beware when an email contains an urgent call to action. Phishing email will try to get you to act quickly so that you don’t have time to think before acting.

Hover over the links in emails

It is always good practice to hover over the links in emails. Hovering over the link will show you where you will be redirected when you click it. This practice often reveals fraudulent links.
Tips for Spotting Phishing Emails

Look for information in the email that doesn’t make sense

Think about whether the email even makes sense. In this example, you are instructed to go to the nearest post office to get your parcel. If this were genuine, it would specify which post office has your package.

There is a good chance that if something doesn’t quite make sense, that the email is a phishing scam.

Is the information in the email body / subject vague?

Using vague information is another sign of a phishing email. In this example, you would expect the subject to contain specific information about the webinar. Again, in the body you might expect more specific information. In addition, the subject and body of the email suggest that you registered for a webinar. If this is the case, you should compare the details of the email to the webinar you did register for.

Look for inconsistencies in the formatting of the email

In addition to the spelling and grammar errors highlighted earlier, phishing emails often have formatting errors in terms of inconsistent use of fonts and font sizes.
Tips for Spotting Phishing Emails

Consider all of the factors

It is unlikely that a phishing email will contain all of the errors outlined above. You may only be looking for one error. This means that to spot phishing emails, you need to be vigilant and consider all of the possible issues outlined in this document.

If you do consider all the factors when looking at an email you might thing is suspicious, it will greatly reduce your risk of getting caught out by a phishing scam.

Remember! If it doesn’t look right, it probably isn’t!!

Trust your instincts. If you suspect an email is suspicious, you should treat it as such.

It is better to be safe than sorry!