HOW TO IDENTIFY A PHISHING EMAIL

Phishing is an attempt to trick the receiver through an electronic communication that seems to come from a trusted source.

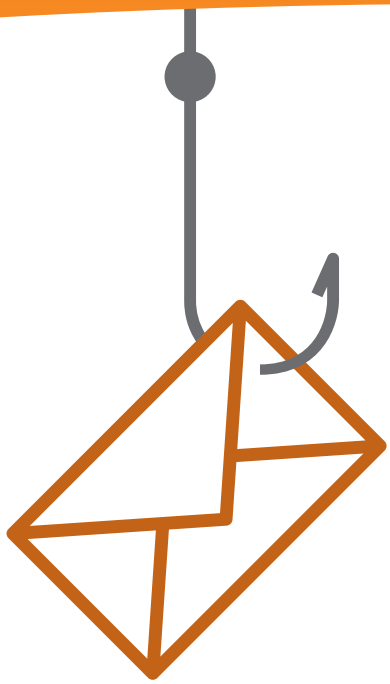
The attack is based on sending an email or message that seems to come from a company, organization or person that we are familiar with, while inviting you to carry out one of the following actions:

Download a file

Click on a link

Provide information

Make a payment



Although the main aim of this type of attack is usually to **obtain confidential information** (such as credit card numbers or passwords), at present this technique is also used to infect equipment or to **make us the victims of some type of scam**.

91% of security incidents begin with a phishing attack

These messages typically call on you to take urgent action, warn you about a problem, threaten you with possible sanctions or tempt you with an attractive offer.

Check out our **6 tips** on how to identify a phishing email

akcent cybersecurity

One of the characteristics that is common to this type of message is the use of a kind of bait designed to get us to bite the hook:

From: MusicStore <franz01@mail.com>
For: Anna Rovira
Date: 17/01/18
Subject: Your purchase at MusicStore
Attachment: Purchase receipt.doc

music store

Dear customer,
Thank you for your purchase at MusicStore on 17/01 10:39.
Product name: 80's Greatest Hits
Order number: 8EK1734-01
Total amount: €39.56
If you have not authorized this purchase, please **click here to begin to process a refund**

http://mail2chef.com/senderip.php

1. **Pay attention to the sender's address**. If the email seems to come from a legitimate entity but the email address corresponds to a personal account (for example, Gmail or Hotmail), it is probably a phishing email.

2. **Never trust attachments**, especially if they are executable files or contain macros. Download only those you are expecting.

3. Be suspicious of emails that **require action**, especially those that attempt to create a sense of urgency.

4. Do not trust emails that contain **generic greetings** ("Dear customer, Dear account holder"). Ask yourself whether the organization that contacts you should know your name.

5. Do not be taken in by the **apparent professionality** of the text or by the use of official logos. Phishing emails are no longer full of bad translations and spelling mistakes.

6. Before clicking on a link **hover the cursor** over it to see where it will take you. Place the cursor over the link (without clicking it!) and do not proceed unless the address that appears corresponds with the entity's domain.

An organization with a team prepared to detect fraudulent emails is less vulnerable to phishing attacks.

Contact **Ackcent Cybersecurity** for more information on how our **educational and training programs** can help you prevent phishing attacks.

info@ackcent.com
+34 935 011 300