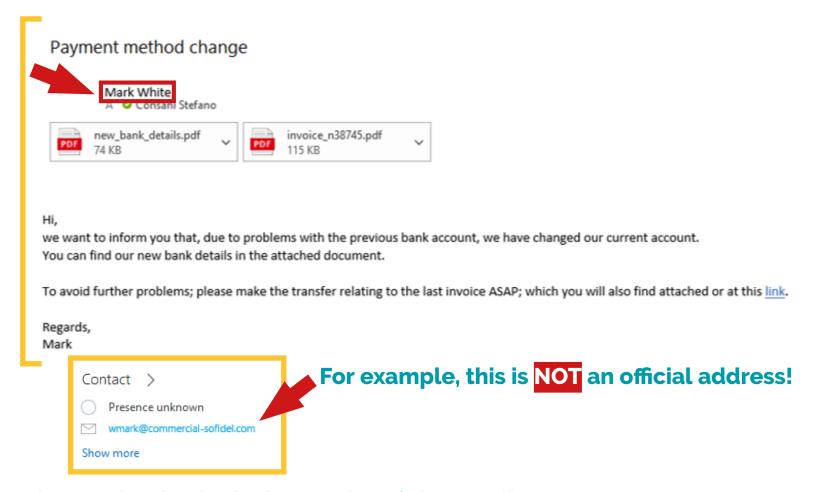
ANTI-SCAM RECOMMENDATIONS





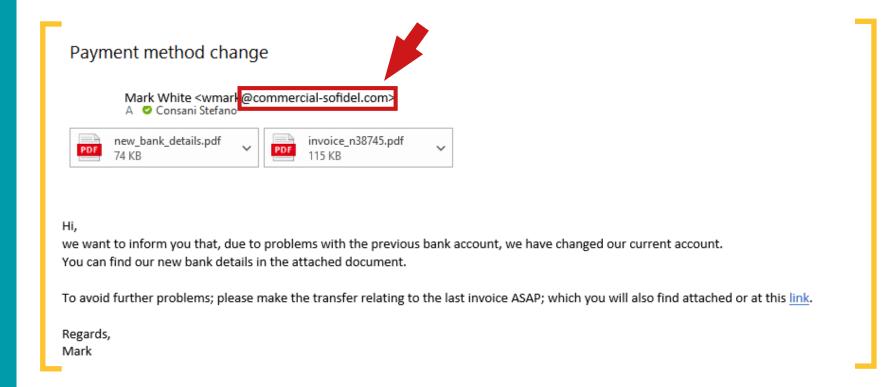
CHECK THE SENDER ADDRESS



Always check who is the sender of the emails.

If you only see the display name (first and last name), we suggest that you hover your cursor over the sender to read the full contact details and their full email address.

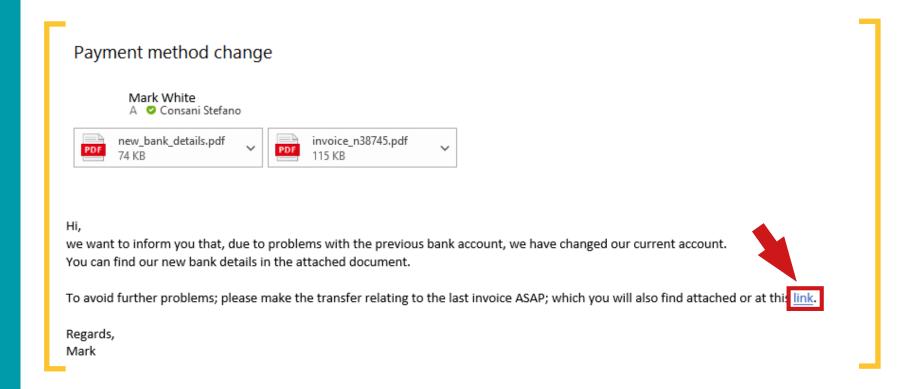
CHECK THE SENDER'S DOMAIN



Check that the email comes from @ sofidel.com or a Sofidel subdomain (@ subdomain.sofidel.com, for example @ communication.sofidel.com).

The one in the example is **NOT** an official address!

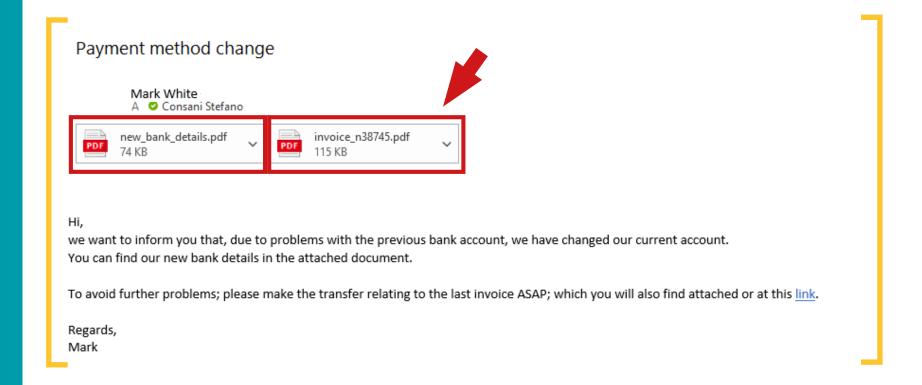
CHECK THE LINK



Always check the links contained in the emails and click only if you are sure.

A suggestion is to hover the mouse cursor over the link without clicking to read the website (URL) to which it refers.

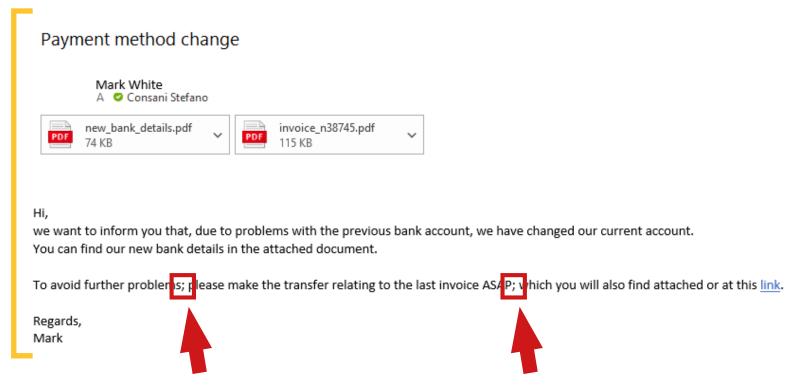
DON'T TRUST THE ATTACHMENTS



Do not open attachments without first checking and identifying the sender.

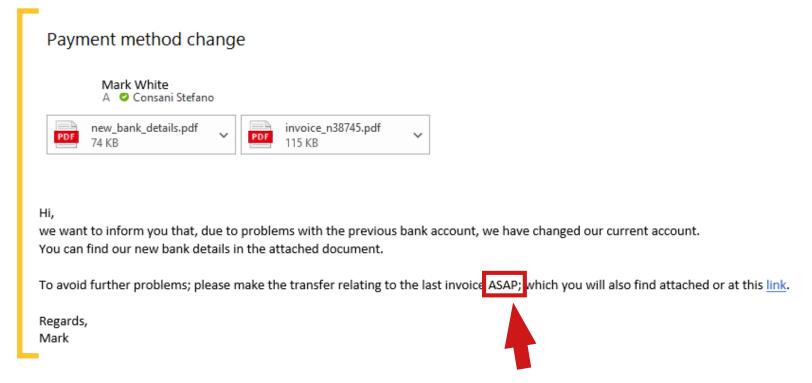
The names are often misleading.

CHECK FOR WEIRD GRAMMATICAL ERRORS



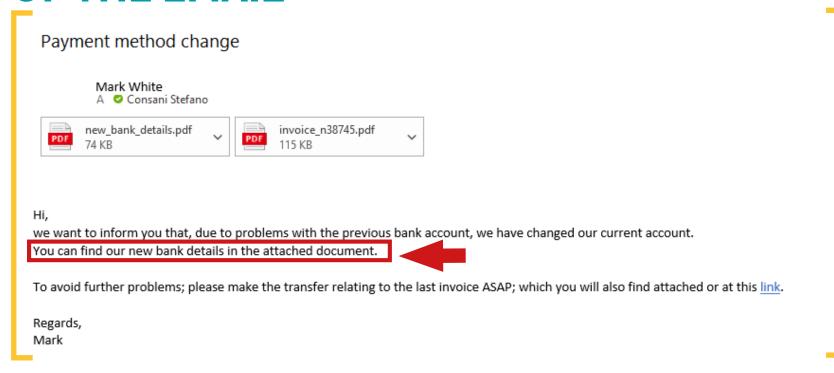
In phishing mail, you can often find repeated grammatical error.

CHECK IF THERE IS URGENCY ON THE REQUEST



Often in phishing emails the hacker tries to give you a **sense of urgency**.

PAY ATTENTION TO THE CONTENT OF THE EMAIL



Sofidel does not communicate information relating to bank details by e-mail.

Pay attention to the content of the email: if you receive communications regarding any changes in IBAN, changes in bank accounts and similar news, we recommend that you always request verbal verification with your Sofidel contact.