Anti-phishing document

Increasing number of scams: be vigilant!

In regards of the increasing number of scams from malicious companies and individuals, we invite you to be more vigilant.
We remind you that KyPay and Olkypay does not offer the sale of credits, shares or other financial investments.
Under no circumstances you should disclose your KyPay or Olkypay codes or identifiers.

What are the common frauds?

Fraudsters usually try to sell shares by e-mail or telephone, pretending to be a neobank or a payment institution such as ours.

What is phishing?

This scam technique aims to collect personal and confidential information by e-mail (login details, bank card number, etc.) and to push victims to carry out a financial transaction.

What is vishing?

Vishing is a method of phishing by telephone, also aiming to extort confidential financial or security data from victims, or even to induce them to make a money transfer. The fraudsters call their victims by phone pretending to be employees of the company.

How to spot fraud? What are the best practices?

Recognising a fraudulent e-mail

When you receive an e-mail claiming to be from KyPay or Olkypay, we offer you some ideas to help you distinguish between a legitimate communication and a phishing attempt.

1. **Is the sender's e-mail address the usual KyPay or Olkypay address?**

Fraudsters usually use an address close to the legitimate one. Make sure to check the sender's address (name and e-mail).

2. **Is the e-mail intended for you personally?**

Look to see if the content of the e-mail is personalised or if it begins with a "Dear Customer" type of message. Another criterion is if your e-mail address does not appear as the recipient: it means that the message is not personally addressed to you and has been sent in a mass mailing.

3. Does the content of the e-mail appear normal in form and substance?

The sender's e-mail address uses the name of the organisation or company whose identity is impersonated but often contains anomalies (inconsistencies in the logo, stretching of the logo, typographical errors, spelling mistakes, formatting, etc.). This should make you cautious.

This type of e-mail generally invites victims to respond within a short period of time. The e-mail may contain either a link to a fraudulent website that closely resembles the company's official website, or an attachment. Do not click on links without checking their origin and do not open attachments from a suspicious e-mail to avoid giving information to scammers and infecting your computer with a virus.

Stay alert when calling

Remember that the number you see on your phone may be spoofed. Do not make any money transfers and never give out your bank ID, PIN or any other security code over the phone.
No one claiming to be an employee of our company or one of our service providers is allowed to contact you to ask for login data or banking information such as a login or password.

What to do in case of doubt?

If you have any doubts about the legitimacy of an e-mail or a call, do not hesitate to contact us using the following form: https://support.olkypay.com/contact.