Anti-phishing document

OlkyPay Service

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 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 fishing ?

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 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

Rappelez-vous que le numéro qui s'affiche sur votre téléphone peut être usurpé. Ne procédez à aucun virement et ne communiquez jamais votre identifiant bancaire, votre code personnel ou tout autre code de sécurité par téléphone.

Aucun interlocuteur se présentant comme un collaborateur de notre établissement ou comme l'un de nos prestataires n'est autorisé à vous contacter pour vous demander des données de connexion ou d'informations bancaires de type identifiant, mot de passe.

What to do in case of doubt ?

Si vous avez un doute sur la légitimité d'un email ou d'un appel, n'hésitez pas à nous contacter via le formulaire suivant : https://www.olky.eu/en/universe/support/