Document anti-phishing

Service OlkyPay

Document anti-phishing

Multiplication des arnaques : soyez vigilants !

Face aux escroqueries de la part de sociétés et d'individus malveillants qui se multiplient, nous vous invitons à renforcer votre vigilance.
Nous vous rappelons que KYPAY et OlkyPay ne proposent pas la vente de crédits, d'actions, ou autres placements financiers. En aucun cas, vous ne devez divulguer vos codes ou vos identifiants KYPAY ou OlkyPay.

Quelles sont les fraudes courantes ?

Les fraudeurs cherchent généralement à vendre des actions par email ou par téléphone en se faisant passer pour une néobanque ou un établissement de paiement tel que le nôtre.

Qu'est-ce que le phishing (ou hameçonnage) ?

Cette technique d'escroquerie vise à récolter des informations personnelles et confidentielles par email (identifiants de connexion, numéro de carte bancaire…) et pousser les victimes à effectuer une opération financière.

Qu'est-ce que le vishing (ou hameçonnage vocal) ?

Le vishing est une méthode de phishing par téléphone, ayant également pour but d'extorquer des données confidentielles financières ou de sécurité des victimes, voire les inciter à réaliser un transfert d'argent. Les fraudeurs appellent leurs victimes par téléphone en se faisant passer pour des collaborateurs de la société.

Comment repérer les fraudes ? Quelles sont les bonnes pratiques ?

- **Reconnaître un courriel frauduleux**

Lorsque vous recevez un email qui prétend provenir de KYPAY ou d'OlkyPay, nous vous proposons quelques pistes de réflexion pour vous aider à distinguer une communication légitime d'une tentative de phishing.

1. **Est-ce que l'adresse mail de l'expéditeur est l'adresse habituelle de KYPAY ou d'OlkyPay**

Les fraudeurs utilisent en général une adresse proche de l'adresse légitime. Vérifiez bien l'adresse (nom et email) de l'émetteur.

2. **Est-ce que l'email vous est personnellement destiné ?**

   Regardez si le contenu de l'email est personnalisé ou s'il commence par une formule de type « Cher client ». Autre critère, si votre adresse mail n'apparait pas comme destinataire, le message ne vous est pas personnellement adressé et a fait l'objet d'un envoi de masse.

3. **Est-ce que le contenu de l'email semble normal sur la forme et sur le fond ?**

   L'adresse mail de l'expéditeur utilise le nom de l'organisme ou de la société dont l'identité est usurpée mais comporte souvent des anomalies (incohérences dans le logo, étirement du logo, erreurs typographiques, fautes d'orthographe, mise en forme…). Celles-ci doivent inciter à la méfiance.

   Ce type de courriel invite généralement les victimes à répondre dans un délai assez court. L'email peut contenir soit un lien qui renvoie vers un site internet frauduleux ressemblant fortement au site officiel de la société, soit une pièce jointe. Ne cliquez pas sur les liens sans vous être assuré de leur origine et n'ouvrez pas les pièces jointes d'un email douteux pour éviter de communiquer des informations à des escrocs et d'infecter votre ordinateur avec un virus.

Restez vigilants lors d'un appel

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.

Que faire en cas de doute ?

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/fr/universe/support