Sources : « le bon coin »

http://www2.leboncoin.fr/dc/phishing?ca=16_s

Chers internautes,

Soucieux de la qualité de notre site Internet, nous surveillons régulièrement les annonces diffusées. Cependant, nous nous sommes rendu compte que des personnes mal intentionnées utilisent notre site pour mettre en ligne des annonces fictives et tenter d'extorquer de l'argent. Nous vous recommandons la plus grande prudence vis-à-vis des cas suivants, il s'agit très certainement de **tentatives d'escroquerie** :

- Le **bien à vendre est à l'étranger** (Angleterre, Italie, Allemagne, Côte d'Ivoire...) et le «soi-disant» vendeur propose d'expédier le bien pour essai avant achat sous réserve du **versement d'un acompte**. Méfiez-vous, le bien risque fort de ne jamais vous parvenir.
- Le «soi-disant» vendeur se fait passer pour le Service Consommateur de notre site et certifie aux acquéreurs potentiels que le site a contrôlé la qualité du bien à vendre, la véracité des informations et documents communiqués par le vendeur. **Refusez systématiquement tout versement d'argent qui vous serait demandé au nom de notre site**. Nous n'intervenons en aucun cas comme intermédiaire ou tiers de confiance dans les transactions entre acheteurs et vendeurs.
- Un acheteur veut vous payer avec PayPal, Kwixo ou un autre service de paiement ou transfert en ligne et vous demande de créer un compte. Après avoir créé votre compte PayPal par exemple, vous avez reçu une confirmation de paiement par email. Avant d'envoyer l'objet de la vente, **connectez-vous à votre compte PayPal et vérifiez que vous avez bien reçu l'argent sur votre solde PayPal**. Méfiez-vous des emails. **Certains fraudeurs envoient de faux emails PayPal pour vous pousser à expédier un colis** alors que vous n'avez pas reçu le paiement. Vérifiez l'adresse email de provenance : si le préfixe rappelle le service de paiement et que le nom de domaine est un webmail gratuit (ex : service.paypal@gmail.com) et non d'une adresse du service de paiement en question (ex : service@paypal.com), c'est une tentative d'escroquerie. **Néamoins, le solde de votre compte PayPal est toujours la meilleure preuve que la vente se passe bien**.
- Vous venez de recevoir un mail vous signalant que **votre compte va être suspendu**. Cet email ne provient en aucun cas de nos services. Il s'agit d'une tentative de phishing, soyez vigilant et ne transmettez jamais vos coordonnées bancaires.
- Vous venez de recevoir un mail vous demandant de renseigner vos coordonnées bancaires suite à l'achat de l'option Logo Urgent. Cet email ne provient en aucun cas de nos services. Il s'agit d'une tentative de phishing, soyez vigilant et ne transmettez jamais vos coordonnées bancaires.
- Si vous recevez un **email de PayPal** vous demandant de **recharger votre compte à l'aide d'une carte PCS**, nous vous conseillons de ne pas donner suite à cette transaction.
- Le paiement du bien que vous souhaitez acheter ou vendre ne peut se faire que par **mandat cash, Western Union, carte PCS Mastercard, Ticket Premium ou Moneygram** ? Ces modes de paiement ne sont pas sécurisés et risquent bien d'être factices. Nous vous conseillons d'utiliser des moyens de paiement plus sécurisés.
- **L'acheteur est momentanément à l'étranger** et vous propose de vous envoyer l'argent par **mandat cash ou Western Union** pour réserver votre bien. Vous recevez ensuite un email de notification du service de paiement ou un email de l'acheteur vous invitant à vérifier que votre paiement a été effectué sur un faux site de La Poste ou de Western Union. Attention, si l'URL du site ou l'adresse email vous semble douteuses, il s'agit d'une tentative d'escroquerie.

- Un contact MSN vous demande un service : déposer une annonce sur notre site. En réalité, **cette personne a piraté le compte MSN de votre contact** et cherche à vous faire déposer une annonce frauduleuse. Ne déposez jamais d'annonce à la place de quelqu'un d'autre. Si vous avez déjà validé l'annonce, merci de nous transmettre les coordonnées avec lesquelles l'annonce a été déposée.
- Vous venez de recevoir un mail ou un SMS, vous devez rappeler une personne intéressée par votre annonce ou **un message vocal vous attend au 0899**... Il s'agit d'une **tentative d'escroquerie via un numéro surtaxé**. Supprimez le mail ou le SMS sans hésitation.
- Vous venez de recevoir **un SMS d'une personne vous demandant de la recontacter par email** (notamment depuis un numéro en 5 chiffres, ex : 37200). Il s'agit d'une tentative d'escroquerie. Supprimez le SMS sans hésitation.
- Certains acheteurs utilisent des **faux billets** pour payer les transactions auprès de particuliers. N'hésitez pas à vérifier l'authenticité des billets avant d'accepter une transaction. Quelques secondes suffisent : touchez, regardez et inclinez-le. Pour plus d'informations, consultez le site de la Banque de France. En cas de doute, refusez la transaction. Si vous êtes victime, déposez plainte devant un service de police ou de gendarmerie.

Nous vous recommandons de faire preuve de vigilance, bien que nous mettions tout en oeuvre pour faire cesser ces agissements. Si vous avez un doute sur la qualité de votre interlocuteur, n'hésitez pas à envoyer un email à notre service clientèle.

Enfin sachez que vous pouvez signaler tout SMS non désiré en le transférant au 33 700.

Fermer la fenêtre