

**Une bonne affaire...trop belle
pour être vraie**

Khadraoui Amine

Achat d'une PS5 sur Facebook Marketplace

- Transaction en ligne classique entre particuliers
- Communication faite via Messenger
- Système de paiement non sécurisé
- Absence de tiers de confiance pour encadrer la transaction



- Description de l'annonce: https://www.facebook.com/marketplace/item/2769168079882602/?ref=facebook_story_share

Déroulement de l'arnaque



- Une offre intéressante
- Vendeur crédible, interaction numérique fluide, envoi de preuves pour renforcer la confiance
- Je me voyais déjà avec ma PS5 !
- Il me transmet même sa carte d'identité, son numéro de téléphone et un IBAN pour effectuer le paiement. À ce stade, tout semblait cohérent, ce qui crée un climat de confiance artificiel.



Profil de la personne :
Anonymous (076 XXX XX
XX)

Techniques d'ingénierie sociale et usurpation d'identité



- Avec du recul, on identifie la une technique d'ingénierie sociale. Il ne s'agit pas d'un piratage, mais d'une manipulation psychologique visant à exploiter le facteur humain.
 - L'attaquant crée artificiellement un climat de confiance en envoyant une pièce d'identité, un nom, une adresse et un compte bancaire suisse.
- Usurpation d'identité (rien ne prouve que c'est vraiment la même personne qui communique avec moi, même avec la photo de 'lui', tenant sa carte d'identité)

Une arnaque montée de toute pièce?

- Paiement effectué par virement bancaire, via IBAN fourni par le vendeur.
 - Ce choix n'est pas anodin : virement bancaire = non réversible, une fois le paiement effectué, la traçabilité devient plus complexe
- Il n'y avait aucun tiers de confiance ni mécanisme de protection pour sécuriser la transaction.
- Compte bancaire situé en Suisse.
 - Possibilité : Il s'agit sûrement d'une mule bancaire, c'est-à-dire d'un compte utilisé pour recevoir des fonds frauduleux avant le transfert vers d'autres comptes.



Place au doute...

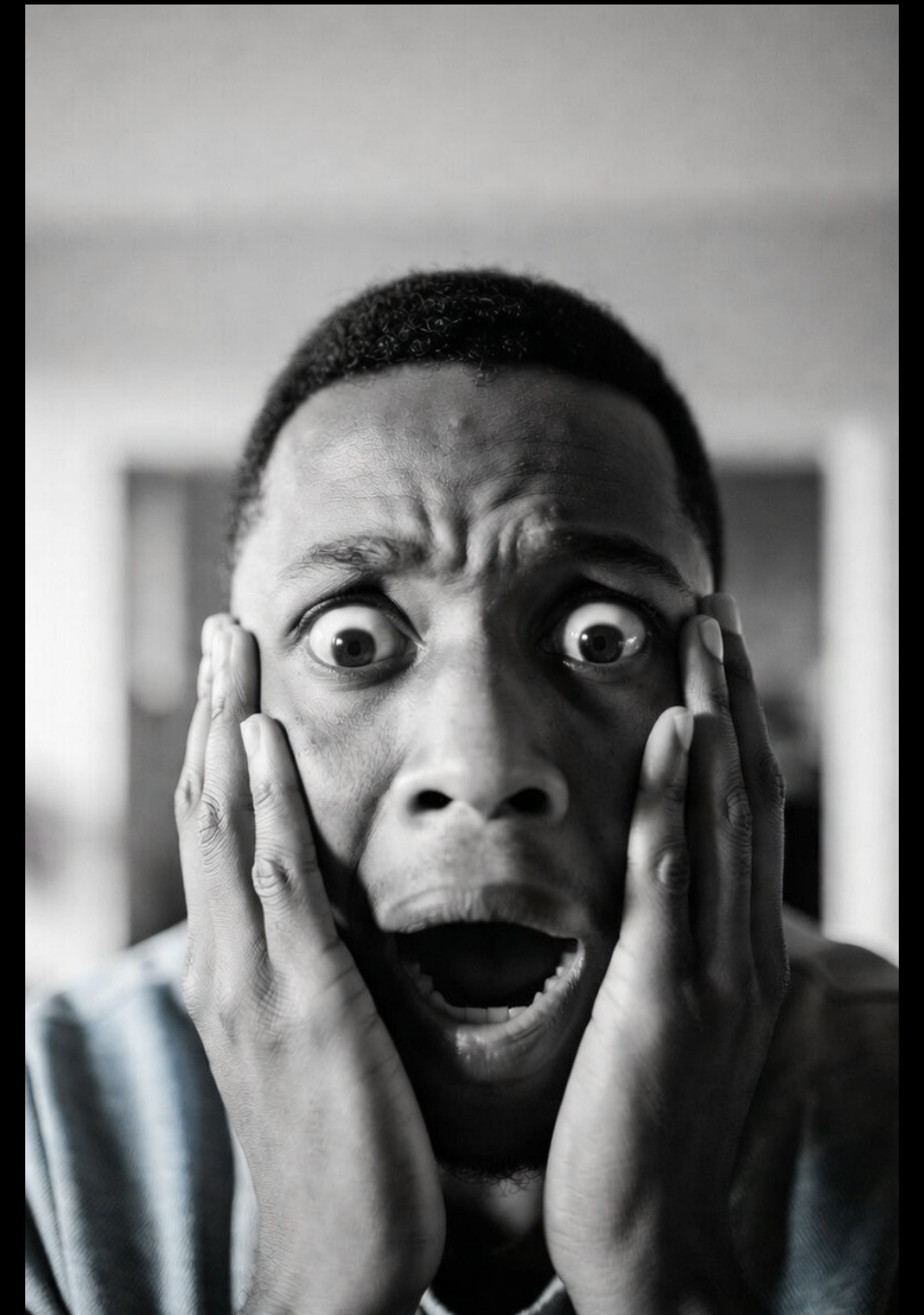


Après avoir mené une petite enquête, on a remarqué que des annonces identiques réapparaissent le lendemain avec les mêmes photos mais sous différents profils. Cela nous montre une stratégie de rotation de comptes

*On voit ici que derrière ce qui semble être une simple arnaque se cache en réalité une stratégie **organisée et répétitive**, presque industrielle!*

Conséquences et enseignements

- Après le paiement, plus de nouvelles !
- Malgré le nom, l'adresse, le numéro de téléphone, et le compte bancaire fournis, l'identification est très difficile



Mais malgré tout, cette arnaque montre que, en Cybersécurité, la principale vulnérabilité n'est pas toujours technique, mais humaine.

Le facteur humain reste le maillon faible! Alors ne faites jamais vraiment confiance et restez vigilants!

Finalement

Aujourd'hui, l'affaire a évolué...

Après plusieurs mois d'instruction, les autorités ont probablement identifié le responsable présumé. (courrier reçu du Tribunal de Thurgovie)

Plusieurs cas similaires, avec plusieurs victimes.

Désormais, nous sommes en mesure déposer une plainte pénale.

Donc finalement, malgré la complexité de la traçabilité numérique, la justice est parvenue à remonter jusqu'aux auteurs.