RÉSEAUX SOCIAUX

Arnaques à la mode Facebook

Les escroqueries s'immiscent partout sur le site, sous forme de faux comptes et de publicités trompeuses. Gare au clic de trop.

— Par **MARIE BOURDELLÈS**

J'ai vu une publicité sur Facebook. J'ai cliqué par curiosité. » Madame A. a commandé trois culottes menstruelles sur Nefina.com, pour seulement 59 €. On lui a livré des slips… pas du tout absorbants et elle n'a jamais pu se faire rembourser. Le site a vite coupé court à la conversation à la suite de ses réclamations. Scénario similaire : « *Sur Facebook, une publicité pour des vêtements m'a tapé dans l'œil. J'ai cliqué* », raconte Madame T. Sur les trois articles achetés sur Beyounging.com (total : 86,60 €), elle n'en reçoit que deux, « *de très mauvaise qualité et pas du tout à ma taille* ».

Les témoignages s'enchaînent. Le piège ? Une belle réclame sur le réseau social, émanant d'un site éphémère, prétendument français mais en réalité situé hors Union européenne. Une fois l'argent débité, on n'obtient plus de réponse et le remboursement devient bien sûr impossible. Le signalement auprès de Facebook demeure sans suite. Le mastodonte créé par Mark Zuckerberg, qui vit grâce à ses revenus publicitaires (55 milliards de dollars en 2018), aurait-il intérêt à laisser faire ? Bien qu'il mette en avant les plus de 30 000 personnes qu'il emploie pour assurer la sécurité, il peine visiblement à faire le ménage. Les faux comptes – profils inventés de toutes pièces et usurpations d'identité – ont également envahi la plateforme. Le but : voler de l'argent aux abonnés par différents stratagèmes. Rémi Ausseil, brigadier-chef au commissariat de Perpignan (66), donne l'exemple d'une page Facebook usurpant la raison sociale d'un garage (lire l'illustration ci-dessus). Les escrocs y publient des annonces de vente de voitures à prix très bas et demandent à être contactés sur Messenger, la messagerie privée du géant américain. Une fois leur victime amadouée, ils exigent qu'elle leur verse un acompte par virement. Ces truands, opérant depuis le Bénin, s'évaporent ensuite avec leur butin… Un autre gendarme, Gentil Gendy sur les réseaux sociaux, témoigne :

N'oubliez pas : si c'est trop beau, il y a un loup !

1 UNE JOLIE VOITURE NEUVE À PRIX CANON, ÇA VOUS FAIT RÊVER…

INKIE / AGENCE MARIE BASTILLE

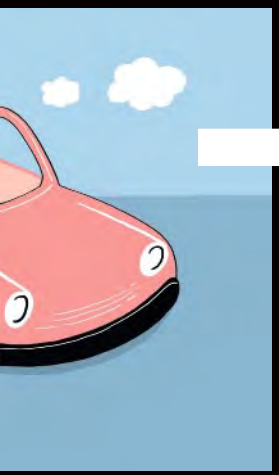
Points de vue

DEUX SPÉCIALISTES EXPLIQUENT LE PHÉNOMÈNE

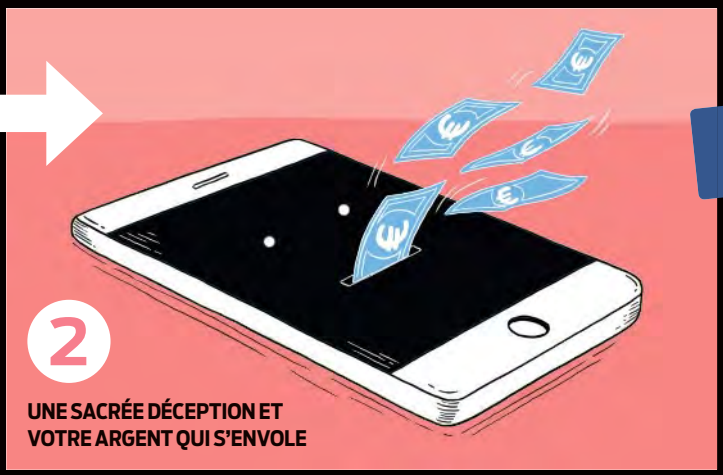
« *La criminalité classique se déporte sur les réseaux sociaux : ça expose moins et ça rapporte plus. Les escrocs misent sur la crédulité des gens et sur le gain de confiance grâce à un système fermé, où les abonnés se connaissent* », explique Jean-Sylvain Chavanne, directeur chez CEIS à Brest, agence spécialisée dans le conseil en stratégie, l'intelligence économique et la cyberdéfense. Avec ses 2,5 milliards d'utilisateurs par mois, Facebook a de quoi attirer les malfaiteurs. « *C'est du* business development *de base : si je veux faire beaucoup d'argent, je dois toucher les foules, d'où ma présence sur Facebook mais également sur WhatsApp ou bien Instagram,* analyse Rayna Stamboliyska, expert en cybercriminalité. *Sur ces réseaux, il y a autant d'usages que de personnes. Donc, il est très difficile de détecter les faux comptes en se basant uniquement sur le comportement.* » Facebook, une planque de rêve ?

NOUN PROJECT

MÉFIEZ-VOUS DE CES DEUX TECHNIQUES



1 UN HAMEÇON BIEN GROS QUI VOUS DONNE ENVIE DE PASSER COMMANDE



2 UNE SACRÉE DÉCEPTION ET VOTRE ARGENT QUI S'ENVOLE

BELLE PUB POUR PRODUIT AFFREUX

1. Visuel attractif, produit sensationnel à prix « défiant toute concurrence », offre « à saisir » : voilà la recette des publicités que des sites frauduleux diffusent sur Facebook. L'internaute qui clique sur le lien arrive sur la page du vendeur et tombe dans le piège.

2. Le client paie sa commande mais ne reçoit rien ou alors un produit défectueux. Et, bien sûr, il peut dire adieu à son argent.

2 VOUS VERSEZ L'ACOMPTE, POUR L'ESCROC, LA PÊCHE EST BONNE !

FAUX COMPTE FACEBOOK

1. Ayant créé un faux profil ou usurpé la raison sociale d'une entreprise, les bandits publient sur Facebook des offres alléchantes : smartphones à 1 € ou véhicules neufs vendus à prix cassés par un garage, par exemple. Pour les contacter, il faut passer par Messenger.

2. Une fois ferrée, la victime reçoit un RIB, toujours via Messenger, et doit verser un gros acompte. Une fois l'argent empoché, les escrocs disparaissent dans la nature.

« Depuis le début de l'année 2019, j'ai enregistré 24 plaintes concernant des escroqueries sur Facebook, pour un total de 18 500 €. La plupart sont du domaine sentimental : un arnaqueur crée le compte d'une femme avec une photo attractive. Il engage la conversation via Messenger avec un homme célibataire au profil sans degré de confidentialité. Petit à petit, il lui fait croire au grand amour, et finit par lui expliquer ses "problèmes" financiers. L'homme abusé lui envoie plusieurs fois de l'argent via des tickets PCS [recharges pour carte prépayée, ndlr] *achetés dans un tabac. »* Ce type d'arnaque peut durer des semaines, pour des montants cumulés *« rarement en dessous de 500 € »*, avant que « l'être aimé » ne s'envole. Or *« 99 % des plaintes n'aboutissent pas, car les criminels agissent depuis des pays (à 95 % en Afrique) avec lesquels la France n'a pas de coopération financière. On commence les investigations et, très vite, on ne peut plus rien faire. Quant à Facebook, il ne fournit que l'adresse IP du compte, et tardivement »*, déplore Gentil Gendy.

La police piétine

La liste de ces duperies est longue : jeu concours pour faire appeler un numéro surtaxé ; offre de Samsung S9 à 1 € qui masque du *phishing* (vol de coordonnées bancaires) ; emploi facile à forte rémunération… Facebook dit avoir désactivé 5,4 milliards de faux comptes entre janvier et septembre 2019. Pourtant, ils foisonnent encore. *« Il y a vraiment un problème de transparence avec ce réseau, aucun audit d'une entité tierce indépendante n'est effectué »*, souligne Rayna Stamboliyska, membre du Club des experts de la sécurité de l'information et du numérique (Cesin) et responsable adjoint de la sécurité des systèmes d'information de l'entreprise Oodrive. Du côté de la police, la chasse aux filous s'embourbe. Les services de lutte contre la cybercriminalité du ministère de l'Intérieur ainsi que ceux de la préfecture de police de Paris n'ont pas souhaité s'exprimer. Un silence qui en dit long. ◆

Nos conseils

 # Vérifiez les offres alléchantes en contactant la société ou l'organisme officiels soi-disant émetteurs.

 # N'acceptez pas d'invitations de personnes/pages que vous ne connaissez pas, et ne leur fournissez jamais de données personnelles.

 # Portez plainte si vous avez été piégé, et faites opposition sur votre carte bancaire au besoin.