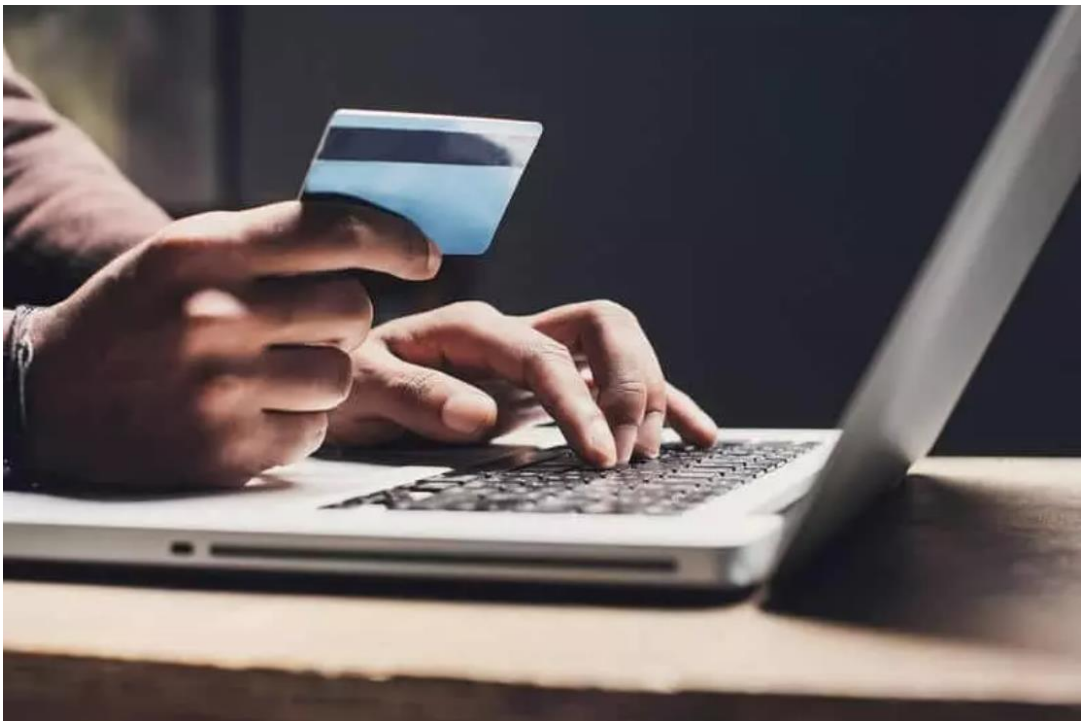
Article publié le 28/09/2021 par Jean-Tenahe FAATAU
EXPERTISE. Outre-mer : L'IEDOM et l'IEOM alertent sur les arnaques financières | Outremers360

EXPERTISE : Outre-mer : L'IEDOM et l'IEOM alertent sur les arnaques financières



La pandémie de COVID-19 a conduit de nombreux consommateurs ultramarins à se tourner vers le commerce électronique ou à répondre aux sollicitations via les réseaux sociaux, alors qu'ils n'y étaient pas familiers jusque-là… et les fraudeurs ne s'y trompent pas ! Les Instituts d'Émission d'Outre-mer font un point sur les principaux canaux des fraudeurs, les arnaques à éviter ainsi que les moyens pour les éviter.

Les fraudes sur les moyens de paiement en outre-mer concernent principalement le chèque qui reste le moyen de paiement le plus fraudé et la carte bancaire. Vient ensuite la fraude au virement, plus faible en nombre mais qui peut être très importante en montant comme l'a montré une importante fraude au Président survenue en Polynésie Française en 2019.

En 2020, la fraude a représenté 1,3 milliard d'euros en métropole et dans les DCOM de la zone euro, en hausse de 4% sur un an, alors que la progression dans le Pacifique a été de 6% entre 2018 et 2020, avec des montants de fraude qui ont atteint un peu moins de 4 millions d'euros.

Quels sont les principaux canaux qu'utilisent les fraudeurs en outre-mer ?

Les réseaux sociaux sont un canal largement utilisé par les fraudeurs, notamment dans le cas de la fraude au virement. Cette fraude peut prendre plusieurs formes : les « prêts sur Facebook », qui consistent pour le fraudeur à créer un lien de proximité avec la victime avant de lui demander l'envoi d'argent, ou encore la promesse de versement d'aide publique quand la victime est invitée à procéder à un virement pour pouvoir bénéficier d'une aide publique de montant important… qui n'arrivera jamais. La vigilance doit donc être de mise lors de la réalisation d'un virement au bénéfice d'une personne que vous ne connaissez pas. Si les autorités publiques comme les banques renforcent la sécurité des moyens de paiement, sachez que le meilleur rempart contre la fraude : c'est vous !

Quelles sont les principales arnaques à éviter ?

Les arnaques financières concernent principalement la fraude aux moyens de paiement, aux crédits et aux placements. Et l'Outre-Mer n'est pas à l'écart de ces arnaques.

S'agissant des moyens de paiement, attention au vol de chéquiers et à la falsification de chèques. Assurez-vous régulièrement que vous l'avez bien en votre possession.

La fraude sur carte de paiement affecte plus particulièrement les paiements en ligne. C'est pour cela que de nouvelles réglementations européennes ont mis en place une double authentification du débiteur, par exemple avec un mot de passe permanent et l'envoi d'un code temporaire sur le téléphone mobile.

Attention également aux offres de crédits aux conditions très, voire trop avantageuses (sans conditions de ressources, avec des fonds disponibles sous quelques jours) qui représentent une source importante d'arnaques qui circulent sur Internet.

De même, dans le contexte de taux bas, la tentation est alors forte d'opter pour des offres de placement plus attractives. C'est dans ce contexte que se développent des arnaques avec des produits d'épargne proposant des rendements élevés de 4% à 8%. Il faut être extrêmement vigilant à l'égard de ces taux hors normes qui incitent les épargnants à verser d'importantes sommes d'argent. Parfois même, l'escroc gagne la confiance de la victime en versant un premier intérêt conforme au taux annoncé, pour que la victime poursuive des versements… qu'elle ne reverra jamais.

Enfin, on peut également citer le trading en ligne, qui s'adresse aux épargnants souhaitant « boursicoter ». Ainsi, de nombreux sites internet se font passer pour des intermédiaires en placements financiers et proposent aux particuliers leurs services en ligne alors qu'ils ne possèdent aucune autorisation pour cela. Là encore, restez vigilants et vérifiez la liste noire des sites frauduleux (à la fin de cet article).

Est-ce-que la pandémie a amplifié la fraude ?

Les fraudeurs renouvellent très régulièrement leurs modes d'approche. La pandémie de COVID-19 a conduit de nombreux consommateurs à se tourner vers le commerce électronique. La fraude sur les

transactions par carte a principalement pour origine l'usurpation des numéros de carte. En Outre-mer, les techniques sont similaires, qu'il s'agisse de l'hameçonnage (*phishing*) et des logiciels malveillants (*malwares*). L'hameçonnage repose le plus souvent sur l'envoi de courriels empruntant les chartes visuelles et logos usurpés de votre fournisseur d'énergie, de téléphonie mobile, ou encore de votre banque, et vous invitant à vous connecter à un site qui s'avère frauduleux. L'objectif est de collecter les données de la carte de paiement et de les utiliser jusqu'à ce que la victime s'en rende compte. Les logiciels malveillants sont souvent installés à votre insu sur votre ordinateur, généralement lorsque vous ouvrez la pièce jointe contaminée d'un e-mail ou lorsque vous cliquez sur un hyperlien via un site Internet infecté.

Quels sont les moyens pour éviter ces arnaques ?

Pour éviter la fraude aux cartes bancaires, il faut éviter d'enregistrer les coordonnées de votre carte sur un site marchand. Vérifiez systématiquement la présence du cadenas et du « s » de https qui assure que le site est sécurisé (ci-dessous). Dans tous les cas, gardez à l'esprit qu'aucun organisme légitime ne vous demandera vos coordonnées bancaires ou mots de passe confidentiels.

Pour déjouer le phishing : il est déconseillé d'ouvrir les pièces jointes ou de cliquer sur des liens des messages provenant d'expéditeurs inconnus. Il convient de privilégier l'accès direct sur le site de l'organisme, ce qui permet d'ailleurs de vérifier l'authenticité de la demande.

Par ailleurs, il est recommandé de faire très régulièrement les mises à jour de sécurité du système d'exploitation de l'ordinateur et du mobile, le plus rapidement possible après l'annonce de votre opérateur.

L'Autorité des Marchés Financiers (AMF) aide les usagers à se protéger contre les arnaques en lien avec l'Autorité de contrôle prudentiel et de résolution (ACPR). Ces deux autorités publient des listes noires de sites ou entités non autorisés en France. Retrouvez-les sur le site dédié : www.abe-infoservice.fr

La zone Pacifique est-elle également concernée par ces arnaques financières ?

Oui tout à fait, la fraude progresse aussi dans les collectivités françaises du Pacifique même si le taux d'incidence reste encore en deçà de ceux observés dans les DCOM de la zone euro et l'Hexagone. En 2020 plus de 50% des montants fraudés dans le Pacifique ont été virés sur un compte métropolitain ou domien. Mais, à l'opposé de ce qui s'observe en France hexagonale et dans les DCOM, le niveau de la fraude sur le chèque se replie dans le Pacifique, de même que la fraude sur virement. Mais il est vrai que l'année 2019 a été marquée par une importante fraude au Président en Polynésie Française, technique d'escroquerie basée sur l'usurpation d'identité d'un dirigeant d'entreprise.

Sources :
Rapport annuel 2020 de l'Observatoire de la sécurité des moyens de paiement (OSMP) du 6 juillet 2021 : 821162_osmp_2020_web.pdf (banque-france.fr)
Cartographie des moyens de paiement scripturaux et recensement de la fraude dans les collectivités d'outre-mer du Pacifique en 2020