



Lutte contre les escroqueries et manœuvres financières frauduleuses



« Vous avez reçu un mail de l'Assurance Maladie. Nous vous informons que vous avez un remboursement en attente d'un montant de 500 euros sur votre espace personnel. Le RIB enregistré sur votre espace personnel n'a pas pu être crédité. Pour accepter le paiement rapide cliquez sur le lien suivant et sélectionnez un remboursement. »

C'EST UN MAIL FRAUDULEUX ! NE RÉPONDEZ PAS ! NE TRANSMETTEZ JAMAIS VOS INFORMATIONS PERSONNELLES !

« L'escroquerie peut être faite soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs, ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. » (Art. 313-1 du code pénal).

Le HAMEÇONNAGE (ou *phishing*) est une escroquerie **par internet** très utilisée par les fraudeurs, par **e-mail**, par **des liens ou des faux sites web** ou **pièces jointes**. Les fraudeurs volent vos données et peuvent se servir de vos numéros de comptes bancaires.

Pour se prémunir contre le phishing :

- Ne **jamais cliquer sur des liens** avant d'avoir lu l'intégralité du message ;
- Ne **jamais transmettre d'informations bancaires** par courrier électronique ;
- Ne **jamais répondre à un courrier électronique vous demandant des informations personnelles**. Les banques ou les administrations ne vous les demanderont jamais par mail ;
- Dans le doute, **appeler l'administration ou l'entreprise concernée**.

Si vous avez déjà cliqué :

- Connectez-vous rapidement sur le compte concerné et **changer le mot de passe** ;
- Appeler **l'organisme concerné pour informer de la situation** ;
- Appeler **Info ESCROQUERIE au 08.05.80.58.17** ;
- Faire une **analyse antivirus par précaution sur votre ordinateur** ;
- **Porter plainte à la brigade de gendarmerie locale**. Munissez-vous des références du transfert frauduleux, ainsi que des références de la personne ou tout renseignement pouvant aider à l'identification de l'escroc.

Dans tous les cas : Transférer le courrier électronique sur internet-signalement.gouv.fr

L'escroquerie peut aussi être effectuée par **téléphone**, par **texto**, ou par **courrier**. Soyez doublement vigilants lorsque l'on vous propose des paiements en PCS ou WESTERN UNION... Il y a de fortes chances que vous soyez victimes d'une arnaque.

SI VOUS AVEZ GAGNÉ ET QUE VOUS DEVEZ PAYER... VOUS ÊTES EN TRAIN DE VOUS FAIRE ESCROQUER !