DOSSIER :
LES ARNAQUES SUR INTERNET

1. Les arnaques les plus fréquentes
2. Les arnaques les plus courantes dans l'hôtellerie
3. Comment déceler une arnaque ?
4. Comment se protéger ?
5. Comment réagir si l'on est victime d'une arnaque ?

1. Les arnaques les plus fréquentes

De nos jours, professionnels ou particuliers : personne n'est épargné.

L'utilisation frauduleuse de vos numéros de carte bancaire sur internet afin de réaliser des achats ou des prélèvements.

Les escroqueries dites « **à la nigériane** » ou « **fraude 419** ». Il existe de nombreuses variantes. Dans la majorité des cas l'interlocuteur rentre en confiance avec vous via un échange de mail concernant, par exemple, une petite annonce, un appel aux dons, ou encore en se faisant passer pour un ami en détresse en piratant une boite mail. Il demande alors un transfert d'argent via Western Union.

Le « **CripLocker** » : il s'agit d'un logiciel malveillant dit « **rançongiciel** » se propageant par courrier électronique à travers une pièce jointe ou un fichier zippé. A l'ouverture de ceux-ci, des données des disques internes ou disponibles par le réseau sont alors bloquées. Les pirates annoncent alors qu'ils rendront l'accès à ces données après le paiement d'une rançon dans un délai imparti. Ils utilisent souvent le graphisme de l'Etat (Police ou Gendarmerie Nationale) pour communiquer. Bien-sûr, même après le paiement, les données ne sont pas restituées.

Le « **phishing** » : l'arnaqueur se fait passer pour votre banque et vous demande vos coordonnées bancaires afin de prélever de l'argent de votre compte.

2. Les arnaques les plus courantes dans l'hôtellerie

Demande de **réservation par e-mail d'un client étranger**, le plus fréquemment africain (souvent de Côte d'Ivoire). Le client souhaite faire une réservation et régler par anticipation. Cependant il vous explique qu'il ne peut pas effectuer un paiement à distance sans que les deux parties aient payé une taxe permettant d'obtenir l'autorisation de virement. Cette situation est dûe à des lois ivoiriennes tentant de lutter contre le trafic d'armes. Vous serez alors également contacté par **un représentant de la commission de transfert de l'UEMOA***. Cela pourra paraitre très convaincant et des pièces justificatives seront présentées. Vous payez alors la taxe par Western Union pensant être remboursé et le client disparait.

* UEMOA : Union Economique Monétaire Ouest Africaine

Un client étranger effectue une réservation et souhaite payer par anticipation. **Vous reçevez bien le paiement sur votre compte bancaire**. Puis le client annonce qu'il souhaite annuler son séjour et demande à être remboursé. Vous effectuez alors **le remboursement par Western Union** sans vous méfier. Cependant le paiement versé par le client était valide mais effectué avec une carte usurpée. Lorsque le propriétaire de la carte réalise qu'elle a été utilisée, il fait opposition et la 1ère transaction bancaire est donc annulée, alors que vous avez déjà réalisé le remboursement par Western Union.

3.Comment déceler une arnaque ?

- Dans les premiers mails l'objectif est souvent de récupérer de nombreuses informations sur l'adresse, et l'état civil de l'hébergeur.
- En général les messages contiennent de nombreuses fautes d'orthographe et des erreurs de syntaxe.
- Les adresses de l'administration française finissent toujours par gouv.fr et non par des noms de domaine privés, notamment pour les agents des ambassades.
- Les logos sont souvent déformés


impots.gouv.fr

Chèr(e) client(e),

Aprés les derniers calculs de votre impots sur le revenu, nous avons déterminé que vous êtes admissible à recevoir un remboursement de notre part d'un montant de 312,00 €

Priére de soumettre votre demande de remboursement et nous permettre de 2 jours ouvrables pour le traitement de votre situation .

Quelles sont les démarches à suivre pour effectué mon remboursement ?

Cliquez ci-dessous et connectez-vous pour mettre à jour vos données pour que votre remboursement soit effectué dans les plus brefs délais .


EDF CHANGER L'ENERGIE ENSEMBLE

Chèr(e) Client(e),

Votre prélevement bancaire a été refusée par votre banque . Afin de regulariser votre situation veuillez vous rettérez ci-déssous :

Cliquez ici pour résoudre ce problème.

Lors d'echec de regularisation de votre situation , nous procèderons à la suspension de votre fourniture d'energie. Cette intervention vous sera facturée.

Merci de votre confiance.

Dominique REMOND
Directeur Service Client

EDF bleu ciel

4. Comment se protéger ?

1. Ne répondez jamais à un courriel vous demandant de transmettre vos coordonnées bancaires. Une banque ou une institution de confiance ne vous demandera jamais d'informations confidentielles à distance. En cas de doute appelez votre banque avant d'effectuer toute réponse.

2. Installez un **anti-virus** efficace.

3. Utilisez des **mots de passe robustes** qui seront difficiles à deviner à l'aide d'outils automatisés. Pour cela, préférez les mots de passe long et à caractères de différents types (majuscules, minuscules, chiffres) et évitez tout mot de passe ayant un lien avec vous. Enfin ne configurez pas les logiciels pour qu'ils retiennent les mots de passe, et variez vos mots de passe d'un compte à l'autre.

4. Effectuez les **mises à jour** de votre système d'exploitation et de vos différents logiciels.

5. Evitez d'utiliser des réseaux Wifi ouverts et non maitrisés pour ajouter ou modifier des contenus de sites internet.

4. Comment se protéger ?

6 Si vous êtes hébergeurs, refusez toujours de rembourser une réservation sur un moyen de paiement différent de celui utilisé pour la réservation.

7 Ne pas envoyer d'argent en ligne ou par chèque. De manière générale, soyez vigilant avec les moyens de paiement à distance tels que Paypal, moneygramme et Western Union.

8 Soyez vigilant lors de l'ouverture de pièces jointes dans des courriels. Pour cela vérifiez la cohérence entre expéditeur et contenu. N'ouvrez pas les pièces jointes dont les extensions sont : **pif, .com, .bat, .exe, .vbs ou .lnk**. À l'inverse privilégiez les formats **.rtf et .pdf**

9 De même pour les liens dans les courriels : avant de cliquer sur un lien passez votre souris dessus, l'adresse qui s'affiche doit alors être **identique** à celle annoncée par le lien. Si ce n'est pas le cas, n'ouvrez pas ce lien

10 Désactivez par défaut les composantes Active X et JavasScript présentant des risques de sécurité pouvant aller jusqu'à la prise de controle d'un ordinateur. Préférez les activer seulement sur des sites de confiance

5.Comment réagir si l'on est victime d'une arnaque ?

Lorsque vous réalisez que vous avez été victime d'une escroquerie il est conseillé de :

- **Conserver les traces disponibles**, notamment si vous souhaitez porter plainte.
- Dans le cas de transaction bancaire : prendre **contact avec votre banque** afin **d'annuler les transferts monétaires.**
- Toujours dans le cas de transaction bancaire : **portez plainte** au commissariat de police ou à la gendarmerie la plus proche.

Pour tout renseignement ou pour signaler un mail ou un site qui vous semble être une tentative d'escroquerie, deux dispositifs ont été mis en place :

✓ INFO ESCROQUERIES
08 11 02 02 17
(Prix d'un appel local depuis un poste fixe)

✓ **www.internet-signalement.gouv.fr**