Alerte aux MESSAGES FRAUDULEUX ou « PHISHING »

L'UNABCC vous met en garde contre le « phishing » : ce sont des messages frauduleux que vous avez peut-être reçus, par courriel ou par téléphone (SMS ou message vocal).

1. Que faire si vous avez reçu un message frauduleux ?

- Ne répondez pas au courriel - ou au SMS - ou au message vocal frauduleux, ne remplissez pas les données qui vous sont demandées, et n'appelez pas le numéro de téléphone qu'il peut comporter.
- Ne cliquez pas sur les liens ni sur les boutons du courriel frauduleux, et n'ouvrez pas les pièces jointes.
- Nous vous invitons à participer à la lutte contre le piratage informatique en signalant l'adresse du site frauduleux sur la page suivante : http://www.phishing-initiative.com
- Si vous avez un doute sur un message, nous vous invitons à contacter votre interlocuteur pour le vérifier avant d'y répondre.
- Supprimez le courriel - ou le SMS – ou le message vocal frauduleux de votre boîte de messages.
- Assurez-vous régulièrement que les systèmes de sécurité de votre ordinateur et de votre téléphone portable sont à jour. En savoir plus sur le site de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)

2. Que faire si vous avez répondu à un message frauduleux ?

- Si vous avez communiqué vos coordonnées bancaires suite à un message frauduleux, faites immédiatement opposition auprès de votre banque.
- Si vous avez communiqué vos identifiants de connexion, sur n'importe quel site, signalez-le vite au site concerné qui vous transmettra un nouveau code confidentiel.
- Si vous avez retourné copie de votre carte d'identité ou tout autre justificatif aux auteurs d'un message frauduleux, nous vous conseillons de porter plainte auprès de la gendarmerie ou du commissariat le plus proche de votre domicile.
- Si vous pensez avoir été victime d'une escroquerie par « phishing », vous pouvez aussi le signaler sur le site officiel suivant : www.internet-signalement.gouv.fr. Cette plateforme permet de signaler les sites internet dont le contenu est illicite, mais aussi les tentatives de « phishing ».
- Supprimez le courriel - ou le SMS – ou le message vocal frauduleux de votre boîte de messages.

3. En savoir plus

Pour en savoir plus sur le piratage informatique de type « phishing », ou « filoutage », et pour mieux vous en prémunir, vous pouvez consulter le site de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)