MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Groupement de gendarmerie départementale de la Somme

11 juin 2024

ALERTECYBERGEND

Plusieurs cas d'usurpation du nom de la DGCCRF à des fins malveillantes ont récemment été signalés aux autorités. Si les techniques utilisées diffèrent, l'objectif des usurpateurs est toujours de vous extorquer de l'argent.

POINT DE SITUATION

Ce vendredi 7 juin 2024, une entreprise samarienne est destinataire d'un mail dont l'expéditeur usurpe l'identité de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) en vue de lui dérober des informations et de l'argent.

La vigilance de ses responsables a permis de déjouer la tentative d'escroquerie.

MODES OPÉRATOIRES

Cette arnaque peut se dérouler de plusieurs manières :

- ➔ Vous êtes contacté par une personne se prétendant de la répression des fraudes ou de la DGCCRF. Elle vous informe que votre carte bancaire a été « repérée » ou que des achats ont été effectués avec elle sans votre consentement. La personne énumère alors des numéros de cartes bancaires afin que vous identifiiez la vôtre.
- ➔ Vous recevez un SMS du « service des fraudes » vous informant qu'un paiement par carte bancaire est en cours, et qu'il est impératif de contacter un numéro non surtaxé en urgence. Il est mentionné que si vous ne répondez pas dans les 45 minutes, le paiement sera validé.
- ➔ Une personne se faisant passer pour un agent de la répression des fraudes vous informe que votre carte bancaire a été utilisée à l'étranger et qu'il lui faut un code que vous venez de recevoir par SMS pour bloquer cette transaction. Si vous communiquez ce code, vous validez en réalité un paiement que l'escroc vient d'initier à votre insu.

CONSEILS PRÉVENTIFS

Pour vous prémunir de ces mails frauduleux de plus en plus élaborés, nous vous invitons à la prudence :

- ✔ **Ne jamais répondre par téléphone à ce type de sollicitation** : dans le cas présent, les enquêteurs de la DGCCRF ne contactent jamais les consommateurs de cette manière. Ils n'ont pas lieu de vous demander un code SMS ou votre numéro de carte bancaire. Tous ces **agissements** doivent vous **alerter** ;
- ✔ **Ne pas réagir à chaud** : les escrocs envoient des messages alléchants ou apeurants. Ils jouent sur les **émotions** et incitent à réagir dans l'**urgence**. Il est primordial de **vérifier l'authenticité** d'un mail avant de faire quoi que ce soit ;
- ✔ **En cas de doute, remonter à la source** : vous recevez un mail qui vous semble officiel, avec un logo et une présentation plus vraie que nature, pourtant vous avez tout de même des doutes sur sa fiabilité. Le plus **prudent** est d'aller **directement** sur le site de l'expéditeur en passant par votre **moteur de recherche** afin de voir en vous connectant à votre compte si ce qui est avancé est vrai ;
- ✔ **Prendre les précautions de base pour se protéger (logiciel, mot de passe…)** : nous vous recommandons d'utiliser un **filtre** ou un **logiciel anti-spam** pour vous prémunir de la majorité des courriels frauduleux. Autre conseil : utiliser des **mots de passe complexes et différents**. Ainsi, si l'un de vos comptes est compromis (votre adresse mail personnelle par exemple), cela évitera de compromettre les autres (votre messagerie professionnelle qui aurait le même mot de passe) ;
- ✔ **Veiller ses SMS** : les hackers procèdent désormais aussi par sms. Ils envoient le même message à 50.000 personnes et attendent de voir qui mord à l'**hameçon**. C'est plus coûteux qu'un mail mais cela leur permet de contourner la problématique du filtre spam ;
- ✔ **Être toujours en alerte** : le manque de **vigilance** peut vous conduire à faire un faux pas.