ATTENTION : pseudo demande de Serafe, qui s'avère être du hameçonnage

2025-12-05 - Florian Cattin - Commentaires (0) - Services Prime

Un e-mail d'hameçonnage circule actuellement **au nom** de l'organe suisse de perception de la redevance radio-télévision **Serafe**. Sous prétexte de devoir vérifier la situation actuelle du ménage, les cybercriminels cherchent à obtenir toute une série d'informations.

Leur objectif est de collecter les données en plusieurs étapes, en commençant par le numéro AVS et en terminant par la carte de crédit», indique l'Office fédéral de la cybersécurité (OFCS).

Concrètement, les victimes reçoivent un message avec un lien sur une page web falsifiée.

Puis, étape par étape, il est demandé d'indiquer des données personnelles: numéro de téléphone, adresse mail, date de naissance, jusqu'au numéro AVS et à des informations sur la carte de crédit

L'Office fédéral de la cybersécurité précise que l'utilisation frauduleuse du nom de Serafe n'a rien d'un hasard. «Lorsque des messages électroniques frauduleux sont envoyés au nom d'une entreprise, le taux de réussite dépend généralement du fait que la victime ait effectivement une relation client avec l'entreprise ou l'autorité concernée : le message semble ainsi plausible», est-il expliqué.

Recommandations

Voici les rappels et conseils de l'OFCS pour ne pas se faire avoir:

- L'entreprise Serafe ne demande jamais de vérifier votre situation par courrier électronique, ni de donner votre numéro AVS ou vos données de cartes de crédit.
- Serafe reçoit les données nécessaires directement du contrôle des habitants de votre commune de domicile (p. ex. déménagement). Il n'est donc pas nécessaire pour vous de les annoncer.
- Ne communiquez jamais de données sensibles sur un site auquel vous accédez par un lien obtenu dans un courriel.
- Les méthodes de paiement officielles de Serafe sont eBill, le système de recouvrement direct ou le bulletin de versement.
- Pour vérifier l'adresse cible d'un lien, passez la souris dessus sans cliquer.
- Annoncez les messages électroniques suspects à l'OFCS.

Source : OFCS