Attention aux mails frauduleux semblant provenir de Service-Public.fr !

Publié le 01 avril 2021 - Direction de l'information légale et administrative (Premier ministre)

Vous avez reçu un mail qui utilise le logo de *Service-Public.fr* et qui vous alerte sur une nouvelle version de la carte vitale ? Ce courriel vous invite à cliquer sur une page et à renseigner vos données personnelles pour obtenir votre nouvelle carte vitale ? Soyez vigilant, ces mails n'émanent pas de *Service-Public.fr* et il ne faut en aucun cas y donner suite.

Comment reconnaître un mail frauduleux ?

Il s'agit de tentatives d'escroqueries appelées phishing (ou hameçonnage). Ces mails, souvent alarmistes, usurpent le nom et le logo de *Service-Public.fr*. Ils vous incitent à livrer des données personnelles (carte d'identité, passeport, permis de conduire, carte vitale). Ces données seront ensuite récupérées par l'auteur du phishing qui les utilisera pour effectuer des achats ou des opérations bancaires. Par exemple, ils peuvent proposer un service en ligne payant de mise à jour de la carte vitale. En vérité, la mise à jour peut se faire gratuitement dans la plupart des pharmacies et sur les bornes dans les points d'accueil de l'Assurance maladie.

Service-Public.fr ne demande pas d'argent, n'en rembourse pas et ne cherche jamais à recueillir des coordonnées bancaires. *Service-Public.fr* peut néanmoins vous envoyer un mail (abonnement à des alertes, suivi d'une démarche...).

D'une manière générale, prenez garde lorsque vous recevez un mail vous invitant à remplir un formulaire afin de changer de carte vitale où l'expéditeur :

- vous demande de l'argent ou propose de vous rembourser une somme d'argent ;
- cherche à recueillir des informations personnelles (coordonnées bancaires, état-civil...).

Que faire du message ?

Il ne faut pas répondre au mail ni cliquer sur le lien contenu dans le message mais détruire le message.

Si vous avez déjà répondu à un message frauduleux en donnant vos coordonnées bancaires, vous devez avant tout faire opposition auprès de votre banque.

Comment signaler ces mails frauduleux ?

Vous pouvez signaler ces tentatives de phishing :

- sur le site Phishing Initiative (https://www.service-public.fr/particuliers/vosdroits/R47282) . Ce signalement permettra d'alimenter les bases de référence des principaux navigateurs pour bloquer l'accès à ces sites ;
- aux services de police sur le site internet signalement (Pharos (https://www.service-public.fr/particuliers/vosdroits/R17674)) ;
- à Info Escroqueries par téléphone au 0 805 805 817 numéro vert (appel gratuit depuis la France) du lundi au vendredi de 9h à 18h30.

Où s'informer ?

- Info Escroqueries

  Par téléphone

  0 805 805 817

  Du lundi au vendredi de 9h à 18h30.

  Numéro vert (appel gratuit depuis la France).

Services en ligne et formulaires

- Signaler un site de phishing (https://www.service-public.fr/particuliers/vosdroits/R47282)
  Téléservice
- Signaler un contenu internet illégal (internet-signalement : Pharos) (https://www.service-public.fr/particuliers/vosdroits/R17674)
  Téléservice

Et aussi

- Phishing (hameçonnage) (https://www.service-public.fr/particuliers/vosdroits/F34800)

Pour en savoir plus

- Multiplication des fraudes par sms, appels ou courriels (https://www.ameli.fr/paris/assure/actualites/multiplication-des-fraudes-par-sms-appels-ou-courriels)
  Caisse nationale d'assurance maladie (Cnam)
- Phishing (hameçonnage) (https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage)
  Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)