ARNAQUES, SMS, APPELS ET MAILS FRAUDULEUX : SOYEZ VIGILANTS !

Vous avez déjà probablement entendu le terme « phishing » ou encore « hameçonnage » qui consiste en « *une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.* » Ces derniers mois plusieurs alertes ont été lancées. Quelles sont-elles ? Comment les identifier ? Comment dénoncer un abus ? La Fédération vous éclaire.

L'arnaque au renouvellement de la carte vitale

Le procédé est le suivant : vous recevez un sms sur votre téléphone vous indiquant que votre nouvelle carte vitale est disponible. Vous êtes ensuite invité à cliquer sur un lien puis vous êtes redirigés vers plusieurs pages internet dans lesquelles il vous est demandé de renseigner un certain nombre d'informations personnelles.

L'arnaque peut s'arrêter ici, vous avez été victime d'un vol de données personnelles.

Attention ! Le piège peut se poursuivre : une fois vos données collectées frauduleusement, vous pouvez recevoir un appel d'un faux conseiller bancaire qui vous informera que votre carte bancaire a fait l'objet d'un piratage et que pour bloquer les paiements, vous devez lui transmettre les codes que vous venez de recevoir par sms. Il s'agit bien entendu d'une arnaque destinée au contraire à valider les paiements.

Usurpation de l'identité de l'Agence Nationale de Sécurité du Médicament et des Produits de Santé (ANSM)

Afin d'obtenir des données sensibles telles que votre numéro de sécurité sociale, vos données bancaires ou vos mots de passe, vous recevez des appels ou des mails frauduleux de personnes utilisant l'identité de l'ANSM. Communiquer ses informations personnelles sans s'assurer de l'identité réelle de l'interlocuteur représente un risque considérable, d'autant plus que les données concernées peuvent toucher différents services publics.

Les conseils

- Ne communiquez jamais vos données personnelles par mail, par téléphone, sans être certain de la fiabilité de la demande.
- Si la sollicitation provient d'une institution ou d'une administration, renseignez vous directement auprès d'elle afin de vous assurer de son authenticité.
- Si vous avez déjà été piégé, faites immédiatement opposition auprès de votre banque et pensez à porter plainte. A défaut, vous ne pourrez pas faire de demande de remboursement auprès de votre banque.

Faites un signalement de l'escroquerie sur le portail du gouvernement Cybermalveillance.gouv ou sur Pharos (Portail officiel de signalement des contenus illicites de l'internet).

- Vous pouvez aussi faire un dépôt de plainte en ligne directement sur la plateforme Thésée dédiée aux arnaques sur internet ou signaler une fraude à la carte bancaire sur le site Perceval.

#Gardons le contact

Adèle est à votre écoute au service juridique si vous vous posez des questions sur la poursuite de votre activité professionnelle dans de bonnes conditions, si vous avez des difficultés d'accès aux soins, si votre permis de conduire arrive à expiration, ou encore si vous avez des questions sur l'assurance. La permanence téléphonique est ouverte au 01-40-09-24-25 le mardi de 8h à 12h30 et le jeudi de 13h30 à 18h et aussi par mail : juriste@federationdesdiabetiques.org.