Ne répondez pas directement aux e-mails
Résistez au réflexe de répondre aux e-mails de phishing. Même si vous répondez sans donner d'informations, vous risquez de recevoir davantage de spam à l'avenir.

Ne donnez pas d'informations privées par e-mail, téléphone ou SMS
Lorsque vous partagez des données personnelles, pensez toujours à leur destinataire et au but visé. Il est donc recommandé de ne jamais fournir de mots de passe, d'informations de connexion ou de données financières à quiconque par téléphone, SMS ou e-mail, même si la demande semble légitime.

Que faire si vous êtes victime d'un phishing

Si vous êtes victime d'un e-mail frauduleux, suivez ces conseils :

Pas de panique : gardez votre calme pour gérer la situation avec lucidité et en atténuer les conséquences.

Modifiez votre mot de passe : votre mot de passe est la clé de votre compte, de vos informations personnelles et financières qu'il contient. Si vous pensez que votre mot de passe a été compromis, remplacez-le immédiatement par une chaîne de caractères longue.

Informez votre banque : certains comptes sont souvent liés à des comptes bancaires, il est donc important d'informer votre banque de la situation. De cette façon, elle peut geler tous les achats non vérifiés et éventuellement aider à arrêter les pirates.

Faites opposition à toutes les cartes bancaires compromises : toutes les cartes bancaires associées à votre compte sont en danger. Par précaution, Faites opposition.

Informez le prestataire : en signalant l'escroquerie au prestataire, vous lui permettrez de sécuriser à nouveau votre compte, de sensibiliser le public afin d'éviter que d'autres personnes en soient victimes et de l'aider à développer des outils et des procédures pour mettre fin aux futures attaques de phishing.