



Les fraudes et autres risques liés à la sécurité en ligne constituent un problème croissant. Nous devons rester prudents et apprendre à les identifier. D'où l'importance de prendre le temps de s'y arrêter, de regarder et de réfléchir. Voici quelques conseils pour utiliser internet et vos appareils mobiles de façon plus sécurisée.



What is phishing?



GDPR Information



Tips for Safer Banking

Qu'est-ce que le hameçonnage ?

Le hameçonnage, ou *fishing* en anglais, est une tactique utilisée par des fraudeurs pour vous soutirer des renseignements personnels. Elle consiste par exemple à envoyer des liens ou fichiers malveillants, généralement par courrier électronique.

Caractéristiques du hameçonnage :

- ⚠ Demande de données personnelles
- ⚠ Pièces jointes suspectes
- ⚠ Sentiment d'urgence
- ⚠ Trop beau pour être vrai

Comment éviter le hameçonnage ?

- ✓ Vérifiez l'adresse de l'expéditeur
- ✓ Faites glisser la souris sur les éventuels liens et vérifiez s'ils ont un rapport avec l'entreprise en question
- ✓ Interrogez l'expéditeur via un autre canal, par exemple le téléphone

Vous avez reçu un SMS ou un e-mail suspect ?

Si l'on vous contacte de façon suspecte par téléphone, par e-mail ou par SMS, soi-disant au nom de MeDirect :

- ⊖ Ne réagissez pas au SMS ou à l'e-mail

🚫 N'ouvrez aucune pièce jointe et ne cliquez pas sur les liens URL présents dans l'e-mail

☎️ Contactez-nous au 02 518 00 00. Les informations que vous nous donnerez nous aideront à lutter contre la fraude financière.

Conseils pour des opérations bancaires plus sûres



Mettez à jour vos logiciels

Effectuez les mises à jour de votre système d'exploitation et de vos applications chaque fois que vos fournisseurs émettent de nouvelles solutions ou améliorations. N'utilisez sur vos appareils que des logiciels disponibles auprès d'un point de vente officiel.

Installez un antivirus

Un antivirus spécial est important pour protéger votre ordinateur et sécuriser vos opérations bancaires en ligne. Installez un antivirus et un pare-feu sur votre ordinateur et mettez-les régulièrement à jour. Scannez régulièrement votre ordinateur.

Ne communiquez jamais vos données personnelles

MeDirect ne vous demandera jamais votre mot de passe ni votre code pin. Ne partagez jamais les détails de votre mot de passe, avec qui que ce soit. Si possible, recourez toujours à l'authentification multifacteur (vérification multiple).

Effectuez des back-ups

Veillez à faire des back-ups de votre ordinateur. Il existe diverses solutions dans le cloud. Vous pourrez ainsi récupérer vos données en cas de perte ou de vol de votre appareil.

Prudence avec les téléchargements

Ne téléchargez aucun programme sur des sites internet inconnus ou non fiables si vous n'êtes pas certain que l'opération soit sans danger.

Évitez d'utiliser le WiFi public

Usez du WiFi public avec prudence. N'ouvrez pas de sites internet sensibles sur le WiFi public pour vos opérations bancaires en ligne, par exemple, à moins d'être certain que le réseau est sécurisé.

Verrouillez votre appareil

Veillez à protéger votre appareil au moyen d'un mot de passe sécurisé et ne le laissez jamais déverrouillé sans surveillance. Utilisez de préférence des fonctions biométriques, comme l'empreinte digitale ou la reconnaissance faciale.

RGPD



Qu'est-ce que le RGPD ?

Le Règlement général sur la protection des données (RGPD) prévoit une série de mesures destinées à protéger les données des citoyens européens. Il s'agit d'une révision de la législation européenne de 1995, la Directive sur la protection des données. Le RGPD poursuit un double objectif : protéger la vie privée des citoyens européens, mais aussi leur donner plus de droits sur l'usage qui est fait de leurs données personnelles. Le RGPD est entré en vigueur le 25 mai 2018.

Protection de vos données personnelles

MeDirect veille à stocker l'intégralité des données personnelles en toute sécurité. Afin de protéger vos données personnelles contre la perte ou l'abus, nous avons mis en œuvre la technologie nécessaire et en assurons régulièrement la mise à jour.

Une convention contractuelle garantit que les tiers offrant un service à MeDirect suivent les procédures de sécurité réglementaires visant à protéger vos données personnelles, par exemple en utilisant des informations cryptées. Les données personnelles ne sont transmises à

des tiers qu'aux fins stipulées dans nos accords avec les clients et/ou dans nos conditions générales.

Que prévoit notre politique de confidentialité ?

Nous avons adapté notre [politique de confidentialité](#) conformément à la législation du RGPD. Cette politique de confidentialité précise quelles sont les données que nous récoltons sur chaque individu, pourquoi nous le faisons et avec quelles parties nous les partageons. La politique de confidentialité fixe également vos droits et indique qui contacter chez MeDirect pour toutes vos questions relatives à la protection des données personnelles.

Quelles mesures a prises MeDirect pour respecter cette législation ?

Diverses actions ont été entreprises pour protéger nos clients et collaborateurs, telles que :

- L'adaptation de notre politique de confidentialité.
- La formation de tous nos collaborateurs en matière de vie privée.
- La modification de nos conditions générales et de notre politique de cookies.
- La formation de nos collaborateurs en matière de demandes RH.
- La révision de la manière dont nous demandons aux personnes si elles souhaitent être informées de nos offres commerciales et lettres d'information.

- La révision de notre politique interne afin qu'elle respecte les directives du RGPD.