Compte piraté, que faire ?

C'est le cauchemar de tout client bancaire : se faire dévaliser son compte par des escrocs. Si l'irréparable s'est déjà produit, il s'agit de limiter les dommages et d'en tirer les leçons.

Que faire si je constate un accès non autorisé à mon compte bancaire :

- En cas de transactions suspectes ou d'erreurs lors de votre connexion aux services d'e-banking, prévenez immédiatement votre banque et faites bloquer le contrat d'e-banking concerné ainsi que vos comptes et cartes de crédit.
- Coupez la connexion au réseau Internet de tous les dispositifs ayant pu être piratés par des hackers ou infectés par des malwares et éteignez-les, ou mettez-les en mode avion. Cependant, ne procédez pas tout de suite à la réinitialisation de vos appareils dans la mesure où ils pourraient servir à l'enquête de la police.
- Changez vos mots de passe depuis un autre dispositif n'ayant pas été infecté. Mettez en place à chaque fois que cela est possible la méthode d'authentification forte à deux facteurs.
- Si l'escroquerie est avérée, portez plainte à la police. Notez le plus d'informations possibles sur la fraude ou l'attaque.
- À l'avenir, protégez-vous contre les accès non autorisés en appliquant nos « 5 mesures pour votre sécurité numérique » ainsi que nos conseils pour un e-banking en toute sécurité.

Comment mon compte a-t-il pu être piraté ?

Les portails d'e-banking des instituts bancaires suisses sont très bien protégés contre les attaques de hackers. On peut donc aujourd'hui exclure que des criminels puissent accéder aux systèmes informatiques d'une banque.

Mais un client bancaire négligeant peut représenter une vulnérabilité : si des hackers réussissent à se procurer ses identifiants de connexion, ils seront en mesure d'ouvrir une session d'e-banking à son nom et d'engager des transactions ou d'accéder à des informations confidentielles. C'est ce qui peut arriver par exemple à la suite à d'une attaque de hameçonnage (https://www.ebas.ch/fr/le-phishing/) ou d'une infection par un malware (https://www.ebas.ch/fr/les-infections-par-malware/) spécifique. Dans ce cas, il ne reste plus à la victime que d'essayer de limiter les dégâts.

Que dois-je faire si je suis victime d'un préjudice ?

Première chose : en cas de doute, il faut réagir vite ! Si l'escroquerie est avérée, vous devez immédiatement bloquer le contrat d'e-banking concerné et les comptes correspondants, afin d'empêcher d'autres sorties de fond.

Si vous pensez avoir été victime d'une escroquerie, en cas de transactions suspectes par exemple ou d'une erreur de connexion à votre session d'e-banking, il faut toujours prévenir votre institut financier afin de décider ensemble de la marche à suivre. Si l'escroquerie est confirmée, portez plainte à la police.

Si même après avoir consulté votre institut financier, vous ne parvenez toujours pas à déterminer comment les criminels ont réussi à opérer sur votre compte, vous devez partir du principe que des étrangers sont en possession de vos identifiants et que votre dispositif a été infecté par un logiciel malveillant, probablement un cheval de Troie bancaire.

Pour éviter que les identifiants supposés volés soient à nouveau utilisés à des fins illicites, vous devez, par mesure de précaution, changer le mot de passe (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) de votre boîte de messagerie électronique, mais aussi de tous vos comptes en ligne, mais en prenant garde de ne pas le faire depuis l'ordinateur ou le dispositif mobile potentiellement infecté, mais en utilisant un autre appareil. Votre accès à l'e-banking ayant d'ores et déjà été bloqué, ce changement de mot de passe ne devra être effectué que dans un deuxième temps, lorsque la situation aura été tirée au clair avec votre banque.

Afin d'augmenter le niveau de protection de vos comptes en ligne, l'idéal est, lorsque cela est possible, de mettre en place un système d'identification à deux facteurs.

Vous devez par ailleurs couper la connexion Internet de votre dispositif, ou le mettre en modalité avion, et ne la réactiver (https://www.ebas.ch/fr/reinstallation-de-windows-10/) que dans le cadre d'une éventuelle enquête de police.

Dernier point, mais non des moindres, vous allez devoir à l'avenir vous protéger efficacement contre les prochaines tentatives d'escroquerie. Pour cela, vous devrez commencer par suivre scrupuleusement les « 5 règles pour votre sécurité numérique » (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) , de même que nos conseils pour un e-banking en toute sécurité (https://www.ebas.ch/fr/conseils-pour-un-e-banking-en-toute-securite/) . En adoptant les bonnes mesures de prévention, vous couperez ainsi l'herbe sous le pied des hackers !

Mesures à prendre immédiatement en cas de doute :

- *prévenir la banque et demander le blocage du compte*
- *couper l'accès Internet*
- *changer les mots de passe*
- *porter plainte*

Les banques sont-elles en mesure de reconnaître et de stopper une opération illégitime ?

Certains instituts financiers à se doter de systèmes de détection des fraudes censés signaler toute transactions suspecte, voire même de la bloquer automatiquement. Bien qu'ils soient de plus en plus perfectionnés, ces systèmes ne permettent pas de garantir une sécurité à 100%, d'autant plus que de leur côté, les escrocs font preuve de plus en plus d'habileté et de discrétion pour déjouer leur surveillance.

À vous donc de prendre vos responsabilités et de ne pas partir du principe que votre banque est en mesure de protéger vos comptes, quoi qu'il arrive, contre tout accès non autorisé, comme cela peut être le cas par exemple d'une attaque de phishing.

Qui est responsable en cas de préjudice ?

La question de la responsabilité ne peut être résolue une fois pour toute et doit être évaluée au cas par cas. En effet, il ne s'agit pas seulement de déterminer à qui attribuer la faute, mais de savoir qui n'a pas rempli son devoir de diligence.

Dans la mesure où les malfaiteurs restent la plupart du temps inconnus et qu'ils opèrent généralement depuis l'étranger, il est souvent difficile de mener une véritable enquête criminelle. Il s'agit souvent d'intermédiaires ignares, ces fameux « passeurs d'argent » ou « Money mules » (https://www.ebas.ch/fr/money-mules-agents-financiers/) , utilisés pour dissimuler les transactions. Dans la plupart des cas, l'argent est alors perdu.

En principe, aussi bien les instituts financiers que leurs clients doivent remplir leur devoir de diligence dans la gestion des comptes bancaires et des sommes qui y sont déposées. Un tribunal s'attachera donc à examiner tout manquement à ce devoir, qui peut parfois être imputé au client, dans le cas par exemple où celui-ci a communiqué ses identifiants de connexion à un tiers, consciemment ou inconsciemment.

Pour éviter d'être confronté à ces questions de responsabilité, mieux vaut donc prévenir et protéger votre compte (https://www.ebas.ch/fr/conseils-pour-un-e-banking-en-toute-securite/) !