29.07.2020

Attention aux ordres de paiement transmis par email !

Un nouvel arrêt de la Cour suprême fédérale fait beaucoup parler de lui. Un client se fait dévaliser son compte par des escrocs et sa banque n'est pas retenue responsable. Mais il est possible de se protéger contre de tels incidents fâcheux.

Pour Jean-Claude Henchoz (nom modifié), le verdict est tombé comme un couperet : le Tribunal fédéral a décidé que ce client d'une banque privée genevoise devait payer pour les dommages que lui ont causé des pirates informatiques et ce, alors que le tribunal cantonal de première instance avait ordonné à la banque de rembourser à Henchoz une grande partie de ses pertes, à hauteur de plusieurs centaines de milliers d'euros.

Les criminels avaient réussi à accéder au compte email de la victime et l'avaient utilisé pour transmettre à sa banque plusieurs ordres de paiement à effectuer sur des comptes étrangers. Le hic, c'est que le contrat passé entre la banque et son client autorisait la transmission d'ordres de paiement par courriel, téléphone et fax, sans autre formalité écrite. Les hackers en ont donc profité pour réaliser des virements à leur attention.

Alors que le Tribunal cantonal de Genève avait établi que la banque aurait dû remarquer et bloquer plus tôt ces paiements frauduleux, le tribunal fédéral a estimé pour sa part que la banque n'avait commis aucune faute dans la mesure où les ordres de paiement transmis par email conformément aux conditions contractuelles ne devaient pas être considérés à priori comme potentiellement frauduleux et ne nécessitaient par conséquent aucune surveillance particulière. C'est en revanche au client que la cour a attribué le risque lié au problème d'identification et de transmission.

Voici donc quelques recommandations à suivre pour vous protéger contre ce genre de pertes liées à des virements frauduleux :

- Pour vos ordres de paiement, utilisez si possible exclusivement l'e-banking ou l'application de banque mobile de votre banque, ou rendez-vous personnellement au guichet et bloquez tous les autres canaux proposés par contrat (email, téléphone et fax).
- Si vous ne pouvez pas faire autrement, utilisez un fournisseur de courrier électronique qui offre une authentification à deux facteurs et profitez de cette protection supplémentaire.
- Utilisez des mots de passe complexes différents pour chacun de vos comptes de messagerie et autres (e-banking, etc.), et conservez-les de manière sécurisée (p. ex. dans un gestionnaire de mots de passe) et ne le transmettez jamais à personne.
- Créez une adresse de courrier électronique dédiée à vos communications avec votre banque. Ne l'utilisez pas à d'autres fins et communiquez-la uniquement à votre banque.
- Demandez à votre banque de mettre en place si possible un système d'autorisation des transactions pour que les virements dépassant un certain montant ne puissent être approuvés sans votre accord explicite via un autre canal (par exemple le téléphone).

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

- Vérifiez régulièrement vos extraits de compte et avertissez immédiatement votre banque en cas d'anomalie.

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique