

Usage frauduleux de votre CB : communiquer vos données est une négligence grave !



Service-Public.fr



Usage frauduleux de votre CB

Communiquer vos données est une négligence grave, même en cas de phishing !



Cour de Cassation, 28/03/2018

Usage frauduleux de votre CB : communiquer vos données est une négligence grave !

De plus en plus d'arnaques sophistiqués voient le jour. Il est impératif de sensibiliser les personnels administratifs des sociétés aux risques auxquels ils pourront être exposés dans le cadre de leur activité au sein de leur entreprise de transport routier. Ci-dessous est abordé le cas sensible de la transmission des coordonnées bancaires par courrier électronique. Ne transmettez jamais vos coordonnées bancaires à une demande faite par courrier électronique. Il faut toujours vérifier l'adresse électronique destinataire d'informations sensibles (contrat, bon de commande, coordonnées bancaires...) afin de ne pas répondre à quelqu'un qui se ferait passer pour un interlocuteur habituel de votre société...

Phishing : négligence fautive du client de la banque

Dans une décision du 28 mars 2018, la Cour de cassation a retenu la négligence grave du client

victime de phishing, pour écarter la responsabilité de la banque.

Le client réclamait à sa banque le remboursement des sommes débitées sur ses comptes. Il invoquait le caractère frauduleux des paiements par carte bancaire et par virement.

La banque s'était opposée à ses demandes en lui reprochant une négligence grave dans la garde et la conservation de ses données personnelles du dispositif de sécurité des instruments de paiement. Le client avait reçu des courriels portant le logo parfaitement imité de sa banque, accompagnés d'un « certificat de sécurité à remplir attentivement » qu'il avait scrupuleusement renseignés. Il avait même demandé à la banque la communication de sa nouvelle carte de clefs personnelle pour pouvoir renseigner complètement le certificat.

La cour d'appel avait ordonné le remboursement des sommes au client considérant que seul un examen vigilant des adresses internet changeantes du correspondant ou certains indices comme les fautes d'orthographe du message, étaient de nature à l'alerter.

Mais l'arrêt est cassé. La Cour de cassation a considéré que le client avait commis une négligence grave. Pour la Cour, l'utilisateur d'un service de paiement qui communique les données personnelles du dispositif de sécurité en réponse à un courriel contenant des indices permettant à un utilisateur normalement attentif de douter de sa provenance, manque à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité.

[Textes de référence : Cour de cassation, Chambre commerciale, 28 mars 2018, 16-20018, Publié au bulletin](#)