

Phishing

Le phishing consiste à tenter d'obtenir, par l'envoi de faux courriels ou le recours à de faux sites web, des données personnelles de consommateurs, telles que des numéros de comptes bancaires, des numéros de cartes de crédit, des mots de passe, des codes d'accès, des codes PIN, etc. Il peut également arriver qu'un consommateur soit contacté par téléphone par une personne se présentant abusivement comme un collaborateur de sa banque afin de lui demander des données personnelles.

Une fois en possession de ces données, le fraudeur peut se faire passer pour sa victime et retirer de l'argent du compte de celle-ci.

Quelques conseils pour ne pas être victime de phishing :

- Sécurisez votre ordinateur.
- Ne communiquez pas à autrui le code PIN ou le code d'accès que vous utilisez lors de vos opérations bancaires par internet ; ne le faites pas non plus lors d'un contact téléphonique avec une personne qui se présente comme un collaborateur de votre banque et que vous ne connaissez pas.
- Ne confirmez pas par internet des virements que vous n'avez pas préparés vous-même ou que vous avez reçus de manière inattendue.
- Lorsque vous effectuez un paiement par carte bancaire, par carte de crédit ou via votre PC et que vous avez l'impression que quelque chose ne se passe pas comme prévu, annulez ce paiement. En cas de doute, arrêtez toujours le paiement immédiatement.

Vous trouverez sur le site web de Febelfin, la Fédération belge du secteur financier, d'autres informations utiles sur le phishing : comment repérer un message de phishing et quelles sont les règles de sécurité à respecter (www.febelfin.be, rubrique Safe internetbanking).

Source URL: <https://www.fsma.be/fr/phishing>