



CC 18 C



RÉGLEMENTATION - JURIDIQUE



Avez-vous été victime d'une escroquerie par faux conseiller bancaire ?

Reconnaître une escroquerie par faux conseiller bancaire

Aline reçoit un appel téléphonique de son conseiller bancaire qui l'a mis en garde d'une transaction frauduleuse sur son compte. Le conseiller bancaire demande à Aline, son identité en lui faisant valider des informations personnelles une à une. Puis, ce conseiller bancaire demande à Aline de se rendre sur son application bancaire et d'annuler les transactions avec lui. Aline s'aperçoit à la fin de l'appel que les transactions en question ont été prélevées de son compte. Aline vient d'être victime d'une escroquerie par faux conseiller bancaire.

Qu'est-ce qu'une escroquerie au faux conseiller bancaire ?

Les cybercriminels envoient un faux formulaire administratif, ils recueillent les informations de la victime. Quelques jours après, l'escroc contacte la victime et se fait passer pour un conseiller bancaire. Il rassure la victime en validant son identité à l'aide des informations qu'il a recueillies sur elle au préalable grâce au formulaire. Une fois qu'il a gagné la confiance de la victime, il l'invite à annuler les virements frauduleux directement via son application bancaire. Mais en réalité, cela permet à l'escroc de valider les transactions frauduleuses qu'il est en train d'effectuer sur le compte de la victime.

Comment réagir si vous êtes victime d'une escroquerie au faux conseiller bancaire ?

Il est important de suivre les 7 étapes suivantes :

- Étape n°1 : ne paniquez pas.
- Étape n°2 : faites opposition à votre carte bancaire en contactant le 0 892 705 705 (service ouvert 7 jours sur 7, 24h sur 24) et alertez votre banque.
- Étape n°3 : changez les codes de confidentialité sur votre compte bancaire et changez les mots de passe de vos boîtes mails.
- Étape n°4 : identifiez les transactions frauduleuses sur votre application bancaire.
- Étape n°5 : gardez les preuves et signalez les faits sur Perceval, un service accessible via [FranceConnect](#) pour signaler une fraude à la carte bancaire.
- Étape n°6 : déposez plainte à la gendarmerie ou au commissariat de votre secteur et laissez une copie de toutes preuves aux forces de l'ordre. Déclarez l'infraction en ligne directement via le lien : [Porter plainte et signaler une infraction en ligne.](#)
- Étape n°7 : assurez-vous que tous vos appareils sont protégés en utilisant des scans d'antivirus, des mots de passe sécurisés, en mettant à jour tous vos logiciels et en vérifiant la sécurité de vos comptes.
- Étape n°8 : renseignez-vous sur les actualités en matière de cybersécurité à l'aide du site : [cybermalveillance.gouv.fr](#)

Que faire afin de vous protéger des escroqueries par faux conseiller bancaire ?

- Ne communiquez pas vos mots de passe et vos identifiants.
- Vérifiez les informations lorsqu'elles viennent de l'extérieur.
- Méfiez-vous des appels et des SMS de numéro inconnu.

Que faire pour sécuriser mes appareils connectés en cas d'escroquerie ?

- Effectuez les mises à jour de vos appareils connectés et un scan antivirus.
- Modifiez vos mots de passe de manière régulière et utilisez des mots de passe sécurisés.
- N'installez pas d'application provenant de sites non fiables.
- Ne fournissez aucune donnée confidentielle lorsque la démarche ne vient pas de vous.

Source : Newsletter La Poste - mai 2024.

Amicalement