VIROFLAYSIENS VIGILANTS
Participation Citoyenne

Fraudes à la carte bancaire

Comment protéger vos données contre la fraude à la carte bancaire ?

- **Ne prêtez votre carte à personne**, même à l'un de vos proches : elle est strictement personnelle ;
- **Conservez votre carte dans un lieu sûr** et vérifiez régulièrement qu'elle est en votre possession. Par exemple, ne la laissez jamais dans votre véhicule ;
- **Apprenez votre code confidentiel par cœur** et ne l'écrivez pas ;
- **Cachez le clavier** du terminal ou du distributeur lors vous effectuez une opération ;
- **Signez votre carte bancaire** dès sa réception. Vous éviterez ainsi qu'un fraudeur appose sa propre signature en cas de perte ou de vol par exemple ;
- **Surveillez vos relevés de compte** régulièrement. Dans le cas où figurerait une opération que vous n'avez pas autorisée, contestez-la immédiatement auprès de votre banque ;
- **Ne communiquez jamais vos données bancaires** (numéro de carte ou autres) ou un code d'authentification en réponse, notamment, à un courriel, même s'il semble provenir : d'une administration ou d'une banque ; d'un appel téléphonique lorsque votre interlocuteur indique, par exemple, être au service de votre banque et propose de débloquer votre compte ou de le sécuriser ; d'un sms contenant, ou non, un lien vers un site internet ;
- Chez un commerçant, **ne quittez jamais votre carte des yeux** et vérifiez le montant affiché par le terminal avant de valider l'opération ;
- Lors de retraits à un distributeur de billets, **ne vous laissez pas distraire par des inconnus**.

Comment sécuriser vos paiements à distance par carte bancaire?

- Vous ne devez jamais saisir votre code confidentiel à 4 chiffres pour ce type de transaction. En revanche, la saisie du **cryptogramme (code à 3 chiffres au dos de la carte)** peut être demandée. Ce code est donc **à protéger soigneusement** ; Quel qu'en soit le motif, ne communiquez jamais le code d'authentification reçu sur votre mobile à un interlocuteur vous ayant contacté par téléphone ou par courriel ;
- Ne confirmez jamais un paiement en cliquant sur un lien reçu. Vérifiez l'URL de l'adresse du commerçant à chaque étape ;
- Lorsque votre paiement est soumis à l'authentification forte, ne vous connectez pas à votre Espace Client à partir d'un lien reçu par courriel ou par sms. **Privilégiez une connexion à partir de votre application bancaire ou d'une nouvelle page internet que vous aurez ouverte séparément**.

En cas d'agression ou si vous remarquez un comportement étrange : appelez le 17

VIROFLAYSIENS VIGILANTS
Participation Citoyenne

Comment protéger vos retraits d'espèces avec votre carte bancaire ?

- **Composez toujours votre code confidentiel à l'abri des regards indiscrets**, ne le communiquez à personne ;
- Privilégiez les distributeurs équipés de caméras de surveillance ou situés à l'intérieur des agences ;
- Placez votre main au-dessus du clavier lorsque vous tapez votre code ;
- Si votre carte est avalée par le distributeur alors que vous n'avez pas saisi de code confidentiel, rentrez dans l'agence pour le signaler à un employé en gardant, si possible, un œil sur la machine. En cas d'impossibilité (retraits en dehors des heures d'ouverture), faites immédiatement opposition.

Comment réagir en cas de fraude à la carte bancaire ?

Dès que vous avez connaissance d'une opération de paiement ou de retrait par carte non autorisée, il convient :

- Dans un premier temps, d'**informer sans tarder votre banque ou le centre d'appel dédié afin de mettre votre carte en opposition** (il en va de même si votre carte est perdue ou volée) :
  - en contactant directement votre conseiller en agence ;
  - en vous rendant sur votre Espace Client ;
  - en appelant le numéro d'opposition propre à votre banque (qui figure sur votre contrat, mais également au dos des tickets de retrait et à côté des distributeurs de billets) ;
  - en appelant le numéro spécial du serveur interbancaire : **0 892 705 705** ouvert 24 h sur 24, 7 jours sur 7, et oriente votre appel vers le centre d'opposition compétent.
- Ensuite, de **confirmer par écrit et sans délai l'opposition** selon les modalités prévues par votre banque. En outre**,** vous devez signaler **sans** délai l'opération non autorisée auprès de votre établissement qui vous indiquera les démarches à effectuer.

Une **nouvelle technique de fraude** est utilisée par des personnes malveillantes afin de collecter les informations nécessaires à la validation d'un paiement sur Internet.

La technique utilisée est celle d'un **appel téléphonique passé par le fraudeur**, et consiste à afficher sur le téléphone du destinataire le numéro de téléphone du **Centre d'opposition de Monext** ; le porteur ainsi mis en confiance communique le numéro de sa carte, la date de validité, le cryptogramme visuel et tout autre élément sécuritaire.

Il est rappelé que, **dans le cadre de ses activités d'oppositions, le Centre d'Appel ne procède jamais à des appels à destination des porteurs de carte bancaire.**

Il est donc impératif que les clients porteurs de cartes bancaires ne communiquent jamais les renseignements ainsi demandés qui permettent l'utilisation frauduleuse de leur carte.

En cas d'agression ou si vous remarquez un comportement étrange : appelez le 17