CONSEIL DE SÉCURITÉ POUR LES UTILISATEURS DE MOYENS DE PAIEMENT SCRIPTURAUX

Dans le cadre de sa mission de surveillance des moyens de paiement, l'Institut d'émission d'Outre-mer publie régulièrement des conseils de sécurité à l'usage des utilisateurs de services de paiement dont le comportement concourt directement à la sécurité des différents moyens de paiement scripturaux.

Conseils de prudence à l'usage des porteurs de carte de paiement

Votre comportement concourt directement à la sécurité de l'utilisation de votre carte. Veillez à respecter les conseils élémentaires de prudence qui suivent afin de protéger vos transactions.

SOYEZ RESPONSABLES

- Votre carte est strictement personnelle : ne la prêtez à personne, même pas à vos proches.
- Vérifiez régulièrement qu'elle est en votre possession.
- Si votre carte comporte un code confidentiel, gardez-le secret. Ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter et surtout ne le rangez jamais avec votre carte.
- Lorsque vous composez votre code confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal ou du distributeur de votre autre main.
- Vérifiez régulièrement et attentivement vos relevés de compte.

SOYEZ ATTENTIFS

Lors des paiements chez un commerçant :

- Vérifiez l'utilisation qui est faite de votre carte par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider la transaction.

Lors des retraits sur les distributeurs de billets :

- Vérifiez l'aspect extérieur du distributeur, évitez si possible ceux qui vous paraîtraient avoir été altérés.
- Suivez exclusivement les consignes indiquées à l'écran du distributeur : ne vous laissez pas distraire par des inconnus, même proposant leur aide.
- Mettez immédiatement en opposition votre carte si elle a été avalée par l'automate et que vous ne pouvez pas la récupérer immédiatement au guichet de l'agence.

Lors des paiements sur internet :

- Protégez votre numéro de carte : ne le stockez pas sur votre ordinateur, ne l'envoyez pas par simple courriel et vérifiez la sécurisation du site du commerçant (cadenas en bas de la fenêtre, adresse commençant par « https », etc.).
- Assurez-vous du sérieux du commerçant, vérifiez que vous êtes bien sur le bon site, lisez attentivement les conditions générales de vente.
- Protégez votre ordinateur, en activant les mises à jour de sécurité proposées par les éditeurs de logiciel (en règle générale gratuites) et en l'équipant d'un antivirus et d'un pare-feu.

Lors de vos déplacements à l'étranger :

- Renseignez-vous sur les précautions à prendre et contactez l'établissement émetteur de votre carte avant votre départ, afin notamment de connaître les mécanismes de protection des cartes qui peuvent être mis en œuvre.
- Pensez à vous munir des numéros internationaux de mise en opposition de votre carte.

SACHEZ RÉAGIR

1. Vous avez perdu ou on vous a volé votre carte :

- Faites immédiatement opposition en appelant le numéro que vous a communiqué l'établissement émetteur de la carte. Pensez à le faire pour toutes vos cartes perdues ou volées.
- En cas de vol, déposez également plainte auprès de la police ou de la gendarmerie au plus vite.
- En faisant opposition sans tarder, vous bénéficierez des dispositions plafonnant les débits frauduleux, au pire des cas, à 18.000 Francs CFP. Si vous ne réagissez pas rapidement, vous risquez de supporter l'intégralité des débits frauduleux précédant la mise en opposition. À partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

2. Vous constatez des anomalies sur votre relevé de compte alors que votre carte est toujours en votre possession

Sauf en cas de négligence grave de votre part (par exemple, vous avez laissé à la vue d'un tiers le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir) ou en cas de non-respect intentionnel de vos obligations contractuelles en matière de sécurité (par exemple, vous avez commis l'imprudence de communiquer à un proche le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir), **il faut déposer une réclamation auprès de l'établissement émetteur de la carte, dès que possible et dans un délai fixé par la loi, de 13 mois à compter de la date de débit de l'opération contestée**. Dans ces conditions, votre responsabilité ne peut être engagée. Les sommes contestées doivent alors vous être immédiatement remboursées sans frais.

Attention, lorsque le détournement a lieu dans un pays non européen, le délai de contestation est ramené à 70 jours à compter de la date de débit de l'opération contestée. Ce délai peut éventuellement être prolongépar votre établissement émetteur sans pouvoir dépasser 120 jours. Bien entendu, en cas d'agissement frauduleux de votre part, les dispositions protectrices de la loi ne trouveront pas à s'appliquer et vous restez tenu des sommesdébités avant comme aprèsl'opposition ainsi que des éventuels autres frais engendréspar ces opérations (par exemple, en cas d'insuffisance de provision).

Le spoofing, une arnaque à la carte bancaire expliquée par la police nationale

Le spoofing consiste à usurper l'identité de votre banque afin d'obtenir vos données personnelles, et pouvoir ainsi détourner l'argent de votre compte vers un autre compte frauduleux. Cette escroquerie est réalisée par téléphone, par SMS ou par mail.
Le tout étant d'obtenir votre confiance grâce à une usurpation particulièrement réussi : le numéro d'appel est bien celui de votre banque, le mail comporte bien l'en-tête de votre établissement bancaire.

Comment se prémunir ?

La règle d'or consiste à ne jamais divulguer vos données personnelles par téléphone ou par mail, quelles que soient les raisons et les urgences invoquées par votre interlocuteur

- Ne pas cliquer sur un lien envoyé par courriel vous demandant de réaliser une mise à jour
- Ne pas ouvrir de pièces jointes
- Vérifier la présence de la mention « https» dans l'adresse, qui garantit que la connexion est sécurisée
- En cas de doute, joindre votre conseiller

Dans une vidéo publiée fin juin sur la page Facebook du ministère de l'Intérieur, la police nationale explique comment cette arnaque est orchestrée : https://www.facebook.com/watch/?v=1088208665107484

Escroquerie au faux courriel : signalement du Ministère de l'Intérieur

Récemment, vous avez peut-être été destinataire d'un mail, dont l'objet est une convocation judiciaire vous accusant de proposer, partager, diffuser et échanger des supports à caractère pornographiques ou pédopornographiques et d'avoir commis des atteintes sexuelles sans violence sur mineurs. Ces courriels usurpent l'appellation de la Gendarmerie nationale, de la Police nationale, de la préfecture de Police de Paris et d'Europol.

Attention : ce type de courriel est une arnaque.

Ce message vous demande de prendre contact au plus vite avec les directeurs de la Police ou de la Gendarmerie nationales. L'objectif de cette arnaque est de vous amener à verser une somme d'argent ou de vous faire communiquer vos données personnelles.

Les services du ministère de l'Intérieur n'envoient jamais de courriel pour procéder à des auditions. Les infractions mentionnées dans cette pseudo convocation ne font jamais l'objet de transaction. Leur traitement s'inscrit dans le cadre judiciaire sous contrôle d'un magistrat.

Si vous êtes destinataire de ce type de mail :

- Ne cédez pas à la panique ;
- Ne répondez jamais : vous confirmeriez que votre adresse est valide et que vous lisez ce type de message, entraînant d'autres sollicitations similaires ;
- Ne prenez jamais contact avec l'expéditeur, celui-ci cherchera à accroître la pression ;
- Ne payez pas ;
- Votre adresse email a sans doute été extraite suite à la consultation d'un site de e-commerce. Il est recommandé de changer votre mot de passe ;
- Ne cliquez sur aucun lien ou pièce jointe : vous pourriez être dirigé sur un site malveillant maquillé en site institutionnel, vous amenant à donner des informations personnelles ou à télécharger des documents contenant des logiciels malveillants ;
- Marquez ce courriel comme étant un courrier indésirable afin que les suivants puissent être filtrés par votre messagerie ;
- Conservez des éléments de preuve par des captures d'écran : note de menace, adresse mail de l'expéditeur, etc.

Déposez un signalement sur https://www.cybermalveillance.gouv.fr/ et à l'adresse mail fraude-bretic@interieur.gouv.fr afin qu'il soit pris en compte dans le cadre de l'enquête ouverte par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Si vous avez donné suite : déposez plainte immédiatement auprès des services de Police ou de Gendarmerie.

https://youtu.be/8xojkRAe1kQ