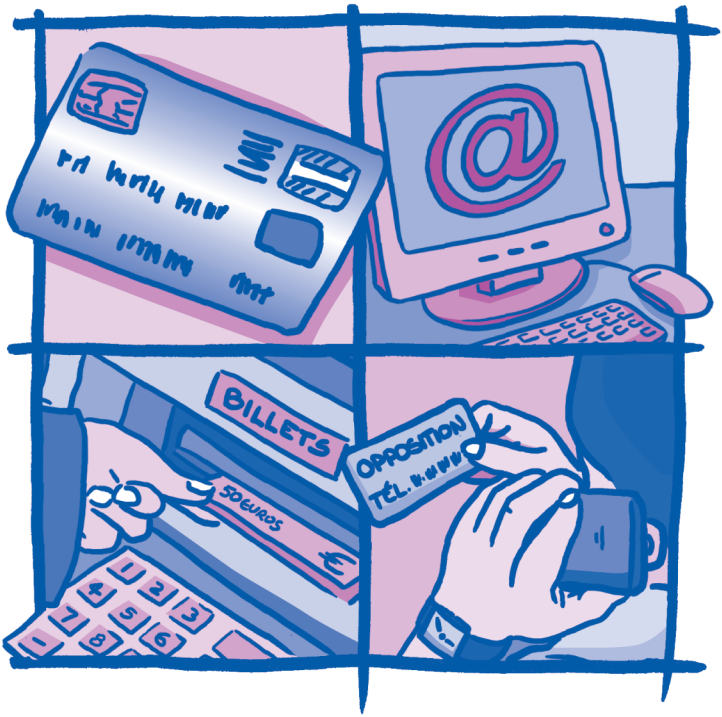
Particuliers,
la Banque de France vous informe



Identifiants bancaires : Être vigilant, c'est important

BANQUE DE FRANCE
EUROSYSTÈME

Être responsable

VOTRE CARTE BANCAIRE

Votre carte bancaire est strictement personnelle. Vous devez vérifier régulièrement qu'elle est en votre possession et ne la prêter à personne.

→ Protégez votre numéro de carte. Ne le stockez ni dans votre ordinateur, ni dans votre smartphone.
Ne le communiquez qu'à des commerçants de confiance au moment de payer.

→ Protégez votre code confidentiel à quatre chiffres. Ne le confiez à personne, pas même à vos proches. Personne n'est habilité à vous le demander, pas même la police.

→ Apprenez votre code confidentiel par cœur, en prenant soin de ne pas le conserver dans votre portefeuille.
Ne le révélez jamais sur Internet ou au téléphone.
Dans les commerces, les distributeurs de billets ou les automates de paiement (stations service 24/24, par exemple), composez toujours votre code à l'abri des regards indiscrets.

VOTRE COMPTE BANCAIRE

Vos coordonnées bancaires sont strictement personnelles.
Ne les communiquez qu'à bon escient : numéro de compte, relevé d'identité bancaire complet (RIB) ou identifiants internationaux.

→ Ne confiez vos coordonnées bancaires à personne, sauf à :
- un créancier devant effectuer un prélèvement sur votre compte. Assurez-vous que l'adresse d'envoi de l'autorisation de prélèvement est bien celle communiquée par votre créancier.
- une personne devant vous régler par virement. Assurez-vous que cette personne est légitime et de bonne foi.

→ Protégez l'identifiant et le mot de passe de votre compte à distance, que ce soit par téléphone ou sur Internet.
Ne confiez ces informations à personne.

→ Vérifiez régulièrement vos relevés de compte et contactez immédiatement votre banque à la moindre anomalie.

Être attentif à l'extérieur

Pour dissuader tout vol de votre carte bancaire ou de vos données personnelles, soyez attentif quand vous utilisez votre carte bancaire chez les commerçants, dans les distributeurs de billets et dans les automates de paiement (station-service 24h/24, par exemple), en France comme à l'étranger.

CHEZ LES COMMERÇANTS

→ Lors des paiements chez un commerçant, ne quittez jamais votre carte des yeux et surveillez l'utilisation qui en est faite par le commerçant.

→ Vérifiez toujours le montant affiché par le terminal de paiement avant de valider la transaction.

AUX DISTRIBUTEURS DE BILLETS ET AUX AUTOMATES DE PAIEMENT

→ Vérifiez l'aspect extérieur de l'appareil. Évitez d'utiliser les appareils qui vous paraissent avoir été altérés.

→ Conformez-vous strictement aux consignes indiquées à l'écran de l'appareil : ne vous laissez pas distraire par des inconnus, même proposant leur aide.

→ Mettez immédiatement votre carte en opposition si elle a été avalée par l'automate ou le distributeur, et que vous ne pouvez pas la récupérer tout de suite chez le commerçant ou au guichet de l'agence bancaire.

AVANT UN DÉPLACEMENT À L'ÉTRANGER

→ Contactez l'établissement émetteur de votre carte pour connaître les précautions à prendre et les protections que vous pouvez activer.

→ Munissez-vous des numéros de téléphone internationaux de mise en opposition de votre carte.

Être attentif sur Internet

→ Assurez-vous du sérieux du commerçant : vérifiez que vous êtes sur le bon site en tapant vous-même l'adresse du site plutôt qu'en cliquant sur le lien d'un courriel et lisez attentivement les conditions générales de vente.

→ Utilisez de préférence les sites qui vous proposent un paiement sécurisé par identification renforcée.

Exemple : le système « 3D-Secure » connu sous l'appellation « *Verified by Visa* » ou « *MasterCard SecureCode* ».
Il vous permet de valider le paiement en saisissant sur Internet un code d'autorisation unique envoyé sur votre téléphone mobile, par SMS, à l'issue de la validation de l'achat.

→ À défaut, vérifiez que le site du commerçant est sécurisé : adresse Internet commençant par « *https* » et cadenas en bas de la fenêtre.

→ Lorsque vous avez fini de naviguer sur le site de votre banque, utilisez le bouton de déconnexion pour clôturer définitivement votre navigation et limiter ainsi le risque de récupération de vos données personnelles.

→ Par principe, ne confiez jamais votre numéro de carte par courriel ou par téléphone. En pratique, si un commerçant (hôtel, chambres d'hôtes, etc.) l'exige pour confirmer une réservation, communiquez-le uniquement à des commerçants de confiance.

Plus de sécurité sur Internet avec le code à usage unique

Aujourd'hui, des mécanismes permettent d'authentifier le porteur de la carte lors d'un paiement sur Internet, c'est-à-dire de s'assurer que l'utilisateur est bien le détenteur légitime de cette carte.

Ces mécanismes reposent généralement sur un code à usage unique qui vous est communiqué par votre banque lors du paiement et que vous devez utiliser pour finaliser la transaction.

En France, il s'agit en grande majorité du système dit « 3D Secure », également désigné sous les appellations « 3DS », « MasterCard SecureCode » ou « Verified by Visa ». Les commerçants en ligne compatibles avec « 3D-Secure » affichent au minimum l'un des logos suivants :

Avec ce dispositif de sécurité, l'opération de paiement se déroule en deux temps :

1. vous saisissez comme d'habitude vos nom et prénom, votre numéro de carte bancaire, la date d'expiration et les trois derniers chiffres du cryptogramme visuel qui figure au dos de la carte.
2. vous êtes redirigé vers le site sécurisé de votre banque. Celle-ci vous demande de renseigner le code à usage unique qu'elle vient de vous communiquer par SMS, ou votre date de naissance ou encore la réponse à une question secrète ou tout autre moyen qu'elle vous aura préalablement fourni : lecteur de carte, générateur autonome de codes aléatoires, etc.

Une fois les deux étapes réussies, vous êtes redirigé sur la page de votre commerçant en ligne qui vous confirme le bon déroulement de la transaction.

En cas de problème, notamment si vous ne recevez pas ou si vous n'arrivez pas à générer le code à usage unique, vous êtes invité à contacter votre banque.

Être attentif à la maison

SUR VOTRE ORDINATEUR PERSONNEL

→ 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.

→ Refusez la mémorisation des mots de passe lorsque votre ordinateur vous le propose.

→ Si vous avez supprimé des documents de votre ordinateur, n'oubliez pas de vider la corbeille.

→ Supprimez régulièrement, après chaque connexion si possible, les cookies et les fichiers temporaires Internet stockés par l'ordinateur.

EN CLASSANT VOS DOCUMENTS

→ Si vous vous débarrassez de documents où figurent des identifiants bancaires ou des numéros de carte (relevés de compte, RIB, tickets d'opération, etc.), prenez soin de les détruire afin de ne pas permettre la réutilisation de vos données personnelles.

Attention, votre responsabilité est engagée

→ Si on peut vous imputer une négligence grave, par exemple, si vous avez confié votre carte et votre code confidentiel à un tiers.

→ Si vous n'avez pas respecté intentionnellement vos obligations contractuelles en matière de sécurité, par exemple, communication à un proche du numéro et/ou du code confidentiel de votre carte et celui-ci en a fait usage à votre insu.

→ En cas d'agissement frauduleux de votre part. Dans ce cas, les dispositions protectrices de la loi ne trouveront pas à s'appliquer et vous resterez tenu des sommes débitées avant comme après l'opposition, ainsi que des éventuels autres frais engendrés par ces opérations (par exemple, en cas d'insuffisance de provision).

Être réactif

CARTE PERDUE OU VOLÉE

→ Faites immédiatement opposition en appelant le numéro que l'établissement émetteur de la carte vous a communiqué. Pensez à le faire pour toutes vos cartes perdues ou volées. En cas de vol de votre carte, déposez également plainte auprès de la police ou de la gendarmerie au plus vite.

→ Si vous ne réagissez pas rapidement, vous risquez de supporter l'intégralité des débits frauduleux précédant la mise en opposition. En revanche, à partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

ANOMALIE SUR VOTRE RELEVÉ DE COMPTE

→ Déposez au plus vite une réclamation auprès de l'établissement émetteur de votre carte ou gestionnaire de votre compte, lorsque l'incident porte sur une usurpation de votre numéro de compte.
Dans ces conditions, votre responsabilité ne peut être engagée et les sommes contestées doivent vous être immédiatement remboursées sans frais.

→ Lorsque l'opération contestée a lieu dans un pays de l'Espace économique européen, votre réclamation doit être faite au plus tard dans un délai de 13 mois à compter de la date de débit de l'opération contestée.

→ Attention, lorsque l'opération contestée a lieu dans un pays hors de l'Espace économique européen, votre réclamation doit être faite au plus tard dans un délai de 70 jours à compter de la date de débit de l'opération contestée (ce délai peut éventuellement être prolongé jusqu'à 120 jours par l'établissement émetteur).

La vigilance, pourquoi

En matière bancaire comme partout ailleurs, la sécurité est l'affaire de tous. De la même manière que vous devez faire attention à votre carte d'identité, à votre passeport ou à vos clefs, vous devez prendre soin de vos relevés d'identité bancaire, numéros de cartes bancaires et codes secrets associés, identifiants et mots de passe correspondants… Ces éléments, qui vous sont confiés par votre banque, sont en effet strictement personnels et vous vous protégez en les protégeant.

La vigilance, pour qui

Cela vous concerne dès lors que vous gérez un compte bancaire et les moyens nécessaires à son fonctionnement (relevé d'identité bancaire, chéquier, carte bancaire, virements, prélèvements, identifiants et mots de passe permettant d'accéder à la gestion de votre compte en ligne…).
Et ce, qu'il s'agisse de votre compte personnel, de celui de votre employeur ou de votre association…

La vigilance, comment

Votre banque a mis en œuvre des systèmes de protection, mais vous êtes responsable des moyens mis à votre disposition et de leur utilisation. En toute occasion, dans la vie de tous les jours, sur Internet ou au téléphone, dans la rue, chez vous ou dans un commerce, vous devez donc être RESPONSABLE, ATTENTIF et RÉACTIF.

CES CONSEILS DE PRUDENCE SONT MIS EN AVANT POUR VOUS ASSURER UNE BONNE UTILISATION DE VOS MOYENS DE PAIEMENT. ILS NE SE SUBSTITUENT EN AUCUNE MANIÈRE AUX TEXTES LÉGISLATIFS ET RÈGLEMENTAIRES EN VIGUEUR EN MATIÈRE DE RESPONSABILITÉ.