ARNAQUES A LA CARTE BANCAIRE EN VILLE OU SUR INTERNET (16 février 2013)

1. Quelles sont les arnaques ? diapo 1
2. Comment essayer de se prémunir ?
3. Quelles sont nos responsabilités ?
4. Que faut-il faire en cas de… ?

Introduction

Mesdames, messieurs, bienvenus à cette réunion d'information sur les « arnaques à la carte bancaire ».

Vous avez constaté qu'on parle beaucoup à la télévision (émissions c dans l'air, envoyé spécial ou les journaux télévisés) ainsi que dans les autres médias des arnaques à la CB. Il y a en effet une raison à cela. Depuis quelques années, le développement des paiements avec une CB entraîne, en effet, une recrudescence des débits bancaires frauduleux. Selon la Banque de France et son rapport 2011 , « Le montant total de la fraude est quant à lui en forte augmentation (+ 12 % par rapport à 2010) pour s'élever à 413,2 millions d'euros en 2011. » diapo 2
Ce sont ainsi 650 000 ménages concernés en France qui ont subi une fraude.

Les chiffres 2012 ne sont pas encore connus en totalité.

Cette hausse sensible de la fraude s'explique de plusieurs manières :
- une augmentation de nouveau importante, comme chaque année, des paiements à distance (sur internet)
- pour la première fois depuis plusieurs années, une hausse de la fraude en paiement de proximité. Par exemple les DAB. (distributeur de billets)
- par la récession qui frappe l'Europe,
- par un gain important et facile et une prise de risque moins dangereuse que pour le trafic de drogue par exemple.

Par exemple les attaques de distributeurs automatiques de billets (DAB) sont en hausse sensible avec 622 piratages de DAB en 2011 (contre 527 en 2010)
À celles-ci s'ajoutent 32 attaques de terminaux de paiement (contre 30 en 2010)

Nous allons voir les principaux aspects de la fraude à la carte bancaire.. diapo 3

1 - QUELLES SONT LES ARNAQUES DE PROXIMITÉ ? DIAPO 4

1.1. Le vol :

Le grand classique se passe souvent aux caisses d'hypermarchés. La personne qui est derrière vous vous surveille, note mentalement votre code, regarde ou vous mettez votre carte, un complice détourne votre attention et on vous vole.

1.2. La copie de la carte ou le vendeur malhonnête

Le vendeur ou serveur indélicat peut faire en une seconde, avec un lecteur de carte, une copie de la bande diapo 5 magnétique de votre carte. IL aura les infos de votre carte. Il lui suffit de noter mentalement le cryptogramme diapo 6 et il peut acheter sur internet. Ceci peut vous arriver dans les boutiques de souvenirs, les restaurants partout où votre carte sort de votre vue. Il peut également fabriquer de fausses cartes ou vendre les informations de votre carte sur internet. (Vu dans « envoyé spécial »)

Vendeur malhonnête
Lors d'un paiement par **carte bancaire** en magasin, le commerçant conserve un ticket qui indique l'intégralité du numéro de carte du client. Il suffit à un vendeur ou un serveur malhonnête, par exemple, de relever le nom de la victime, la date de validité et le cryptogramme à trois chiffres qui figurent au dos de la carte. Et le tour est joué. Lors des achats à distance, ces éléments suffisent souvent pour sceller la transaction, sans que personne ne sache si celui qui les délivre est bien le détenteur légal de la carte.

1.3. Le distributeur trafiqué (appelé aussi le skimming)

Vous arrivez au distributeur et vous essayez de retirer de l'argent. Ça ne marche pas. Un client derrière vous vous propose son aide et vous demande de refaire votre code. C'est alors trop tard. Rien ne fonctionne, vous partez mais le voleur retourne au DAB et récupère votre carte. Il peut alors retirer de l'argent et acheter sur internet. diapos 7 à 21
Et diapos diapo 22 et 23 + vidéo
Concrètement, un lecteur copieur a été appliqué sur la fente d'insertion de la carte bancaire et une micro-caméra alimentée par des batteries de téléphone portable a été disposée à l'intérieur d'une réglette apposée discrètement au-dessus du clavier du DAB afin de filmer et mémoriser le code secret. Voir vidéo http://www.stop-skimming.ch/fr/qu_est-ce_que_le_skimming/

1.4 Passons maintenant aux arnaques sur internet

1.5 Logiciels espions

Quiconque n'utilise pas ou ne met pas à jour son logiciel antivirus s'expose à voir son ordinateur infecté par l'un de ces mouchards. Dans le cas des fraudes à la carte bancaire, il prend la forme d'un petit programme espion qui s'installe à l'occasion d'un téléchargement, en visionnant, par exemple, une vidéo licencieuse ou en piratant de la musique. Ce logiciel malveillant se réveille lorsque le client se connecte à un site payant, même sécurisé (https). Puis il enregistre toutes les informations saisies sur le clavier lors de la phase de paiement. Pour les transmettre instantanément à des pirates informatiques dans les pays de l'est ou ailleurs.

Il y aura dans quelques semaines une réunion d'information sur les virus, logiciels malveillants (appelé aussi malwares) et anti-virus

1.6 Mails trompeurs ou phishing (appelé aussi filoutage) diapo 24

Cette technique consiste à soutirer des informations personnelles à un internaute en se faisant passer pour un tiers de confiance (banque, gendarmerie, EDF, Orange etc…). La victime reçoit un courriel où il lui est demandé de confirmer ses données bancaires, dans le cadre d'un soi-disant contrôle de sécurité. Et souvent les personnes y croient et plongent. On vous demande alors de cliquer sur un lien qui vous renvoit vers un faux site imitant à la perfection le vrai site. Mais il existe un moyen de reconnaître un faux site de votre banque. Dans la barre d'adresse de votre navigateur il y aura obligatoirement une incohérence dans l'URL ou adresse internet de la banque. Il ne faut pas cliquer sur un lien mail mais utiliser l'URL de vos favoris ou bien passez par google. Il est important de vérifier l'URL affiché par le navigateur et comparer avec celui de la banque (attention parfois il n'y a qu'une lettre de différence) et bien sur ne pas hésiter à téléphoner à la banque ou au site pour vérifier.

Bien entendu, aucune banque, aucun service public ou privé ne demande à ses clients ce type d'information, mais le faible nombre de personnes qui acceptent de délivrer ces informations suffisent aux hameçonneurs pour récupérer quelques dizaines de milliers d'euros en prélevant de petites sommes sur chaque numéro de carte bleue frauduleusement récupéré.

Je sors un peu de l'arnaque à la CB pour parler aussi d'un autre mail trompeur. L'usurpation d'identité. Votre boîte mail a été piratée et le pirate à tous vos contacts. Il fait donc un faux mail vous demandant de l'argent sous un prétexte quelconque (maladie, difficulties financières…) et vous promettant un remboursement avec de gros intérêts. Vérifiez l'orthographe, les tournures de phrases, s'il y a des accents sur les lettres s'il n'y a pas d'accents sur les lettres cela signifie que la message a été tapé avec un clavier anglais.

2 - Comment essayer de se prémunir ? DIAPO 25

2.1 Quand vous êtes au supermarché :

Regardez autour de vous, (au besoin fixez du regard une personne qui vous observe – devant ou derrière vous – vous donnez ainsi un signal au à la personne qui vous observe, cachez avec votre main (ou si vous n'osez pas, tenez une publicité du magasin dans la main gauche pour cacher le terminal de paiement) quand vous tapez votre code. Mettez votre carte dans votre sac (ou votre portefeuille) et fermer celui-ci. Enfin, ne vous laissez pas importuner par quelqu'un que vous ne connaissez pas. Restez concentré sur ce que vous faites. Si vous ne vous sentez pas à l'aise payez par chèque.

2.2 Si on retire de l'argent d'un DAB (distributeur automatique de banque)

- vérifiez l'aspect extérieur du distributeur, évitez si possible ceux qui vous paraîtraient avoir été altérés
- Vérifiez dans le haut du DAB s'il n'y a pas un petit trou (signifie qu'il y a une caméra qui filme lorsque vous composez votre code)
- ne vous laissez pas distraire, l'arnaque se fera principalement le dimanche (car banques fermées)
- composez votre code confidentiel à l'abri des regards, mettez un journal, une revue pour cacher la composition du code.
- refusez l'aide de toute personne,
- si vous ne parvenez pas à récupérer votre carte bancaire, faites immédiatement opposition (vous supposez alors un DAB trafiqué à moins que vous ayez fait trois fois un mauvais code dans ce cas la carte est conservé par la machine).
- Faites vous accompagner par un proche qui gênera la présence de toute autre personne.
- Se fier à son intuition
  Faites confiance à votre intuition : si un distributeur vous paraît suspect ou que vous ne vous sentez pas à l'aise parce que des personnes douteuses se trouvent à proximité, ou encore parce que quelqu'un vous interpelle ou s'approche trop près de vous, annulez le paiement ou le retrait et cherchez un autre automate.

2.3 Si vous payez dans un restaurant ou une boutique

Ne quittez pas votre carte des yeux pendant le paiement. Au restaurant déplacez-vous au comptoir pour payer. Un serveur ou vendeur mal intentionné peut copier très rapidement votre carte et retenir votre cryptogramme (voir diapo 26 du cryptogramme). Il peut alors acheter à loisir sur internet tant que vous n'aurez pas fait opposition (nous verrons plus loin comment faire opposition). Vous pouvez très bien mettre une « gommette » sur votre cryptogramme pour le cacher (vous n'en avez pas besoin pour payer dans un restaurant ou une boutique…). Pour éviter de décoller la gommette à chaque utilisation sur internet, noyez les trois chiffres dans un n° de téléphone de votre portable.
Ex : Charles Baraud 05 55 27 12 30 (dans l'exemple je l'ai mis à la fin mais vous pouvez le mettre n'importe où)
Vous pouvez aussi le gratter ou passer un coup de marqueur indélébile par dessus. N'oubliez pas de le noter de façon cachée !
Sachez que le cryptogramme est seulement demandé lors des achats sur internet.
Composez là aussi votre code confidentiel à l'abri des regards.

Ce nombre, que vous seul pouvez voir et donc inscrire manuellement lors de votre commande, rend impossible l'utilisation de vos numéros de carte bancaire par quelqu'un qui ne possèderai pas physiquement la carte bancaire.

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 oeuvre ;
• pensez à vous munir des numéros de téléphone internationaux de mise en opposition de votre carte.

2.4 SUR INTERNET

Voici quelques conseils pour sécuriser votre paiement par carte bancaire sur Internet :

- Privilégiez les sites marchands connus et les enseignes de notoriété publique ou recommandés par un ami.
- Méfiez-vous des sites des sociétés étrangères.
- Identifiez les coordonnées de l'entreprise commerciale. Lisez les conditions générales de vente (CGV ces informations doivent être accessibles dès la page d'accueil, c'est un gage de transparence).
- Payez sur une page sécurisée en vérifiant :
  - l'affichage sur la page d'un cadenas fermé,
  - l'adresse URL du site doit débuter par **https://** (le « s » signifie sécurisé) et être de couleur verte. diapo 27 (malheureusement des sites pirates apparaissent maintenant sécurisés)
- Conservez le mail de confirmation de votre commande.
- Faites des captures ou des impressions d'écran de votre commande. (si possible)

- Vérifiez, dans les jours suivants sur votre site de banque ou dès la réception de votre relevé bancaire le montant du paiement effectué.
- Ne stockez pas sur votre ordinateur votre numéro de carte bancaire, ni son code.
- Mettez à jour les systèmes de protection de votre ordinateur (antivirus).

***Bon à savoir** : Bien que beaucoup d'internautes soient réticents à payer en ligne leurs achats avec leur carte bancaire, sachez que ce système est bien sécurisé par un système crypté. Certaines sociétés de vente à distance utilise le système 3D secure et vous envoie sur votre téléphone portable un code que vous devez ajouter à votre paiement sur internet. Ça donne l'assurance que vous êtes le bon acheteur .*

Soyez toujours très vigilant. Les trop bonnes affaires sont toujours douteuses. Évitez les sites basés en Chine, Europe de l'est etc… ou les sites dont les fautes d'orthographe sont trop nombreuses.

Si vraiment vous avez un doute, alors vérifiez la réelle existence de la société.

En France, il est obligatoire pour un site faisant du e-commerce, d'indiquer (liste non exhaustive) :

- l'adresse de l'établissement, son mail et son numéro de téléphone

- son numéro d'inscription au Registre du commerce et des sociétés ou au Répertoire des métiers.
Vous les trouverez généralement sur une page "Mention Légales". Avec le numéro d'immatriculation SIREN ou la raison sociale, rendez-vous sur le site http://www.infogreffe.fr , et faite une recherche afin de vérifier si la société existe bien et si elle n'a pas été radiée.
Vous pouvez aussi vérifier sur le site sur http://www.whois-raynette.fr/ . Diapo 28 Prendre pour exemple rue du commerce

Si vous ne la trouvez pas, cette société n'exerce pas en France, vous devrez être encore plus attentif.

Vérifier où se trouve l'adresse postale de contact / de retour de matériel

Vous devriez trouver cette adresse dans une page appelée "Conditions Générales de Vente" (CGV).

Vérifier l'adresse email de contact

Vous devriez trouver cette adresse sur le site dans la section "Contact", ou bien dans les "Mentions légales".
Si l'adresse de contact n'est pas une adresse xxx@nomdelasociete.xxx, par exemple @gmail.com, une nouvelle fois, passez votre chemin.

Vérifier les moyens de paiement proposés et les frais de port

Sur un site fiable, vous pouvez habituellement payer par CB, PayPal, virement bancaire ou chèque.

"Si vous voyez Western Union, fuyez !!! "

Western Union est une banque qui fait du transfert d'argent à ne pas utiliser comme moyen de paiement. C'est-à-dire que vous envoyez de l'argent par mandat à une personne désigné. Elle se présente à la banque et encaisse en cash.

Si la livraison est gratuite DANS LE MONDE entier : même punition !

Vérifier le contenu du site internet : textes, descriptions de produits, ...

95% des sites vendant des copies présentent des textes ayant fait l'objet d'une simple traduction via google : vous remarquerez des tournures de phrases étranges voire incompréhensibles. Passez alors votre chemin.

3 – Quelles sont nos responsabilités ?

Carte bancaire et fraude : qui est responsable ?

Si vous êtes titulaire d'une carte bancaire de paiement, vous pouvez découvrir un jour, sur vos relevés de comptes, des débits pour des achats qui vous sont totalement étrangers ?
Se pose alors une question: qui est responsable en cas de fraude ?

3.1 Avant l'opposition

En principe, vous êtes responsable des opérations effectuées avec votre carte avant la date de votre opposition. Mais dans la limite d'un plafond qui ne peut dépasser 150 euros depuis le 1er janvier 2003 (Code mon. et fin. art. L 132-3 nouveau).
Attention : là encore, votre responsabilité peut être engagée sans plafond aucun, si votre comportement a été particulièrement négligent. Ce peut être par exemple le cas si vous avez tardé à faire opposition ou si un membre de votre famille a utilisé votre code laissé en évidence...
Le contrat entre le titulaire et la banque peut imposer un délai maximal d'opposition, au delà duquel votre responsabilité peut être engagée sans plafond aucun. Ce délai ne peut être inférieur à deux jours francs.
A l'inverse, la banque ne doit pas non plus faire preuve de négligence. C'est à elle, par exemple, de vérifier que la signature qui figure sur les facturettes est bien la vôtre même si ces facturettes ont été émises avant l'opposition. Elle doit également alerter le titulaire du compte si les retraits ou les paiements sont largement exagérés par rapport aux mouvements habituels du compte.

3.2 Faire opposition

Dès que vous constatez la disparition de votre carte, vous devez immédiatement prévenir votre établissement bancaire par téléphone et faire opposition, avant de confirmer votre démarche par lettre recommandée avec accusé de réception.
S'il s'agit d'un vol, vous devez également porter plainte au commissariat ou à la gendarmerie et joindre à votre lettre le récépissé de déclaration.
S'il s'agit d'une carte Bleue, vous pouvez également faire opposition si un membre de votre famille l'a subtilisée sans qu'il s'agisse réellement d'un vol. En principe, l'opposition est réputée effectuée dès que votre établissement bancaire est prévenu. Mais en cas de litige, c'est la date de réception de la lettre recommandée qui est prise en compte. Mieux vaut donc l'expédier le plus tôt possible, voire même se rendre en personne à la banque pour réduire les délais.
A l'étranger : Si la carte a été volée à l'étranger, le titulaire de la carte doit contacter les autorités consulaires et la police pour déclarer le vol. Une fois l'opposition enregistrée, les données sont mises à jour à la banque, rendant la carte inutilisable.

3.3 Après l'opposition

Le principe est simple et intangible : votre responsabilité est totalement dégagée pour toutes les opérations frauduleuses effectuées après la date de votre opposition. Rien de plus logique puisque c'est maintenant à la banque de mettre en oeuvre tous les moyens techniques pour empêcher l'utilisation de la carte perdue ou volée (blocage dans les distributeurs, etc.).
Attention : dans certains cas, heureusement assez rares, votre responsabilité peut être engagée même après l'opposition si votre comportement a été particulièrement fautif ou imprudent.
Exemples : vous n'avez pas apposé votre signature au dos de la carte, vous avez noté le code secret sur un papier collé à la carte, etc. Mais c'est naturellement à la banque de prouver votre négligence...

3.4 En cas de fraude

Même si vous êtes encore en possession de votre carte et que vous n'avez donc pas fait opposition, votre responsabilité est totalement dégagée (sans limites aucunes) en cas d'utilisation frauduleuse de votre numéro de carte (achat par correspondance) ou de contrefaçon.
Il vous suffit de notifier par écrit votre contestation à l'établissement émetteur (voir modèle de lettre sur le site soursac-informatique). Vous avez également la possibilité de porter plainte au commissariat, mais sachez que les banques n'ont pas le droit de conditionner le remboursement des sommes versées à un dépôt de plainte de leur client.
L'établissement bancaire doit alors vous recréditer les sommes litigieuses dans le délai d'un mois qui suit la réception de votre lettre recommandée (Code mon. et fin. art. L 132-4).

3.5 Délai de réclamation

La réclamation doit être faite dans un délai de 13 mois à compter de la date du débit sous peine de forclusion. Pour les paiements effectués hors Union Européenne, vous avez le droit de déposer une réclamation auprès de l'établissement émetteur pendant un délai minimal de 70 jours après la date de l'opération litigieuse. Ce délai peut être porté à 120 jours au plus par le contrat signé avec l'établissement.

En résumé : diapo 29

- *Carte bancaire : responsabilité en cas d'utilisation frauduleuse dans les cas suivants :*
  - sans utilisation physique de la carte pour un paiement à distance : tout est à la charge de la banque (loi du 15/11/2001, article L. 132-4 du Code monétaire et financier). Contestez dans un délai de 70 jours.

  - avec frappe du code : franchise 150 € (article L. 132-3 du Code monétaire et financier) sauf faute lourde du consommateur (opposition tardive par exemple).

  - en cas de contrefaçon : aucune somme ne sera laissée à la charge du consommateur.

  -à partir de l'opposition, plus aucune somme n'est due.

4 – Que faut-il faire en cas de …

Carte bancaire : opposition en cas de perte ou vol diapo 30

Vous devez faire opposition en cas :

- de perte,
- de vol,
- d'utilisation frauduleuse de la carte ou des données liées à son utilisation,

Le plus urgent

Le plus simple et le plus rapide est d'appeler le numéro spécial du serveur interbancaire 0 892 705 705 (0,34€ / mn), serveur vocal interactif, ouvert 7 jours sur 7, qui oriente chaque appel vers le centre d'opposition compétent.
Mais vous pouvez aussi appeler directement le numéro propre à votre banque. Vous trouverez aussi le numéro de téléphone à appeler à côté des distributeurs de billets, et il est en général également indiqué au dos des tickets de retrait.
Si votre carte a été volée, contactez la police pour leur déclarer le vol.

Si l'incident a eu lieu à l'étranger, contactez les autorités consulaires et déclarer le vol à la police locale. Appelez votre banque ou le serveur interbancaire.

4.1 Les informations à fournir

Lorsque vous contacterez le service concerné, il vous sera demandé le numéro à 16 chiffres de votre carte et sa date d'expiration, car cela facilitera la recherche et permettra d'accélérer l'opposition.
Par prudence, vous avez donc intérêt à noter ces informations sur un document conservé en sécurité, évidemment pas au même endroit que la carte, et facilement accessible en cas de perte ou vol de votre carte.
Le centre de mise en opposition vous communiquera en principe un numéro d'enregistrement à conserver.

4.2 La confirmation écrite

Confirmez ensuite votre opposition par lettre envoyée en recommandé avec accusé de réception
La réception par la banque de votre opposition écrite dégage votre responsabilité s'il y a eu utilisation frauduleuse. Vous êtes responsable de tout paiement fait avant l'opposition.
L'opposition sur carte coûte généralement selon les banques entre 7 et 20 euros.

4.3 En cas de non opposition

Si vous omettez de faire opposition après la perte ou le vol de votre carte, votre responsabilité peut être engagée jusqu'à un montant maximum de 150 € (depuis le 1er janvier 2003 - art. L132-2 du Code monétaire et financier). Vous ne supporterez donc la perte subie avant la mise en opposition que dans la limite de ce plafond de 150 euros.

En revanche, le plafond n'est pas applicable si vous avez agi avec négligence ou si vous n'avez pas effectué l'opposition dans les meilleurs délais. Ce délai pour faire opposition et bénéficier du plafond ne peut être inférieur à deux jours francs après le vol ou la perte de la carte. (Art.L132-3 du Code monétaire et financier).

Je rappelle que même si vous êtes toujours en possession de votre carte bancaire, vous pouvez être victime d'opérations frauduleuses et constater sur votre relevé des débits pour des achats dont vous n'êtes pas l'auteur. Dès lors qu'il n'y a pas eu utilisation physique de votre carte, par exemple pour des achats à distance, votre responsabilité n'est pas engagée et la banque doit vous rembourser les sommes en question dans le délai d'un mois à compter de la réception de votre réclamation. A noter qu'une banque n'a pas le droit de conditionner le remboursement des sommes versées à un dépôt de plainte de son client.

J'en arrive à la conclusion

Ce sujet n'a pas la prétention d'être exhaustif car les voleurs ont toujours une imagination débordante et trouvent sans cesse de nouvelles manières de nous arnaquer. Il n'y a pas très longtemps, à Bordeaux, un escroc a volé à la fermeture d'une boutique le terminal diapo 31 de paiement (vous savez le petit boitier où vous tapez votre code et l'a remplacé par un autre. Avec celui qu'il a volé il a récupéré toutes les instructions des cartes. Le lendemain matin à l'ouverture du magasin il a remis discrètement le terminal en place. Ni vu ni connu, le responsable de la boutique n'a rien vu.

Ce que je vous ai raconté doit sans doute vous faire peur mais il ne faut pas tomber dans la paranoïa. Il faut connaître le danger, savoir se prémunir et savoir réagir ensuite. Je rappelle enfin que votre responsabilité est réduite dans la mesure où vous réagissez vite et bien.

J'en termine ici et vous voyez que cela peut nous arriver, les témoignages exposés nous le prouvent. Donc

- Soyez vigilant sur internet ou en ville, diapo 32
- Ne donnez votre code à personne (même pas aux gendarmes)
- Ayez votre anti-virus à jour
- surveillez vos comptes fréquemment

et vous laisserez le moins de chance possible aux voleurs.

La prochaine réunion portera sur les virus et anti-virus, elle aura lieu au mois d'avril.

Toutes les lettres doivent être adressées en recommandé avec accusé de réception, avec vos noms et adresses en haut à gauche, le destinataire en dessous à droite, et éventuellement les références du dossier et la liste des pièces jointes.

Nom Prénom expéditeur
N° Rue
CP Ville

Date

Nom Prénom destinataire
N° Rue
CP Ville

Objet : réclamation pour débits frauduleux par carte bancaire

Je vous confirme, par la présente, que je ne suis pas l'auteur des débits suivants qui apparaissent sur le relevé de ma carte bancaire.

(détailler le montant, le bénéficiaire, et les dates de débits contestés).

Vous trouverez ci-joint la copie de ce relevé où j'ai mentionné les opérations frauduleuses.

Comme le stipule l'Article L133-19 du Code monétaire et financier, La responsabilité du titulaire d'une carte de paiement n'est pas engagée si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de sa carte.

Je vous demande donc de me recréditer la somme de xxx euros, montant total des débits injustifiés, dans le délai d'un mois, conformément aux dispositions de cet article.

Formule de politesse