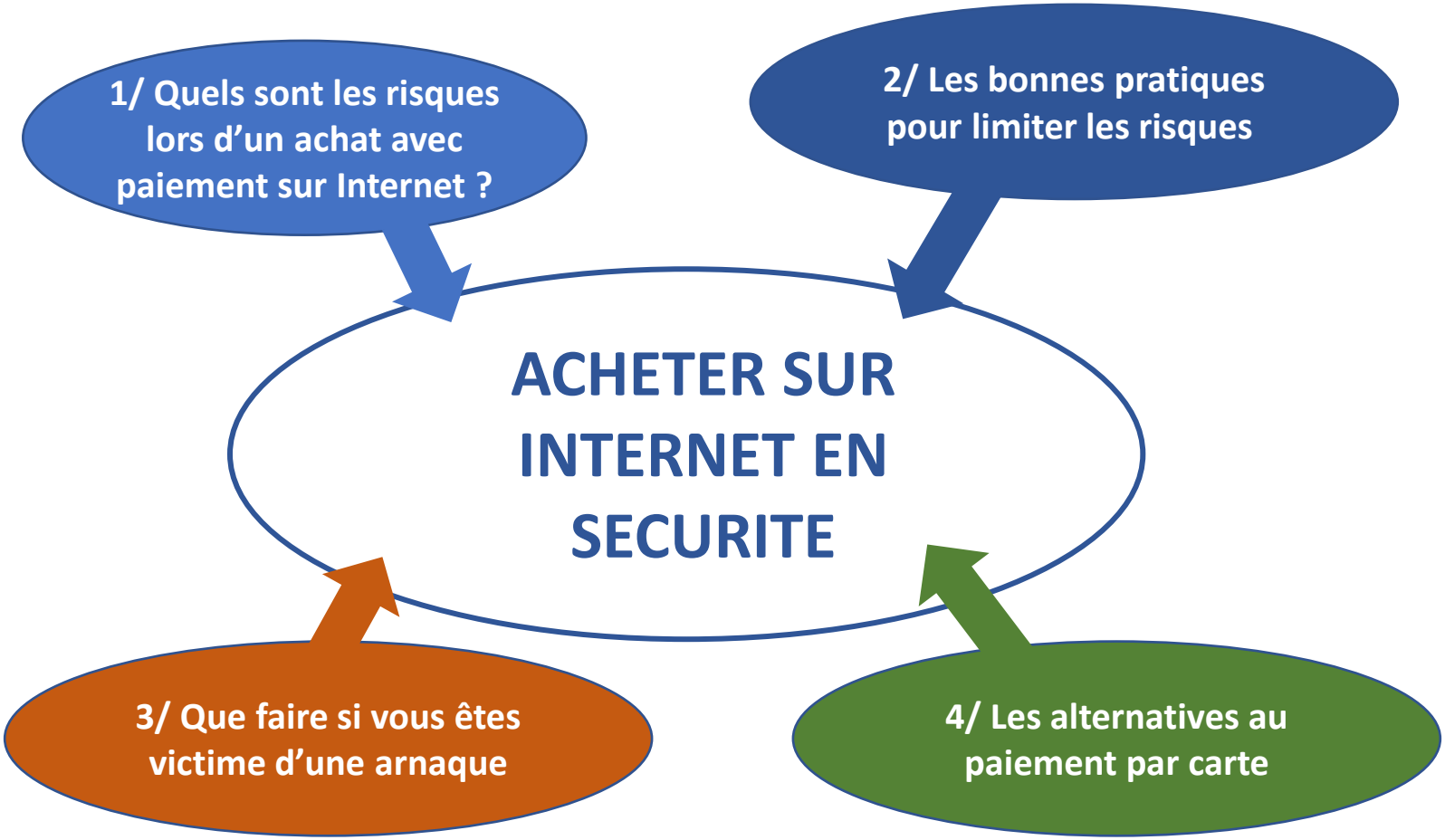
L'ETAPE
COWORKING ASSOCIATIF

L'ETAPE
LE NUMERIQUE POUR TOUS



Les cahiers numériques de l'Etape – 33650 Saint-Selve – février 2023

L'ETAPE
LE NUMERIQUE POUR TOUS

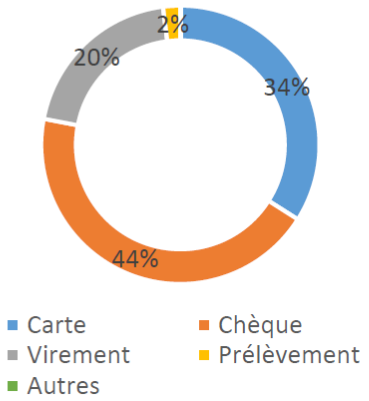
Quelques chiffres

(source : Observatoire de la sécurité des moyens de paiement)

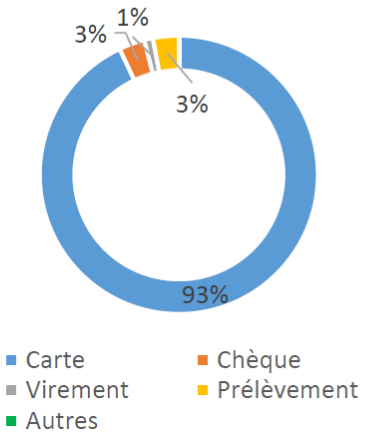
La fraude aux moyens de paiement au 1er semestre 2021

Le nombre de cas de fraude via la carte est important , mais il porte sur des montants très inférieurs aux fraudes sur les chèques

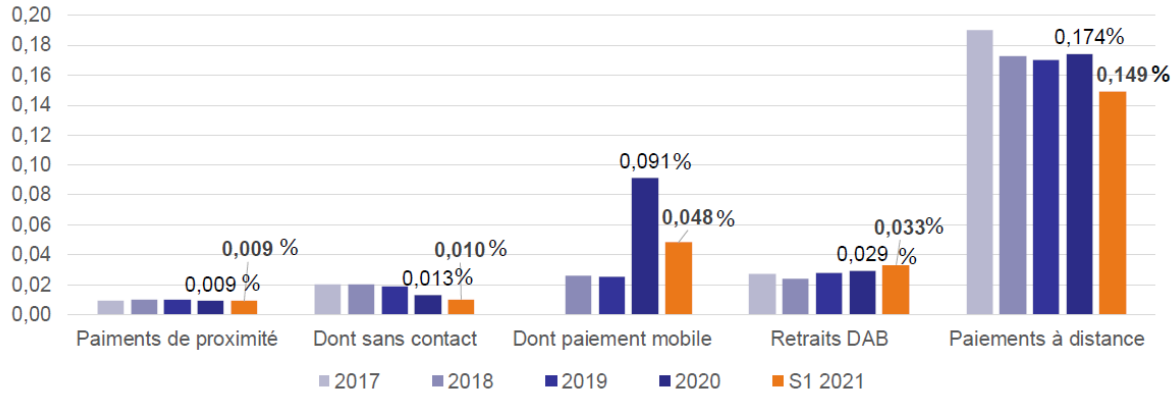
644 millions d'euros de fraude



3,6 millions de cas de fraude



Évolution des taux de fraude sur la carte par canal d'initiation pour les transactions nationales



Un taux de fraude en baisse depuis la mise en place de l'authentification forte : pour 1000 transactions à distance, combien de fraudes ?

Quels sont les risques lors d'un achat avec paiement sur Internet ?

2 grands risques sont occasionnés par de faux sites marchands

1. **Arnaque sur les produits achetés** = le site débitera votre compte mais ne vous enverra pas vos produits ou vous enverra un produit non conforme.
2. **Se faire voler des données personnelles**, ce qui ouvre la porte vers différentes arnaques :
   - usurpation de compte : ouvre la possibilité d'achats par des escrocs avec vos moyens de paiement : produits livrés à d'autres adresses, achats de moyens de paiement anonymes (équivalents à des retraits), ou même virements sur d'autres comptes bancaires
   - blocage de certains de vos comptes en ligne avec ou pas demande de rançon (risque pas forcément lié à un achat sur Internet – tout type de compte en ligne peut être concerné)

Quels sont les risques lors d'un achat avec paiement sur Internet ?

- **Le risque existe à partir du moment où vous remplissez un formulaire** = communiquer des informations personnelles pouvant être utilisées par d'autres.
  - vos coordonnées personnelles (nom, adresse, tél , email, etc)
  - vos numéros de carte bancaire (N°, date exp, code de vérif)
  - un mot de passe (si vous êtes amenés à créer un compte sur le site d'e-commerce)

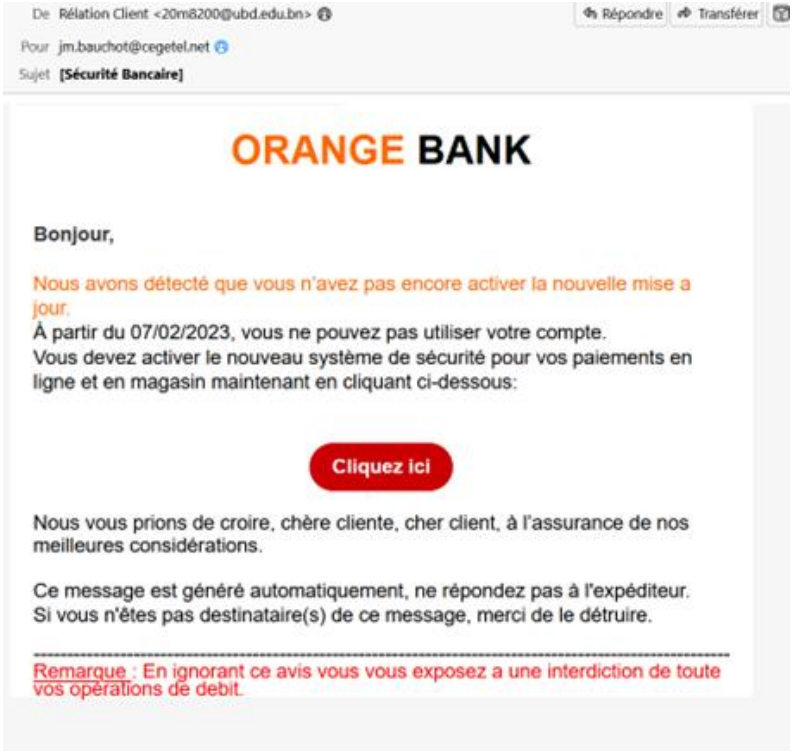
    → exemple de formulaire page suivante

- Plus rare, voire rarissime :
  - piratage des bases de données de vos fournisseurs en ligne (= fuites de données : vérifier sur https://monitor.firefox.com et changer mots de passe de votre compte concerné)
  - interception de vos données lors de leur envoi (pour s'en prémunir, possibilité d'utiliser VPN Virtual Private Network qui crypte les données envoyées. Gratuit ou payant)

Exemple de formulaire frauduleux

le lien en rouge ci-dessous conduit vers :
https://medicationland.com/indexx.php
(*NB : attention à ne pas aller sur ce lien sans précautions, notamment antivirus à jour)*

Ce site frauduleux imite l'apparence d'un site Orange Bank, mais l'invitation à compléter le formulaire ci-dessous, amène à un autre formulaire visant à récupérer vos données personnelles



De Rélation Client <20m8200@ubd.edu.bn>
Répondre Transférer
Pour jm.bauchot@cegetel.net
Sujet **[Sécurité Bancaire]**

ORANGE BANK

Bonjour,

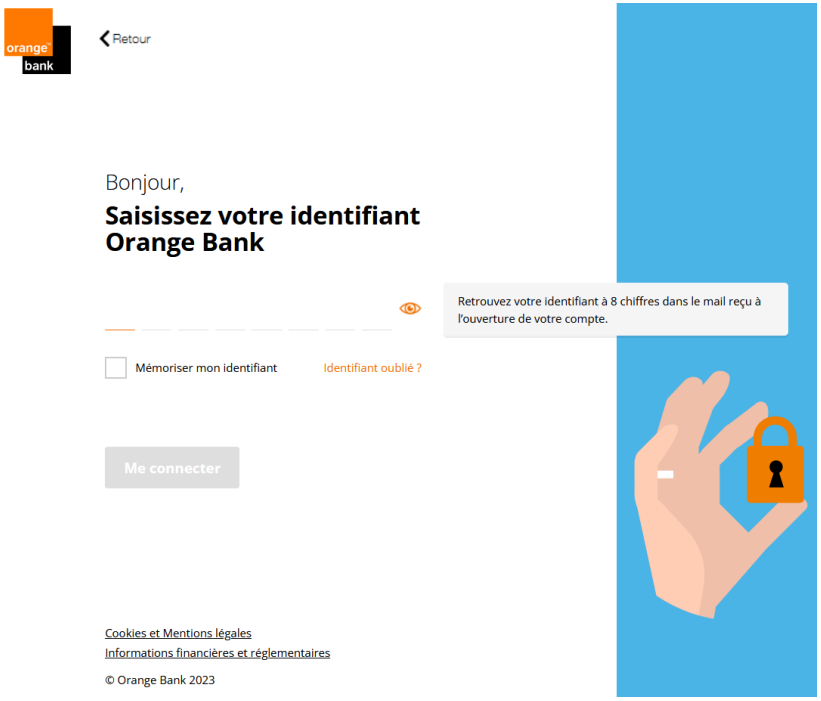
Nous avons détecté que vous n'avez pas encore activer la nouvelle mise a jour.
À partir du 07/02/2023, vous ne pouvez pas utiliser votre compte.
Vous devez activer le nouveau système de sécurité pour vos paiements en ligne et en magasin maintenant en cliquant ci-dessous:

Cliquez ici

Nous vous prions de croire, chère cliente, cher client, à l'assurance de nos meilleures considérations.

Ce message est généré automatiquement, ne répondez pas à l'expéditeur.
Si vous n'êtes pas destinataire(s) de ce message, merci de le détruire.

Remarque : En ignorant ce avis vous vous exposez a une interdiction de toute vos opérations de debit.



orange bank
Retour

Bonjour,
Saisissez votre identifiant Orange Bank

Retrouvez votre identifiant à 8 chiffres dans le mail reçu à l'ouverture de votre compte.

Mémoriser mon identifiant
Identifiant oublié ?

Me connecter

Cookies et Mentions légales
Informations financières et réglementaires
© Orange Bank 2023

L'ETAPE
LE NUMERIQUE POUR TOUS

Les bonnes pratiques pour limiter les risques

1. Vérifier les dispositions prises par votre banque en matière de sécurité des achats
2. Avant de passer à l'achat : Vérifier la fiabilité du site d'e-commerce
3. Au moment de l'achat : vérifier certains paramètres

Vérifier les dispositions prises par votre banque en matière de sécurité des achats

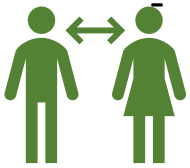
- Toutes les banques européennes sont désormais tenues de mettre en place une **procédure d'authentification forte**. Connaissez-vous celle qui est mise en place par votre banque ? Les plus connues consistent à valider votre achat effectué avec votre carte sur votre Smartphone, via l'application de votre banque.
- La DSP2 (Directive Européenne sur les services de paiement) prévoit cependant des exemptions à cette authentification forte dans certains cas comme les petits montants, les achats « habituels » (habitudes d'achat), les commerçants « sans risques » …
- **Limiter vos plafonds d'achats par Internet** (possibilité de les augmenter ponctuellement) ou même bloquer les paiements à distance quand vous n'en n'avez pas besoin.

- **Les garanties bancaires** en cas de fraude : la loi prévoit que votre banque vous rembourse une somme prélevée non autorisée par vous, sauf en cas de "négligence grave" de votre part. En pratique, pas toujours évident …

Avant de passer à l'achat : Vérifier la fiabilité du site d'e-commerce

- **Préférez les sites d'e-commerce connus et réputés :** c'est l'assurance d'être en face de vrais e-commerçants et de procédures internes plus sécurisées chez le commerçant.
- Pour un site d'e-commerce peu connu ou que vous ne connaissez pas déjà, **vérifiez la réputation du site** : https://fr.trustpilot.com, https://franceverif.fr , www.avis-verifies.com/fr/ ,ou même www.tripadvisor.fr

  Les avis peuvent être à prendre avec du recul, les mécontents s'expriment beaucoup plus souvent que les personnes satisfaites. Les commerçants ont cependant la possibilité de répondre publiquement au cas par cas sur ces sites.
- **Vérifier l'adresse, le téléphone du site – dans les mentions légales** (et même appeler ce numéro si vous n'êtes pas sûr) = la possibilité de se retourner légalement et "facilement" contre le site.



L'ETAPE
LE NUMERIQUE POUR TOUS

Exemple
https://www.edf.fr/ et pas
http://www.monagences-bleuciel.fr

Au moment de l'achat : vérifier les paramètres suivants

- **Vérifier la cohérence de l'adresse du site web** sur lequel vous êtes (éviter le « site miroir »)
- Un **cadenas** doit être présent dans la barre d'adresse et l'adresse du site doit commencer par **HTTPS** (et non http) , pour garantir que vos données , si elles sont interceptées par un tiers , ne sont pas lisibles.

- Il est difficile de s'assurer des procédures et systèmes mis en place par l'e-commercant, car s'il est un escroc, il peut donner à sa page l'apparence et tous les signes du sérieux. En principe, un commerçant qui utilise le système 3D secure appelé « Verified by Visa » ou « Mastercard SecureCode » devrait faire apparaître le logo de ces applis , mais dans la réalité il est introuvable.

- La CNIL déconseille d'enregistrer sa carte bancaire pour une utilisation ultérieure
- Si vous avez des doutes mais que vous achetez quand même : gardez des "preuves" de votre achat comme des copies d'écran.

Les bonnes pratiques pour limiter les risques

Plus généralement 1/2

- **Ne pas cliquer sur des offres qui vous arrive par des spams**. Ou par des publicités sur des réseaux sociaux. Voire même par SMS. et ne pas ouvrir de pièces jointes quand vous ne savez pas ce que c'est.
- **Mettre à jour ses logiciels**, dont son anti-virus (anti-malware) et son anti-phishing (hameçonnage)
- **Ne pas utiliser les mêmes mots de passe pour différents comptes :** il est courant d'utilisez pour différents comptes en ligne un même identifiant, qui est votre adresse mail. Si vous créez un compte sur un site d'e-commerce douteux avec le même mot de passe que sur vos autres comptes (google, edf, etc .) vous donnez la possibilité au « pirate » **d'entrer sur tous vos comptes** à votre place. Même d'acheter à votre place sur des sites d'e-commerce que vous fréquentez, notamment si vous y avez enregistré votre carte bancaire.

Jojo457

Exemple sarhada@store.mymodernmet.com qui écrit en se prétendant Pôle Emploi ou info@kudichobousa.com qui dit être la Française des Jeux

Les bonnes pratiques pour limiter les risques

Plus généralement 2/2

- En cas d'échanges par mail, bien **vérifier la cohérence de l'adresse mail** de votre correspondant.
- Il arrive qu'un e-commerçant ait des opérateurs pour vous aider à acheter (ex. SNCF, location de véhicule etc etc) : Si vous avez une démarche d'achat - ou même une caution à déposer - à réaliser par téléphone. Dans ce cas, on vous demande vos N° de carte bancaire : **c'est à vous à appeler le service sur son numéro de tél officiel et ne jamais communiquer d'infos – surtout pas bancaires - au téléphone si on vous appelle** … soit-disant au nom de tel ou tel site ou service.
- **Vérifier ses comptes bancaires régulièrement** et appeler sa banque en cas de doute.
- Et bien sûr : **ne pas se faire voler son téléphone** ! Et le **verrouiller** avec un code sérieux ou une procédure de type empreintes digitales, schéma de verrouillage.

Que faire si vous êtes victime d'une arnaque ?

- **Démarches vis-à-vis de sa banque**

  - **faire opposition** immédiatement si vol identifiants de carte bancaire
  - Dans un délai assez rapide, **demander le remboursement** des sommes indûment utilisées. Les banques sont tenues de vous rembourser … si vous avez pris les précautions d'usage avant de livrer vos identifiants.

- **Démarches vis-à-vis des autorités de police**

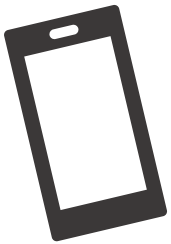
  - Selon la somme qui vous a été dérobée, vous pouvez déposer une plainte. Cela peut se faire en ligne : système Thésée à retrouver et accès sur France Connect (Traitement harmonisé des enquêtes et signalements pour les e-escroqueries) via https://franceconnect.gouv.fr/nos-services --> rubrique "argent" (fait suite à la précédente plateforme Perceval)

L'ETAPE
LE NUMERIQUE POUR TOUS

Pas besoin de renseigner un numéro de carte bancaire

les alternatives au paiement en ligne par carte

- **Virement bancaire** : simple efficace, souvent gratuit. Nécessite quelques jours avant validation, sauf virement immédiat mais souvent payant d'une banque à une autre. **Sécurisé à condition d'être absolument certain du N°IBAN du destinataire du virement.**
- Nouveaux modes de **paiement par téléphone**, Il suffit d'entrer le numéro de téléphone de votre « vendeur » ou de votre ami à rembourser et vous pouvez lui virer la somme convenue.
  - **Paylib** : développé par les banques par association de votre carte bancaire avec votre N° de téléphone. Souvent utiles pour des petits achats, de type particulier à particulier, vers un professionnel indépendant etc. vérifier si votre banque le propose. Nécessite un smartphone. Gratuit.
  - Systèmes de paiement proposés par des prestataires de services de paiement. Services possiblement payants. B**asés sur une réserve d'argent** (**Paypal**) = porte-monnaie en ligne) ou **l'ouverture d'un compte** (**Lydia**) (Possibilité aussi d'éditer une carte de paiement virtuelle).



L'ETAPE
LE NUMERIQUE POUR TOUS

Webographie

- Des guides pratiques publiés par la Fédération bancaire française (FBF) pour se prémunir contre les fraudes :
  - https://fr.calameo.com/read/002024705674a536b8d4e **sur les achats en ligne**
  - https://fr.calameo.com/read/00202470578f5e175e7c2 **sur les Cartes bancaires**

- Un **guide de prévention** publié par la task force nationale de lutte contre les arnaques, accessible par exemple ici **:** https://acpr.banque-france.fr/sites/default/files/medias/documents/vf20220719_cp_task_force_anti_arnaques.pdf

- Pour adopter un **nouveau moyen de paiement** : **un site très pédagogique** présente diverses solutions : https://www.lafinancepourtous.com/ → plus particulièrement les nouveaux moyens de paieme(publié par Institut pour l'Education Financière du Public (IEFP) nt dans la rubrique: https://www.lafinancepourtous.com/pratique/banque/moyens-de-paiement/)