

## VOL DE COORDONNÉES BANCAIRES : DES MANOEUVRES SIMPLES ET QUASI-INVISIBLES

«En consultant mon relevé de compte, j'ai découvert que des opérations avaient été réalisées à mon insu avec les références de ma carte bancaire».

### PROTECTION DES COORDONNÉES BANCAIRES : LES RÈGLES DE VIGILANCE

#### 1. Sur Internet

- Je réalise mes achats **uniquement sur les sites de confiance**, signalés par le logo et dont l'adresse commence, au moment de la transaction, par «https»
- J'évite le piratage de ma carte bancaire en protégeant mon ordinateur avec un anti-virus, un pare-feu et un logiciel anti-espion à jour

#### 2. Les automates (distributeurs de billets)

- Je compose discrètement mon code et masque le clavier avec ma main
- Je ne me laisse pas distraire par des inconnus qui proposent leur «aide» ; il s'agit souvent d'escrocs qui cherchent à subtiliser ma carte et récupérer mon code secret.
- Si la carte reste bloquée dans l'automate, s'adresser uniquement au guichet ou appeler votre centre d'opposition

#### 3. En magasins

- Numéro de carte bancaire + date d'expiration + cryptogramme = danger !  
*Dans le cadre d'une transaction en magasin, il est très facile pour l'escroc d'identifier ces numéros et de les noter. Ces références sont suffisantes pour effectuer des achats en ligne.*
- Je ne quitte jamais des yeux ma carte bancaire, je ne la confie à personne
- Je ne conserve pas mon code secret au même endroit que la carte

- 4. De manière générale,  
je suis les conseils de mon banquier

## L'ESCROQUERIE : CE QUE DIT LA LOI

Extraits

### Article L313-1 du Code Pénal

«L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende».

### Si vous êtes victime, portez plainte

Si vous êtes victime d'une escroquerie, déposez plainte au commissariat ou à la gendarmerie la plus proche.

Munissez-vous de tous les renseignements en votre possession :

- références du ou des transferts d'argent effectués,
- références de la ou des personnes contactées : adresse de messagerie ou postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels/courriers échangés...,
- tout autre renseignement pouvant aider à l'identification de l'escroc.

## POUR TOUT RENSEIGNEMENT

**0 811 020 217** (coût d'un appel local)

Pour signaler un courriel ou un site internet d'escroqueries  
[www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)



# 3740

## Infractions et escroqueries économiques et financières en 2010 dans le Doubs



## Restez vigilants Ne soyez pas victimes

## INFO ESCROQUERIES

**0 811 020 217** (coût d'un appel local)

Pour signaler un courriel ou un site internet d'escroqueries  
[www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)



# Zoom sur quelques escroqueries dans le DOUBS



## Secteur Saint-Vit 2010

Annnonce sur un site de vente entre particuliers d'une moto. Le vendeur sollicite un mandat cash western union pour la transaction car il se trouve actuellement en mission professionnelle à l'étranger. Le véhicule doit arriver par l'intermédiaire d'un transporteur. Il n'arrivera jamais et le mandat cash sera encaissé dans un pays d'Afrique francophone. PREJUDICE : 2300 €

### Que faire ?

Ne pas régler de transactions via Internet avec des mandats cash western union lorsque vous ne connaissez pas votre intermédiaire. Ne pas répondre aux offres trop alléchantes sans vérifications préalables.



## Secteur Besançon 2010

Une étudiante de Côte d'Ivoire envoie un mail sollicitant de l'aide afin de transférer une malle contenant une très forte somme d'argent. En contrepartie, elle propose d'indemniser fortement son mecène. L'argent est envoyé pour le transfert de la malle mais suite à des problèmes techniques celle-ci ne peut partir et d'autres sommes d'argent sont ainsi sollicitées. Il s'agit bien évidemment d'une escroquerie grossière. PREJUDICE 8000 €

### Que faire ?

Ne jamais répondre à des sollicitations de ce type ni confier de l'argent à un inconnu.



## Secteur Morteau 2011

Une victime constate plusieurs prélèvements manifestement frauduleux sur ses relevés bancaires. Il s'agit d'achats effectués par usage de ses coordonnées bancaires. Elle se souvient avoir reçu quelques jours auparavant, un mail de son fournisseur d'accès, l'informant d'une erreur sur son compte client. Afin de se faire rembourser elle devait renseigner un formulaire obtenu à partir d'un lien sur le mail

### Que faire ?

Il s'agit d'un cas de phishing. Il ne faut jamais communiquer de données sensibles en réponse à un mail. Il ne faut pas transmettre de coordonnées bancaires sur un site non sécurisé.



## Secteur Besançon 2010

Une victime vient de se faire voler son sac à main contenant chéquier, carte bancaire, et de fidélité.

### Que faire ?

Sans tarder, appelez votre banque ou l'organisme financier gestionnaire de votre carte pour faire opposition sur les cartes et les chèques volés

Plus généralement, pour éviter d'être victime de vol, ne laissez jamais votre sac ou votre portefeuille sans surveillance (dans un caddy, sur un comptoir ou une table de bar, dans une veste laissée sans surveillance, etc.) ; ne laissez jamais sacs, vestes, portefeuille dans votre véhicule

Pour éviter le vol de vos chèquiers ou de vos cartes bancaires dans les boîtes aux lettres, exigez de votre banque un envoi par recommandé ou retirez les à votre agence bancaire.

Ne jamais communiquer votre code de carte bancaire à personne même à votre banque.



## Secteur Besançon 2011

A la lecture de son relevé bancaire, une victime s'aperçoit que des paiements dont elle n'a aucun souvenir ont été réalisés avec sa carte bancaire ; elle est toujours en possession de sa carte et elle a la certitude de ne pas être à l'origine de ces paiements.

Un malfaisant est parvenu à se procurer son numéro de carte à son insu.

### Que faire ?

Ne pas abandonner sur la voie publique ou dans les commerces la facturette de ses achats ; sur celle-ci figure une partie des informations qui permettront à certains escrocs de reconstituer votre n° de carte et de l'utiliser sur internet

Quand vous effectuez des achats sur internet, utilisez des sites grand public, utilisez des sites sécurisés (https)

Méfiez-vous des achats sur des sites étrangers ; en cas de problème ou de contestation vous n'aurez aucun recours efficace



Le phishing est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.

Le mail (rédigé en langue anglaise ou française) usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et invite les internautes à se connecter en ligne par le biais d'un lien hypertexte. Il leur est demandé de mettre à jour des informations les concernant sur un site Web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de chance d'aboutir puisque l'internaute n'est peut être pas client de la banque dont semble provenir le courriel. Mais sur la quantité des messages envoyés, il arrive que le destinataire soit effectivement client de cet organisme.

Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes, leurs données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.)

Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte.

### Que faire ?

Ne cliquez jamais directement sur le lien contenu dans le mail, mais ouvrez votre navigateur et saisissez vous-même l'adresse URL d'accès au service.

Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare (voire impossible) qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute, contactez directement votre agence par téléphone.

Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par *https* et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur.



## NUMÉROS UTILES

Carte de crédit perdue ou volée

0 892 705 705

Opposition chéquier

0 892 683 208

