INGENIEURS ET SCIENTIFIQUES DE FRANCE
Organisme reconnu d'Utilité Publique depuis 1860
UNION REGIONALE DES INGENIEURS ET SCIENTIFIQUES
DE FRANCHE COMTE

Compte-rendu du Bar des Sciences du lundi 8 avril 2013 «Fraude à la carte bancaire et sécurité des banques » … des escrocs invisibles…

Soirée organisée par : le **« Pavillon des Sciences »** et animée avec dynamisme par **Pascal REMOND**.
Lieu - Horaire : Bar de **l'Hôtel Bristol** – 2, Rue Velotte - 25200 MONTBELIARD – **le lundi 8 avril 2013 - de 20h00 à 22h30**

Participation : bonne, environ **100 personnes** étaient dans la grande salle du haut.

Participants URIS FC : Jean-Pierre BULLIARD (INSA) – Gérard BULLIARD (UTBM) - Joseph CAVALLIN (AM) et d'autres non identifiés.

Intervenants :

- **Pierre PIAZZA** - Sociologue, CNRS - Sciences politiques – Université de Cergy-Pontoise et CESDIP/Lejep –Paris. Maître de Conférences. S'intéresse A l'identification et à la traçabilité des personnes.
- **David FOREST** - Avocat, spécialiste du "Droit de la société et de l'information", Barreau de Paris. Intervient dans le droit du numérique, le droit de l'immatériel (technologies de l'information)
- **Major Didier DOUILLY** - Direction Générale de la Gendarmerie Nationale, Bureau de la Lutte contre la cybercriminalité – Paris. A déjà participé à 2 autres Bars des Sciences, en particulier sur la contrefaçon.

Contexte de cette soirée :

Les arnaques en tout genre se multiplient. C'est une véritable économie clandestine qui au plan mondial coûterait 284 milliards d'euros ! Le Net est le terrain de chasse favori de ces escrocs invisibles.
L'éventail des menaces est large : usurpation d'identité, vol de données bancaires, espionnage industriel et même attaque de Pays… Mais toute arnaque si grande soit-elle, débute toujours par le vol de données personnelles.
Or nos données, c'est nous qui, chaque jour, donnons gentiment notre laine à ceux qui nous la vendent pour le mieux ou nous la vole pour le pire. Combien donnons-nous de renseignements rien que pour l'achat d'un téléphone portable. Avec ces données volées laissées çà et là, n'importe qui peut devenir usurpateur, voleur, escroc… Et toutes les méthodes sont bonnes :
-Fouiller les poubelles reste une bonne vieille recette pour trouver des infos laissées par un imprudent, la technicité de notre société fera le reste. Notre téléphone portable par exemple est aussi un merveilleux mouchard. Autre exemple : une étude britannique affirme qu'il est possible d'en apprendre beaucoup sur les internautes en fonction de leurs clics sur les boutons «j'aime» de Facebook.
-Plus grave encore : en juin 2012, Yahoo! Reconnaît s'être fait voler 450 000 mots de passe; la CNIL dans son rapport du 27 juillet 2012 établi que dans la même base de données de la Société « FNAC Direct » apparaissent le nom du porteur de la carte, son numéro de carte bancaire, la date d'expiration de celle-ci et son cryptogramme visuel en clair. C'est rassurant !
-Il y a déjà trois millions de cartes bancaires sans contact en circulation en France, sept millions d'ici la fin de l'année. Une personne mal intentionnée équipée d'un simple Smartphone piraté ou d'une clé USB qui fonctionne à distance peut changer la donne et ainsi vous voler la somme désirée, affirme un récent rapport sur le sujet…
Comment concilier nouvelles technologies et respect de la vie privée ? Comment concilier la sécurité de notre identité, la sécurité des banques, la sécurité des états … et notre liberté ? Comment vivre dans cette société numérique en restant prudent et libre ? C'est ce à quoi le Bar des sciences s'attachera à répondre.

Les Bars des sciences sont financés par Pays de Montbéliard Agglomération.

Déroulement de la soirée :

Pierre PIAZZA débute la soirée en présentant les **origines de la police scientifique** qui doit beaucoup à **Alphonse Bertillon**, né à Paris le 22 avril 1853 et mort à Paris le 13 février 1914. Il est un criminologue français qui fonda en 1870 le premier laboratoire de police d'identification criminelle et inventa l'anthropométrie judiciaire, appelée « système Bertillon » ou « bertillonnage », un système d'identification rapidement adopté dans toute l'Europe, puis aux États-Unis, et utilisé jusqu'en 1970. On lui doit, en particulier, le développement du fichage et la photo face/profil.

Le Major Didier DOUILLY demande aux participants : qui a été confronté à un problème de capture de données bancaires utilisées sur internet ? 8 personnes sur la centaine présente lèvent le doigt et répondent par l'affirmative. Ce mini-sondage est révélateur d'un problème réel prenant de l'ampleur. Le Major développe alors les **deux fraudes principales** :

1) **La fraude « classique » de piratage des données de la Carte Bancaire (CB) par installation d'un système électronique sur les DAB (Distributeurs Automatiques de Billets)**, avec un processeur et une caméra qui filme le code PIN au moment où on l'introduit avec le doigt. Ces fraudeurs recréent de fausses Cartes Bancaires avec les données lues sur la piste magnétique (pas celles contenues dans la puce) et vont faire des retraits immédiats à l'étranger. Ce type de fraude existe aussi sur les Distributeurs Automatiques d'Essence dans les Stations Services. Ces fraudeurs ne captent que les données de la piste magnétique de la CB, et **pas les données EMV** (Europay Mastercard Visa) présentes **sur la puce**.

Comment s'en rendre compte ? On ne voit la fraude qu'en recevant les relevés bancaires un ou deux mois plus tard. Par exemple, un retrait « pirate » fait à Taiwan alors qu'on n'a jamais été dans ce pays. La difficulté est qu'on a du retard quand on s'en aperçoit.

Quelle démarche doit-on suivre ? Souvent on est appelé par le banquier avant même de s'être rendu compte de la fraude par soi-même. Notre banquier connait nos habitudes d'achat avec notre CB, nos habitudes de voyage. On est pisté en permanence et les systèmes bancaires permettent de déceler des anomalies d'achat. Si on lui prouve notre bonne foi, le banquier a l'obligation de nous rembourser, car notre système bancaire de CB est sécurisé. Ces pirates, lorsqu'ils s'attaquent à une région, font en général une dizaine de larcins de ce type et la gendarmerie voit alors affluer les plaignants.

Quelle peut être notre action dans cette lutte contre les escrocs à la CB ? Il faut en permanence se méfier lorsqu'on utilise un DAB **: jeter un œil critique sur ce distributeur**, voir s'il y a quelque chose d'anormal (par exemple de la présence de colle). Il faut **signaler à la banque ou à la gendarmerie** tout élément suspect concernant le DAB. Les banques font une certaine observation de leurs DAB mais pas le banquier directement : elles utilisent un « **Dabiste** », chargé de recharger les DABs et il peut y avoir un décalage dans leurs observations car ces Dabistes ne rechargent pas les DABs chaque jour (pas le week-end en particulier).
Autre action : mettre la main au dessus du clavier pour **cacher le code pin introduit**.

Conséquences d'une telle fraude : la CB incriminée sera annulée, la banque y faisant opposition et l'on sera pendant un temps sans carte bancaire en attendant la réalisation d'une nouvelle carte. La victime devra **justifier l'ensemble de ses achats précédents** avec la CB piratée. Un participant signale qu'on réalise des achats avec notre CB dans les pays étrangers en utilisant le système « fer à repasser ». Ces achats se pratiquent de moins en moins. La carte copié est appelée « **White Card** » (Carte Blanche) : elle ne contient qu'une piste magnétique avec vos données.

David FOREST précise qu'il faut **bien surveiller ses relevés de compte CB**. Il a lui-même été débité de 400 Euros par une transaction en Italie où il n'est jamais allé. La banque l'a remboursé. Mais la suite est intéressante car **on rentre alors dans un fichier de police : le STIC (Système de Traitement des Infractions Constatées)** qui recense toutes les victimes, toutes les mises en cause suite à infractions de tous ordres, suite à enquêtes. Ce fichier a, autrefois, été créé dans l'illégalité. Il a été ensuite légalisé au bout de plusieurs années d'utilisation et il est devenu énorme, tentaculaire, finissant par échapper au contrôle de ses maîtres : **83% d'erreurs** ont été détectées dans ce fichier par une **commission d'enquête**, des victimes ayant été transformées en coupables. David souligne la **nécessité d'encadrer et de manipuler ces fichiers avec rigueur.**

Pierre PIAZZA complète ces affirmations en signalant que **la gendarmerie** a un fichier équivalent au STIC de la police : c'est les **Fichier des Antécédents**. La police a besoin de ces fichiers. **Le problème est le contrôle de ses contrôleurs**. Il existe aussi un problème de **détournement de finalité**. Le fichier servait au départ pour savoir si la personne était dangereuse ; il est devenu ensuite **un fichier d'enquête de moralité** pour autoriser, par exemple, le travail dans une société de sécurité privée. Il est alors utilisé comme un **véritable casier judiciaire**. Une autre question se pose également : la police est-elle plus efficace dans son travail en se servant d'un tel fichier truffé d'erreurs ?

Le Major Didier DOUILLY indique que **la fraude à la CB en France représente 310 Millions d'€ par an**. En % des transactions, c'est très faible car cela ne représente que **0,03% des sommes échangées par CB**.
Ce taux est à peu près le même dans tous les pays du monde. Par contre, pour les constructeurs de DAB, ce n'est pas bon car leur produit n'est plus considéré comme inviolable (par exemple : DIEBOLD construit des DAB en Allemagne). **Le système piratant les DAB s'appelle un « skimmer ».** La capture de données bancaires est le **« skimming ».** Les constructeurs ont alors rajouté des **dispositifs « antiskimming »** à leurs DABs (par exemple un voyant vert qui clignote ou un cadre métallique) mais les pirates volent les nouveaux DABs pour étudier ces systèmes et les violer. Pour le Major, **il manque des informations aux clients concernant les DABs.** Ces informations sont **très difficiles à fournir par les banques** car, implicitement, cela reviendrait à admettre que les DABs et les CB ne sont pas fiables. Il manque donc beaucoup d'informations aux utilisateurs concernant les risques à la CB. Signalons **qu'un commerçant peut refuser un paiement de faible valeur avec une CB** car il pourrait avoir des frais supérieurs au montant de l'achat et il perdrait donc de l'argent.

Le Major détaille alors **la 2ème sorte de fraude à la CB :**

2) **La fraude à la CB via internet.** Cette fraude est **très difficile à détecter**. La fraude la plus connue consiste à faire des achats sur internet sur le compte de votre CB sur des sites de vente à distance. En fait, les données bancaires du possesseur de CB ne sont pas piratées directement sur internet mais plus par un contact « physique » : on va faire le plein d'essence dans une station service la nuit sur l'autoroute, le réceptionniste vous demande votre carte au moment du paiement, confiant, vous la lui donnez un instant qui suffit à la copie de son numéro et de son cryptogramme au verso … et votre CB est ainsi piratée même si vous la récupérez ensuite. Ses données vont servir au malfrat à faire des achats sur internet (qui ne demande pas le code secret dans la bande magnétique ou la puce mais seulement les caractères supplémentaires du cryptogramme au verso). Le même type de piratage peut se faire au restaurant si vous la donnez : vous courrez alors le risque de vous la faire recopier sous le comptoir avec le code cryptogramme au verso. **Ce code cryptogramme au verso de la CB a la même valeur que le code pin de la carte demandé au DAB.** Le cryptogramme est le code confidentiel de la CB pour faire un achat sur internet. **Un conseil : cacher ce cryptogramme au marqueur** indélébile après l'avoir retenu par cœur.

Possibilité de sécuriser ses achats sur internet : utiliser **une E-CB (Carte Bancaire Electronique).** Elle vous est attribuée sur internet **pour un achat unique** et ne sert donc qu'une seule fois. Avant l'achat, on fait une déclaration sur internet qui vous affecte un numéro servant de code de CB unique. Il faut que le site d'achat accepte ce type d'E-CB, ce n'est pas le cas chez tous les commerçants par internet. Par ailleurs, **de nombreux sites sécurisés existent** (adresse commençant par **https – « s » comme « sécurisé »)** qui donnent de **bonnes garanties sécuritaires**. Une autre possibilité existe aussi pour certains achats sécurisés sur internet : **envoi d'un code par sms** pour **vérifier votre identité** et **confirmation par appel téléphonique** avant accord sur les données bancaires que vous remplissez sur internet lors de votre achat.

Fraudes mafieuses : Attention : il faut savoir que **votre commerçant**, même s'il fournit une facture barrant les premiers numéros de votre CB, **a, lui, ces numéros en clair** : s'il fraude, il peut ainsi vous pirater vos données de CB en prenant votre cryptogramme et peut ainsi commander sous votre nom sur internet. S'il se fait alors livrer la marchandise, on pense qu'on va pouvoir le prendre facilement. Ceci est faux car **il existe de véritables réseaux maffieux très bien organisés** : ils sont placés dans ces commerces pour récupérer vos données CB (station service, Mac Donald…). Dans la demi-heure qui suit le piratage de vos données, votre CB est utilisée pour des achats sur internet (nota : pas de panique ! Si on s'en rend compte, **le banquier est tenu de vous rembourser**) puis la livraison est faite quelque part : ces pirates vont **usurper sur internet des identités et adresses réelles** (en utilisant facebook ou copains d'avant…) : ils vont obtenir un nom, prénom et une adresse et vont guetter le facteur sur le trottoir à l'arrivée du colis et récupérer le matériel. **La problématique est que tout le monde met ses renseignements personnels sur internet et qu'on alimente ainsi les fraudeurs.**

Question d'un participant : doit-on prendre les mêmes précautions en utilisant notre CB à l'étranger ? Le Major répond **« oui » pour les DABs à l'étranger**. Il signale aussi que certaines banques avaient un sas qui s'ouvrait par passage de votre CB devant un lecteur de carte. Il y avait aussi des skimmers sur ces sas et vos données de CB étaient ainsi piratées.

Question d'un participant : existe-t-il un délit d'usurpation d'identité ?
David FOREST répond que, dans le code pénal, il existait une **incrimination difficile à appliquer pour internet car il faut prouver que l'usurpateur a pour but de faire une infraction**. Il n'y a pas forcément de délit car, sur internet, on peut, en toute légalité, se faire passer pour autrui. **Une loi récente a été faite pour l'usurpation d'identité numérique**. Mais cette identité numérique n'a pas été définie (nom, prénom, identifiants) et on a ainsi créé cette nouvelle infraction sans définir son objet. Par exemple, sur facebook, je peux créer une page en me faisant passer pour mon idole (« des jeunes ») et bénéficier de ses relations.

Autre exemple d'usurpation d'identité : le « phishing » ou hameçonnage, et, plus rarement filoutage, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques. Par exemple, les pages d'accueil d'Orange, de LCL, des impôts, de la CAF… falsifiées sont pratiquement identiques aux pages réelles, ce qui crée la confusion chez l'internaute qui les reçoit. **Conseil : ne jamais donner ses numéros de code de CB sur internet ni partout ailleurs, aucune banque ne peut vous les demander.** Ces fraudeurs font des milliers d'envois frauduleux et, sur la quantité, récupèrent des dizaines de données des CB qu'ils vont ensuite utiliser pour faire des achats via internet. Parfois, ils essaient la menace pour arriver à leurs fins (ils vous disent : si, sous quinze jours, vous ne remplissez pas les données suivantes, vous serez interdit bancaire ! etc.). Ils sont **passibles du délit de contrefaçon** car reproduire un site bancaire est illégal (risque au maximum 5 années d'emprisonnement. Signalons qu'un adepte de trafic de stupéfiant risque 10 ans)

David FOREST indique qu'il a traité récemment un **dossier intéressant** : un père soucieux de l'avenir de son fils va le consulter. Ce fils a été pris **à 13 ans pour trafic de stupéfiant** (haschich). Il a fait l'objet d'une garde à vue qui s'est soldée par un **simple rappel à la loi** par le procureur de la république. « Ce n'est pas bien ! Voilà ce que tu risques si tu recommences !... ». Le jeune a maintenant 18 ans mais, depuis cette affaire, **ses données ont été introduites dans le STIC**, bien qu'il n'ait pas fait l'objet d'une condamnation **et que son casier judiciaire soit vierge**. **Le papa**, voyant son fils entrer à l'ENA, est inquiet et **souhaite que ses éléments dans le STIC soient effacés**. David demande qu'on lui amène le jeune homme. Il lui pose quelques questions comme : fais-tu du syndicalisme étudiant ? Et David essaie de s'attaquer au STIC. Mais cela est fort compliqué car **ces données sont tentaculaires**, **difficiles à contrôler**. David promet au père de faire ce qu'il peut mais il s'attaque à un mur infranchissable ! Il cherche cependant à savoir en quelle qualité le jeune homme est fiché dans le STIC. Il passe de nombreuses journées à étudier les lois qui ont conduit à l'élaboration de ce fichier. Il ne sait pas qui saisir pour demander l'effacement des données du fils. **Il saisit donc la CNIL (Commission Nationale d'Informatique et Liberté)** dans le cas de son **droit d'accès indirect**. La CNIL dépêche ses commissaires pour aller vérifier les données sur place. Cela dure 9 mois et ils n'y parviennent pas. On peut demander ce recours seul, ou par l'intermédiaire d'un avocat, ou par le procureur de la république. David appelle le secrétariat du procureur : « puis-je vous saisir pour cette affaire ? ». La réponse est : « Tentez votre chance ! » mais rien ne filtre et David ne pourra pas donner satisfaction à ce père.
Le législateur s'est saisi de ces difficultés : la **fusion du fichier STIC** (décret du 4 mai 2012 - CPP, art. R. 40-23 à R. 40-34), système de traitement des infractions constatées **de la police nationale** et le **système judiciaire de documentation et d'exploitation de la gendarmerie nationale (JUDEX),** et les **remplace par un nouveau fichier** de données à caractère personnel relatifs aux « antécédents judiciaires» : le **TAJ (Traitement des Antécédents Judiciaires).** Des magistrats spécialisés vont être missionnés pour effacer les données inutiles ou erronées. Le procureur a répondu rapidement à David et l'a conforté dans ses croyances **: il ne peut effacer car il s'agit d'un traitement d'antécédent**. C'est une **« mémoire policière » mais pas une condamnation**.

Pierre PIAZZA confirme que **le problème est le fichage par des opérateurs privés**. Il y a partout, avec internet, du **fichage** et du **profilage** : on connait parfaitement vos habitudes d'achat. Ce fichage a existé depuis longtemps (les juifs pendant la guerre, les français d'Algérie ensuite…). Il faut donc **mettre en place des dispositifs pour contrôler les contrôleurs et réguler tout cela.** Mais, quand le fichier fonctionne, on a du mal de faire machine arrière. La CNIL a trop de dossiers à traiter. **La production des données se fait**

à l'échelon international (données biométriques sur votre passeport aux USA…). Ce problème est lié à la mondialisation : il y a un vrai marché mondial des données. Le site FNAC.fr a laissé partir plus de 700.000 données concernant ses clients. On a volé 350.000 codes à YAHO. **Toute fraude à la CB passe par le vol des données personnelles de quelqu'un.**

Instruments mis en place par l'état pour ficher les identités : on cherche les aveux ou la mise en code (code unique). On fait parler le corps et l'on a ainsi des **caractéristiques physiques toutes différentes** d'un individu à l'autre (**iris de l'œil, empreintes digitales, ADN**…). La solution est-elle de vouloir coupler l'identité du corps avec ce corps lui-même ? (objet de la biométrie). On tend vers cela mais **cela pose bien des problèmes de liberté individuelle**. **Réduire la personne à son identité corporelle** satisfait cependant le secteur marchand.

Le Major Didier DOUILLY précise que l'on peut aller plus loin que la Carte Bancaire traditionnelle utilisée actuellement. On a du mal à imaginer vers quoi l'on se dirige en termes de paiement. Les grandes chaînes commerciales s'y dirigent avec les banques **: on parle maintenant de paiement sans contact**. Au travers du téléphone mobile, on va payer sans qu'il y ait besoin de présenter sa CB, elle peut rester dans notre poche. **Sur les nouvelles CB on a de nouvelles puces RFID** (de l'anglais **« Radio Frequency Identification »**). Il s'agit de la **radio-identification** qui est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés **« radio-étiquettes »** (« RFID tag » ou « RFID transponder » en anglais.
Les **radio-étiquettes** sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collés ou **incorporés dans des objets ou produits et même implantés dans des organismes vivants** (animaux, corps humain). Les radio-étiquettes comprennent **une antenne associée à une puce électronique** qui leur permet de recevoir et de répondre aux requêtes radio émises depuis l'émetteur-récepteur.
Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires.
Cette technologie d'identification peut être utilisée pour identifier :

- les objets, comme avec un code-barres (on parle alors d'étiquette électronique) ;
- les personnes, en étant intégrée dans les passeports, carte de transport, carte de paiement (on parle alors de carte sans contact) ;
- les carnivores domestiques (chats, chiens et furets) dont l'identification RFID est obligatoire dans de nombreux pays, en étant implantée sous la peau. C'est également le cas de manière non obligatoire pour d'autres animaux de compagnie ou d'élevage (on parle alors de puce sous-cutanée).

Ces puces sont basées sur la **même idée que le « pass » des transports parisiens**.
Le problème est **qu'à aucun moment la banque ne vous informe que vous avez une CB munie d'une radio-étiquette RFID**. **On a le droit de refuser à la banque ce type de paiement sans contact**. Sur internet on trouve même des logiciels vous permettant de dépasser les maximums d'argent disponibles avec votre CB. **Auchan développe un système pour payer en utilisant votre empreinte digitale :** votre empreinte est prise par la banque, arrivé en caisse, le système détecte sans contact la carte bancaire que vous avez dans votre portefeuille, vous n'avez donc pas à la présenter, vous présentez seulement votre doigt, l'empreinte est prise et comparée à vos données bancaires et les achats sont payés automatiquement.

Pierre PIAZZA précise que **la lutte contre la fraude est importante** et **qu'elle évolue en même temps que la fraude elle-même**. **On va ainsi dans le sens de profilage des individus**, ce profilage servant **à des fins policières et économiques**. Les principes de lutte ne vont pas à la même vitesse et sont **en retard sur les méthodes des fraudeurs** (exemple : le consentement). Les principes de finalité évoluent (la fin souvent change) ainsi que la proportionnalité (la fin doit justifier les moyens). La **Carte d'Identité Biométrique** a été **refusée au départ** par le Conseil de Surveillance. Faut-il « biométriser » des millions de personnes, toute une population, pour seulement quelques milliers de fraudeurs ?
Rappel : la Carte d'Identité en France (comme en Angleterre) n'est pas obligatoire mais on doit en permanence **être en mesure de prouver son identité**.

Le Major Didier DOUILLY indique **les nouveaux systèmes mis en place par les fraudeurs à la CB** : ils élaborent **des réseaux structurés pour récupérer les livraisons faites à partir d'usurpation d'identité**. Ils créent des **« mules »** qui sont des **personnes recrutées officiellement** sur internet, avec des contrats de travail en bonne et due forme, répondant à une offre d'emploi sur internet, emploi en CDI. **L'objet de l'emploi est de récupérer des colis chez vous, à votre adresse puis de les réemballer et les réexpédier soit par la poste soit par express à une liste d'adresse des fraudeurs**. Le **salaire est alléchant : 1500€ nets** par mois. Ceux qui répondent à ces annonces sont, évidemment, des personnes en misère sociale ou intellectuelle. La « mule » reçoit par mail un contrat de travail : on lui demande d'envoyer

une photocopie de sa carte d'identité, de sa facture EDF et de son RIB. Tout semble normal…Les colis arrivent chez la « mule » qui les réexpédie. Au bout d'un mois les choses se compliquent : la « mule » reçoit 1700€ (au lieu des 1500 annoncés dans le contrat de travail). La « mule » croit qu'elle a obtenu une prime. Ce virement arrive généralement un vendredi. Vous recevez un mail qui vous signale que c'est une erreur, on vous demande de renvoyer les 200€ de surplus par mandat cash. Le mardi, le banquier vous appelle et signale que les 1700€ ne sont pas versés car il s'agit d'un faux : votre identité a été usurpée et vous rentrez dans une spirale policière infernale. **Côté policier, la « mule » est officiellement un « receleur ». Côté humain, la « mule » est une victime**. Souvent la police abandonne les poursuites à son endroit. Mais, cependant, elle sera **rentrée dans le STIC** (comme mis en cause). Régulièrement on l'appellera car son identité a été usurpée et « clonée ». **Faisons donc attention aux annonces alléchantes sur internet.**

Un participant signale qu'il faut surtout se méfier des DABs entre la période du vendredi et du lundi. Il a lui-même réalisé une action volontaire (en plaçant sur 40 DABS de la région des repères ne devant pas s'y trouver) et il a prouvé ainsi que les Dabistes n'ont rien observé d'anormal du vendredi au lundi suivant, les repères suspects y figuraient toujours. L'entretien du DAB ne se faisant pas le week-end, c'est surtout dans cette période que les malfrats en profitent pour les truquer.

Le Major Didier DOUILLY confirme que **sur les sites sécurisés d'internet, il y a peu de chances de se faire pirater.**

Un participant, Bernard, demande pourquoi on ne contrôle pas les terminaux bancaires ? Le Major lui répond que **ce sont les DABs, en amont des terminaux, qui se font pirater**, pas les terminaux bancaires (les DABs ne sont que des périphériques associés aux terminaux bancaires). La fraude se produit donc avant le passage dans le terminal.

Une participante, Annette, demande s'il est vrai qu'en introduisant son code pin à l'envers dans un DAB on déclencha automatiquement une alarme de police ? Le Major répond que **cela est faux et fait partie des « arnaques » circulant sur internet.**

Le Major Didier DOUILLY nous informe que 10 personnes en France avaient créé des sites internet sur lesquelles **elles revendaient des informations bancaires piratées**. Chaque référence bancaire était revendue 5€. Des faux « grossistes » les rachetaient et les revendaient finalement à des particuliers pour 50€. Ces personnes ont été conduites sous les verrous.

Un participant demande si la gendarmerie a édité un fascicule expliquant ces fraudes à la CB ? Le Major confirme **qu'un dépliant a été envoyé à tous les brigadiers de gendarmerie** au sujet du piratage des CB par les DABs et par internet. Ce document est utile à chaque gendarme et lui sert pour accueillir correctement la victime et pour l'aider. **La gendarmerie a alors contacté la Fédération Bancaire Française pour que ce fascicule soit distribué à chacun à chaque renouvellement de CB**. Mais ils sont très réluctants, ayant du mal à reconnaître le manque de fiabilité de la CB.

Un participant indique un autre cas d'usurpation d'identité : un jeune **s'est fait pirater son numéro d'immatriculation de son véhicule.** Le malfrat ayant eu des amendes, celles-ci sont arrivées chez le vrai propriétaire qui a galéré pendant deux ans pour faire reconnaître son bon droit, malgré des attestations de son employeur prouvant qu'il était au travail pendant le temps où les infractions étaient commises.

Pascal indique qu'il va essayer de se faire réaliser une vraie fausse carte d'identité : il veut aller à la police déclarer qu'il a perdu sa carte d'identité. Il fournit de faux papiers de données piratées et demande une nouvelle carte…. Le Major lui conseille de ne pas faire cela dans son département d'origine !...

David FOREST cite une réflexion de **Louis JOINET**, ancien Président de la CNIL : « si les faux papiers n'avaient pas existé pendant la seconde guerre mondiale, la Résistance aussi n'aurait pas existé ! ».

Conseil donné par un participant pour réaliser par internet le visa vers les USA : aller sur un autre PC que le vôtre, et **utiliser une autre CB** que la vôtre (une CB d'un membre de votre famille). Cela désorientera les amalgames de fichiers et de données personnelles. Ceci est parfaitement légal et montre qu'on peut jouer sur les identités sans être dans l'illégalité.

Le Major Didier DOUILLY nous donne des informations supplémentaires concernant la vente à distance sur internet. Il est **compliqué pour la gendarmerie de déterminer le vrai point de compromission** en

cas de fraude. Où la CB a-t-elle été réellement usurpée ? Ils ont du mal de remonter au pirate mais y arrivent dans 20% des cas. En termes de **fraude au DAB ou au Distributeur Automatique de Carburant**, la gendarmerie essaie d'être proactive dans ces deux domaines. Ils repèrent un « skimming » installé sur une pompe de distribution d'essence. **Un réseau complet de malfrats bulgares est démantelé** : avec l'aide de la gendarmerie de Sofia, ils détectent 3 immeubles à Sofia, achetés par les malfrats qui y exerçaient leurs fraudes. Ces immeubles sont saisis, les malfrats emprisonnés. La gendarmerie bulgare a très bien collaboré avec la française. **La gendarmerie a alors travaillé avec les constructeurs de Distributeurs Automatiques d'Essence (Société TOKHEIM).** Ceux-ci ont créé de nouvelles pompes avec des écrans tactiles. Dans les 3 mois qui ont suivi leurs installations, ces pompes se sont fait voler : ainsi les pirates ont pu étudier à loisir les nouveaux dispositifs de sécurité sur ces pompes. C'est une **éternelle partie de cache-cache entre fraudeurs et policiers**.

CONCLUSIONS

Pierre PIAZZA conclut en attestant que, **pour sécuriser notre identité et nos transactions par CB, il faut mettre en place des dispositifs très importants**. Il faut, en permanence, **trouver un équilibre entre « sécurité » et « perte de liberté »**. La fraude ne doit pas être un prétexte pour empiéter sur nos libertés fondamentales. **Les politiques ont peur du débat sur ce sujet** et croient résoudre les problèmes de sécurité en **faisant appel uniquement à la technologie**.

David FOREST explique son impossibilité à conclure. Prenons seulement conscience que **nos données personnelles sont les matières premières de notre ère,** c'est le nouveau pétrole alimentant notre économie. Ayons-en bien conscience. Renseignons-nous sur nos droits, utilisons la CNIL. Des débats ont lieu à l'échelon communautaire, hélas, sans que l'on progresse réellement. **C'est une question politique majeure non abordée par nos politiques.**

Le Major Didier DOUILLY indique que **les données personnelles sont la bataille majeure qui arrive**. **Ne jetez pas pour autant vos CB ! Quant à internet, à chacune de nos utilisations, posons-nous la question de savoir si on ferait la même chose dans la vraie vie ?** On a l'impression qu'il n'y a plus de barrière lorsque nous utilisons internet. Ceci est un leurre. **Internet est le terrain de jeu des délinquants !**

Bibliographie

- **de David FOREST :** « Droit des données personnelles » et « Droit des marques et des noms de domaines » aux Editions GUALINO – iexterne
- **de Pierre PIAZZA :** « Histoire de la carte nationale d'identité – « L'identification biométrique » - « Aux origines de la police scientifique » aux Editions des Sciences de l'Homme.

Rédacteur : Jean-Pierre BULLIARD
Vice - Président de l'URIS de Franche-Comté
Vice - Président des Ingénieurs INSA de Franche-Comté
Pour le compte du Pavillon des Sciences

Programme des prochains « Bar des Sciences » :

- **Jeudi 25 avril 2013 :** l'**HYPERTENSION : un problème de santé publique** - 19h00 en duplex avec l'INSERM et Universcience à **Numerica** à Montbéliard
- **Mardi 30 avril 2013 :** les **NANOS dans la vie de tous les jours** - 20h00 au Bar de **l'Hôtel Bristol** à Montbéliard
- **Mardi 28 mai 2013 :** la **POUPEE ET LE CAMION : le cerveau a-t-il un sexe ?** - 20h00 au Bar de **l'Hôtel Bristol** à Montbéliard
- **Mardi 11 juin 2013 : VIN et PARFUM** - 20h00 au Bar de **l'Hôtel Bristol** à Montbéliard
- **Mardi 24 septembre 2013 : Ces sous-marins qui nous défendent ?** (avec l'Amiral Jean-Louis BARBIER) - 20h00 au **Centre de Conférences Saint Georges** à Montbéliard

Site Internet du Pavillon des Sciences : *www.pavillon-sciences.com*.

Parc Scientifique du Près-la-Rose – 25200 MONTBELIARD
Renseignements Bar des Sciences : Pascal REMOND – Tél 03 81 97 18 21 –
E-Mail : pascal@pavillon-sciences.com

2 Expositions en ce moment au Pavillon des Sciences :

- Au fil des Araignées - Du 18 mars au 17 novembre 2013 - À partir de 6 ans
- Vélosciences, le tour de la question* - Du 18 mars au 17 novembre 2013 - *À partir de 9 ans