Faits d'escroqueries, abus de confiance et tentatives sur le ressort de la Compagnie de Gendarmerie départementale de BEAUNE
- 2eme trimestre 2018 -

Madame B 52 ans Sainte Marie la Blanche

Manière d'opérer La victime se rend sur un site internet de petites annonces afin d'acheter une voiture. Une des annonces l'intéresse et elle donne rendez-vous à son vendeur. La rencontre se passe bien et les deux parties concluent la transaction.
Quelques temps après, la voiture achetée subit des pannes à répétition et doit être réparée en garage. Lors des réparations, un mécanicien affirme à la victime que le kilométrage affiché au compteur (78 902km) est faux. En réalité, le véhicule justifie d' un kilométrage supérieur à 210000km.

Madame M 71 ans Mimeure

Manière d'opérer La victime consulte une publicité concernant l'investissement de fonds dans la crypto-monnaie.
Quelques jours plus tard, elle est contactée téléphoniquement par une soit disant société dénommée GMT-crypto qui la convainc d'investir de l'argent dans cette monnaie fictive. Elle fournit alors son numéro de compte ainsi que son identifiant pour que la société puisse effectuer les virements. Au total, 2 virements de 3000 euros puis un autre de 9000 euros sont effectués.
La banque destinataire des virements est située en ESPAGNE.
Préjudice final de 15000 euros.

Madame B 94 ans Seurre

Manière d'opérer Les deux mis en cause se présentent au domicile de la victime et sollicitent un don. La victime, âgée et seule, fait rentrer les individus chez elle puis se rend dans sa chambre, ouvre son porte-monnaie et donne 5€ à l'un des deux individus. Pendant qu'un homme lui fait signer un faux récépissé de don, le second se rend dans la chambre de la victime et dérobe les 300 euros demeurant dans le porte monnaie de celle-ci. **Préjudice de 305 euros.**

Madame B 46 ans Comblanchien

Manière d'opérer La victime s'inscrit sur un site de rencontre. Rapidement elle fait la connaissance d'un profil lui plaisant. Après plusieurs échanges le profil lui demande la somme de 1000 € en deux envois au MAROC par « TRANSCAH ». Trouvant le profil sympathique et attachant, attirée, la victime envoie naïvement les 1000 € réclamés par cet homme.
Préjudice de 1000 euros

Madame G 31 ans Nuits saint Georges

Manière d'opérer Chercheuse d'emploi, la victime est démarchée sur internet pour faire des ménages suite à des travaux de plomberie prétendument effectués au sein d'un domicile privé. L'employeur, prétextant habiter en Corse, lui envoie par courrier un chèque de 1440 euros. 240 euros sont supposés servir à sa rémunération au titre de son travail de nettoyage et le restant censé financer l'intervention d'un prétendu plombier qui attend d'être payé. Elle dépose le chèque sur son compte bancaire et constate qu'il est effectivement provisionné d'un montant de 1440 euros.
Un prétendu plombier (le complice) la contacte par téléphone et lui demande de lui verser les 1200 euros qui lui sont dus sous forme de coupons « Transcash ». Elle s'exécute en transmettant les codes par sms, en toute confiance, le chèque ayant été crédité sur son compte.
5 jours après l'encaissement, après vérifications d'usage par la banque, le chèque est rejeté au motif "impayé" par sa banque , et son compte est bien sûr débité des 1440 euros initialement versés. **Préjudice final de 1200 euros**

Monsieur T 53 ans Corberon

Manière d'opérer L'auteur contacte téléphoniquement la victime afin de lui proposer une publicité dans un site de référencement. Devant l'insistance de l'interlocuteur, la victime signe un contrat et accepte l'offre. 03 chèques pour un montant total de 429 euros sont établis et encaissés par la société prestataire.

Monsieur A 57 ans Les Maillys

Manière d'opérer L'ex compagne de la victime souscrit plusieurs crédits à la consommation et désigne ce dernier co-emprunteur. Elle signe à sa place. A ce jour elle ne règle plus les organismes de crédits et de ce fait ces derniers se retournent contre la victime et lui demandent d'acquitter les sommes dues.

Madame B 47 ans Esbarres

Manière d'opérer La victime se sépare de son compagnon, elle quitte le domicile et s'installe dans un village voisin. Une officine de crédit, auprès de laquelle elle avait souscrit un emprunt, envoie à son ancien domicile une carte de paiement et le code permettant de l'utiliser. Son ex compagnon s'en sert et retire 900 euros.

Monsieur G 66 ans Seurre

Manière d'opérer La victime achète un scooter PEUGEOT, sur un site spécialisé, qu'elle règle par virement bancaire de 760,64 euros comme exigé par le vendeur.
Ce dernier demande ensuite un règlement de 394 euros pour les frais d'immatriculation alors que ceux-ci n'ont jamais été abordés lors de la vente afin de livrer le scooter. Après que la victime s'en soit acquittée afin d'obtenir son bien, le vendeur demande 126,21 euros pour une assurance d'un an, sans vouloir communiquer l'identité de la compagnie.
La victime réalise enfin qu'elle se fait escroquer. **Préjudice de 1281 euros.**

Madame H 43 ans Sainte Marie la Blanche

Manière d'opérer La victime reçoit des messages de sa mère via l'application Messenger de Facebook. Celle-ci lui demande d'appeler un numéro pour pouvoir débloquer son téléphone. La victime s'exécute et appelle 36 fois. Il s'avère que l'identité de sa mère est usurpée et que le numéro est surtaxé. **Préjudice de 95 euros.**

Madame R 56 ans Baubigny

Manière d'opérer La victime rencontre une personne sur internet et noue une relation épistolaire Celle dernière prétend à un moment être en grande difficulté à l'étranger (Égypte et Maroc). L'homme dont il est question demande ainsi à la victime de lui verser de l'argent en lui transférant les codes de coupons recharge PCS, NEOSURF et TONEOFIRST afin de régler ses difficultés (perte de document d'identité, problèmes médicaux).
La victime procède au versement de 14 recharges PCS, NEOSURF ou TONEOFIRST, pour un montant total de 3880 euros avant de parvenir à finalement comprendre qu'elle se fait escroquer. **Préjudice 3880 euros.**

Monsieur L 55 ans Foissy

Manière d'opérer Souhaitant acquérir de nouvelles machines pour son entreprise, la victime a répondu à une annonce sur le site internet "le bon coin". Après avoir pris attache avec le vendeur, ce dernier lui transmet son RIB afin qu'elle puisse lui verser directement la somme de 8400€. La victime étant également à la recherche d'une machine spécifique, le vendeur lui affirme en avoir une en sa possession et pouvoir la lui vendre pour 3240 €. À ce jour, la victime a réalisé des versements à hauteur de 11640€ à cet acheteur pour deux machines qu'elle n'a jamais reçues. **Préjudice 11640 euros**

Monsieur V 25 ans Nolay

Manière d'opérer La victime reçoit un appel sur son téléphone portable de son soit disant banquier. Cette personne lui demande la communication des codes qu'il vient de recevoir par message sur son téléphone portable. Dans un premier temps il communique ces numéros en toute confiance. Puis, une fois les codes communiqués, pris d'un doute, il contacte sa banque afin de se renseigner sur l'authenticité de l'appel. On lui confirme qu'il vient d'être victime d'une arnaque. De plus, la victime n'a bien sûr jamais rien commandé sur les sites western union France et C discount. Il a suffit à l'escroc de le contacter et de se faire passer pour un banquier pour recevoir communication des codes d'authentification dont il avait impérativement besoin pour valider les achats effectués à l'aide de la carte bleue de la victime dont il avait préalablement pris connaissance .

Madame S 74 ans Nuits saint Georges

Manière d'opérer Dans le cadre d'un démarchage commercial agressif réalisé par téléphone, une entreprise se faisant passer pour un organisme agrée propose à la victime : professionnel de la santé ayant un cabinet, la réalisation d'un diagnostic d'accessibilité de son local. La victime pensant que ce service est obligatoire. Elle effectue un paiement de 820 euros

Madame M 57 ans Meursanges

Manière d'opérer La victime reçoit un courrier de L'ADAP lui indiquant qu'elle a dépassé la date de dépôt concernant les déclarations relatives à l'accessibilité. La victime ayant un cabinet médical ne se méfie pas. Appelle le numéro indiqué, et effectue un paiement de 984€ en donnant ses numéros de carte à l'opératrice. Elle appelle la préfecture par la suite laquelle lui indique naturellement qu'il s'agit d'une escroquerie. **Préjudice de 948 euros.**

Madame R 75 ans Aubaine

Manière d'opérer La victime reçoit plusieurs documents par voie postal lui indiquant l'obligation d'effectuer des démarches sur l'accessibilité des personnes à mobilité réduite pour les établissement recevant du public (ADAP).
Ayant dépassé la date limite indiqué sur le document (07/05/2018), la victime appelle le numéro indiqué sur celui-ci. Son interlocutrice lui indique qu'elle doit s'acquitter de la somme de 720 euros. La victime donne les coordonnées de sa carte bancaire à l'interlocutrice.
Plusieurs minutes après avoir raccroché, la victime rappelle le même numéro et indique à son interlocuteur son souhait d'annuler le paiement de 720 euros. L'interlocuteur lui indique qu'ils vont procéder à son remboursement.
La victime rappelle le numéro plusieurs jours après et son interlocuteur lui indique qu'elle doit patienter trois quatre jours avant d'avoir son remboursement.
Trois jours plus tard la victime rappelle le même numéro et demande directement à parler à la comptable. Son interlocutrice (la comptable) lui envoie un mail en lui indiquant que la victime doit demander comment elle souhaite être remboursé par chèque ou virement bancaire à condition de fournir les coordonnées bancaire.
À ce jour la victime n'ayant bien sûr toujours pas été remboursé se présente dans nos locaux pour déposer plainte. **Préjudice de 720 euros**

Monsieur F 35 ans La Perriere sur Saône

Manière d'opérer Les mis en cause rencontrent la victime pour acheter un chien de race suite à une annonce sur le site internet « Le bon coin ». Les MEC ont choisi le chien puis se sont mis d' accord sur le mode de paiement . L'accord stipulait que deux versements de 300 euros auraient du être fait en juin et juillet. A ce jour, bien sûr, rien n'a été versé.

Madame R 70 ans Nuits Saint Georges

Manière d'opérer La victime constate que son ordinateur est bloqué et qu'il lui faut cliquer sur un lien pour l'assistance. L'opératrice sollicitera les numéros de carte bleue du couple victime afin de lui vendre des opérations de maintenant pour 620 €. Enclins au doute, les victimes feront opposition à leurs CB. Aucun retrait ne sera constaté. Leur vigilance leur a permis d'échapper à l'escroquerie.

Madame C 60 ans Aloxe Corton

Manière d'opérer La victime se fait démarcher par mail par un certain "Stéphane LAFON" qui se dit commercial pour le compte de la société "PASSYDIS". Le 09 mai 2018, l'intéressé passe une commande de vin qui s'élève à 18 948 euros TTC. Le 29 mai 2018 la commande est prise en charge par le transporteur "LOGIVIN" mandaté par la victime. Le 04 juin 2018, la victime reçoit un mail de la part du transporteur l'informant que la commande n'a pas été livrée pour motif "Problème adresse". En effectuant des recherches sur internet la victime se rend compte que la société où devait être livré le vin n'existe pas et annule la livraison.
Il s'avère que la société PASSYDIS (Super U) basée à PASSY (74) fait actuellement l'objet d'une usurpation d'identité, une plainte a été déposée. Les auteurs sollicitent les vignerons sous le nom de "Stéphane LAFON" et passent des commandes de vins qu'ils font livrer à différentes adresses en FRANCE. Or, la société n'est pas à l'origine de ce démarchage. Les documents fournis par les auteurs mentionnent les références de la société usurpée (SIREN, adresse, dirigeant, extrait KBIS….) . L'escroquerie par chance et vigilance en est restée à l'état de tentative.

Madame B 50 ans Argilly

Manière d'opérer La victime met un vente sur le site « le bon coin » un contrôleur de son pour la somme de 100 euros. Une personne (l'escroc) prend contact avec elle et lui demande d'acheter un coupon recharge « Transcash » d'un montant de 100€ et de lui en faire parvenir le code car elle réside prétendument en SUISSE.
Elle lui affirme qu'après cela son compte serait crédité de 270 euros et qu'elle n'aurait plus qu'à expédier le matériel.
La victime s'exécute, et ne reçoit bien sûr jamais la somme de 270€ sur son compte. Préjudice de 100 euros.

Il est essentiel de connaître et de faire connaître les modes opératoires suivants inhérents aux escroqueries et abus de confiance :

- Une carte PCS est un outil de paiement, qui se présente comme une carte bancaire et qui possède d'ailleurs beaucoup de points communs avec une carte bleue telle que votre banque traditionnelle peut vous délivrer. Avec une carte PCS, il est à la fois possible de payer n'importe quel commerçant qui accepte les cartes bancaires et retirer de l'argent dans n'importe quel distributeur affilié au réseau Mastercard, c'est à dire quasiment tous les distributeurs d'argent.

La principale différence entre une carte bleue venant de votre banque et une carte PCS est que cette dernière n'est reliée à aucun compte en banque et est donc totalement anonyme. Il est possible de l'acheter dans beaucoup de bureaux de tabac en France sans avoir à fournir la moindre identité.

Les cartes PCS se créditent par des coupons recharges PCS, elles aussi disponibles dans les bureaux de tabac. A la manière d'une carte cadeau ou d'une recharge téléphonique, un coupon recharge PCS est une carte créditée d'un certain montant (20€, 50€, 100€, 150€, 250€). Une carte PCS se recharge en entrant le code du coupon recharge. Lors des correspondances avec leurs victimes, les escrocs demandent à leurs cibles d'acheter des coupons recharges et de leur envoyer les codes. De cette façon, les escrocs créditent leur propre carte PCS avec l'argent de leurs victimes. Cette opération étant anonyme et irréversible, il est impossible pour les victimes de se faire rembourser ou de retrouver les escrocs en question.

- il importe ainsi de retenir que dés que l'on vous demandera de communiquer des coupons recharges PCS, NEOSURF, TONEO FIRST TRANSCASH ….ou de procéder à un ou plusieurs virements WESTERN UNION à l'issue d'une correspondance sentimentale, sur des sites de rencontres ou réseaux sociaux ou quelles qu'en soient les circonstances (vente d'un objet...) et les motivations ….C'est que vous êtes en train de vous faire escroquer.

- Dés que l'on vous demande d'ouvrir un compte Paypal pour faciliter une transaction quelle qu'elle soit c'est que vous êtes en train de vous faire escroquer.

- Dés que l'on vous demande d'encaisser un chèque en récompense d'un service, d'une transaction, de l'obtention d'un emploi ... Et que l'on vous demander d'adresser une contrepartie d'un montant moins élevé (afin de vous y inciter) en coupons recharges PCS, NEOSURF ou TRANS CASH ...C'est que vous êtes en train de vous faire escroquer.
En effet le montant crédité sur votre compte par votre banque lors de l'encaissement du dit chèque sera débité dés le lendemain lorsqu'elle aura procédé aux vérifications d'usage : « chèque volé ou déclaré perdu » !
Concrètement l'escroc dispose de 24 heures une fois que le chèque vous a été adressé et qu'il est encaissé pour réussir à vous convaincre par tous moyens (appels, textos) de lui adresser une somme à peu près correspondante en coupons recharges qui lui permettront avec les codes communiqués de recharger sa propre carte de crédit.

- Si une prétendue administration ou entreprise financière privée : Services fiscaux, impôts, banque etc. vous demande une communication de vos coordonnées bancaires , carte bleue et /ou codes quel que soit le motif avancé . C'est que vous êtes en train de vous faire escroquer.
La logique est la même pour les achats sécurisés par envoi d'un code sécurisé par texto sur votre téléphone portable. Si un interlocuteur vous demande de le lui communiquer c'est qu'il a réalisé un achat frauduleux avec les coordonnées carte bleue et code de sécurité (au verso de la carte) que vous lui avez communiqué ou que vous vous êtes fait subtiliser à votre insu , et qu'il a besoin de valider la transaction au moyen du code texto que vous avez reçu sur votre téléphone portable.

- Si lors de la consultation d'un site internet il vous est demandé 1 euro pour l'acquisition d'un objet ou le bénéfice d'un service avec communication de vos coordonnées bancaires / carte bleue lors du paiement il est plus que probable que vous vous fassiez escroquer.

- Si vous êtes contacté par un opérateur téléphonique lequel vous fait savoir que vous avez été tiré au sort et avez gagné un lot d'objets, des bons d'achats ou qu'il vous faut

choisir vos cadeaux à partir du site en ligne d'une chaîne de distribution c'est que vous vous faites escroquer. Dans la logique de l'escroquerie il vous communique un numéro de téléphone à rappeler , ce numéro est surtaxé et il cherche à vous y faire passer le temps le plus long possible afin d'en tirer bénéfice . Les préjudices peuvent être de plusieurs centaines d'euros en fonction de la durée de la communication.

- Dans le cadre particulier de la falsification de chèques , ne pas utiliser d'encre effaçable mais une encre indélébile et surtout ne laisser aucun espace sur le libellé du chèque susceptible de permettre au délinquant de rajouter un «cent» ou un «mille», voir bien plus ....

- Si en qualité de professionnel, et quel que soit le secteur d'activité exercé , vous êtes démarché par téléphone par une prétendue administration ,pour de prétendues obligations légales **en matière d'aménagement des locaux professionnels pour l'accessibilité des personnes handicapées** , pour un aménagement de normes ou des obligations diverses etc. et que l'on évoque un paiement impératif et rapide sous réserve de se voir infliger des amendes importantes …. C'est que vous êtes en train de vous faire escroquer.

- Si vous vendez votre véhicule , vous ne pouvez pas savoir ce qu'il en sera de l'attitude de votre acquéreur après la transaction. Rien ne vous garantit notamment qu'il respectera les obligations légales relatives à la mutation de la carte grise auprès des services de la préfecture après achat. Concrètement , il se pourrait donc que vous receviez des procès verbaux relatifs à des infractions à la police de la route commis par votre acquéreur puisque votre identité et votre adresse figureront toujours sur la dite carte grise en cas de non mutation.
En substance, adressez toujours le certificat de cession de votre véhicule à la préfecture. Conservez toujours une photocopie de ce certificat de cession , ainsi que celle de la carte grise barrée et annotée « vendue le *** à *** » en cas de réception indue d'un procès verbal et afin de prouver votre bonne foi lors de l'établissement de la requête en exonération.

- Si vous faites l'achat d'un véhicule d'occasion par l'intermédiaire d' un site de vente en ligne, quel qu'il soit, il est impératif que vous soyez certain du kilométrage affiché par le compteur du véhicule. Que l'achat soit réalisé auprès d'un garage ou auprès d'un particulier il convient d'exiger que soit fourni l'ensemble des factures d'entretien relatives au véhicule concerné. Elles seules vous permettent d'avoir des certitudes sue le kilométrage effectif du véhicule et de vous prémunir d'une falsification de ce compteur.

- Après avoir effectué un retrait dans un DAB (distributeur automatique de banque) , ne pas oublier de repartir avec la carte , sinon celui qui suit immédiatement et avant que la carte ne soit avalée n'aura plus qu'à se servir sur votre compte .

Capitaine Hervé MOREAU
Commandant en second la compagnie de gendarmerie de Beaune