

Faits d'escroqueries, abus de confiance et tentatives sur le ressort de la compagnie de gendarmerie départementale de BEAUNE - 4eme trimestre 2017 -

Monsieur F 63 ans CORGOLOIN

Manière d'opérer La victime reçoit un mail lui demandant de confirmer des informations en vue d'un remboursement des impôts. Elle envoie différentes informations relatives à sa carte bancaire. Le lendemain, une personne se faisant passer pour sa banque lui demande de lui communiquer des codes de confirmation reçus par SMS. sur son téléphone portable (suite à un achat frauduleux). La victime s'exécute. 806 euros sont prélevés sur son compte.

Monsieur G 23 ans JOUEY

Manière d'opérer Le ou les auteurs contactent la victime par le biais du site internet "le bon coin" pour l'annonce mise en ligne relative à la vente d'un téléphone portable de marque APPLE type Iphone 7 . La victime et l'auteur conviennent que la transaction se fera à la réception d'un chèque par le vendeur.. Lors de la réception de ce chèque la victime envoie le colis contenant le téléphone sans RESPECTER LE DÉLAI DE 24 À 48 HEURES et s'assurer ainsi de la validité du chèque. La banque de la victime n'accepte pas le paiement car ce dernier est déclaré volé.

Monsieur B 50 ans SEURRE

Manière d'opérer L'auteur vend un véhicule à la victime avec 161600kms au compteur. Quelques temps plus tard, alors que la victime apporte son véhicule affichant 171800kms au garage pour un entretien, le garagiste lui fait savoir que celui-ci totalise plus de 300000kms.

Madame C 30ans POUILLY SUR SAONE

Manière d'opérer La victime effectue un virement sur internet pour visionner des films en streaming. On lui demande de payer 01 euros. Elle se voit débiter deux fois de 49.95 euros début novembre et début décembre par le site 247MUZIC.COM.

Madame D 33 ans Le CHATELET

Manière d'opérer La victime est contacté par un individu se présentant comme un technicien de la plateforme de sécurité de sa banque.. Celui l'informe que des mouvements bancaires vont être effectués depuis la Roumanie et l'Espagne. Celui-ci lui demande donc de lui donner les codes permettant d'effectuer les virements afin de bloquer ces mouvements. La victime les lui fournit et plusieurs sommes sont bien sûr retirées de son compte par l'escroc pour un **PRÉJUDICE DE 5400 euros**

Madame B 25 ans ARNAY LE DUC

Manière d'opérer La victime met en vente sur le site LEBONCOIN, un coffret DVD pour une valeur de 100€. Une personne intéressée par la présente offre, entre en contact avec la victime. Il l'incite à utiliser PAYPAL pour le règlement. La victime reçoit un mail d'un site "écran", logoté PAYPAL Premium. Le mail l'oblige à un premier versement de 600€ pour "activer" son compte. Une fois fait, le lendemain, le même site l'informe d'un trop perçu de 1200€ en sa faveur. Ils la mettent en demeure de rembourser la somme. Le compte est dès lors bloqué jusqu'à règlement complet. Entre temps, l'acheteur exerce une pression sur la victime via des SMS répétés et l'incite à régulariser sa situation avec le site PAYPAL Premium. De plus, il lui envoie un chèque d'un montant de 2500€ en guise de règlement du coffret et pour couvrir le montant des frais PAYPAL ; le restant de la somme devant lui être retourné via des coupons PCS. La victime envoie pour 1050€ de coupon TONEO FIRST pour règlement de sa dette PAYPAL, en supplément des 600€ versés en amont ; et pour 600€ de coupon PCS au supposé acheteur. Le chèque reçu par la victime, est quant à lui, une fois encaissé, déclaré sans provision. **Le préjudice final est de 2500 euros**

Monsieur F 39 ans SAINTE SABINE

Manière d'opérer La victime se fait contacter par une inconnue qui, au fil de la conversation, lui évoque une dette de 1800 euros. Elle lui demande 8500 euros en mandat cash. La victime lui envoie 300 euros. Par la suite, cette inconnue lui envoie un chèque de 8573 euros émanant soit disant du « trésor public » qu'il doit encaisser en contrepartie de quoi il devra faire un virement de 7000 euros, gardant ainsi 1573 euros pour lui. Il effectue 3 virements de 2000 euros chacun via un RIB que la mise en cause lui a envoyé puis un virement de 750 euros via un 2ème RIB différent du 1er. La banque de la victime l'informe que le chèque est un faux chèque. La victime stoppe alors les virements. Ensuite, puisque ça marche, l'escroc auteur des faits demande à la victime de procéder de la même manière pour un autre chèque d'un montant de 18000 euros qu'elle lui enverra ultérieurement. L'escroquerie cesse là. **PRÉJUDICE DE 7500 EUROS**

Monsieur V 33 ans EPINAC

Manière d'opérer La victime s'aperçoit après avoir acheté un véhicule que celui ci possède un vice caché important. Le vendeur ne pouvait ignorer et a omis volontairement de le lui préciser.. De plus, le vendeur est arrivé à lui céder ce véhicule alors que celui ci n'est pas titulaire du certificat d'immatriculation à son nom.

Madame P 23 ans L'ETANG VERGY

Manière d'opérer La victime met en vente son ordinateur sur le site "LE BON COIN". Un homme se manifeste et se dit intéressé, il propose de payer via PAYPAL, ce que la victime accepte. La victime envoie l'ordinateur par colissimo. Suite à cela, elle reçoit un mail de PAYPAL, l'informant qu'elle doit payer 450 euros pour créer un compte premium afin de pouvoir récupérer les 200 euros correspondant à la vente de l'ordinateur. La victime refuse de payer les 450 euros et comprend qu'elle s'est faite escroquer.

Monsieur T 45 ans SAINT SYMPHORIEN SUR SAONE

Manière d'opérer La victime s'inscrit sur un site de rencontre. Elle est contactée par une personne et commence à échanger avec elle. Au bout de quelques jours, la personne lui déclare qu'elle va lui envoyer un chèque d'un montant de 2 200 euros, qu'il faut qu'elle l'encaisse et qu'elle lui fasse un virement de ce même montant. Quelques jours plus tard, la banque appelle la victime pour l'informer que le chèque encaissé est volé. Préjudice de 2200 euros.
Mis en cause localisé en côte d'Ivoire

Monsieur J 43 ans CHAMPIGNOLLES

Manière d'opérer La victime reçoit un mail frauduleux de sa banque le crédit agricole. Elle a ouvert ce mail mais n'a pas répondu. Plus tard elle reçoit un SMS lui demandant des codes de sécurité pour un achat via sa carte bancaire, la victime se rend dans son agence bancaire et signale les faits à son conseiller, lequel bloque sa carte bancaire.
Sur son relevé bancaire elle aperçoit que deux retraits frauduleux ont été effectués sur son compte bancaire. Pour un préjudice de 200 euros.

Madame J 57 ans VIEVY

Manière d'opérer La victime reçoit un coup de téléphone d'une femme, laquelle lui indique que sa carte bancaire a été piratée. L'interlocutrice lui demande bien sûr de lui communiquer les numéros de sa carte bancaire. La victime ne se méfie pas, ne voit pas venir l'escroquerie et les lui communique. Le soir des faits la victime se rend compte que ce n'est pas normal et appelle sa banque pour faire opposition à sa carte bancaire.
Sur son relevé bancaire elle s'aperçoit qu'un retrait frauduleux de 210 euros a été effectué sur son compte bancaire.

Monsieur F 31 ans BLIGNY LES BEAUNE

Manière d'opérer Le mis en cause communique par mail avec un interlocuteur qui lui explique qu'un chèque de 1800€ va lui être envoyé. Il doit établir à l'encaissement de ce chèque trois mandats cash pour un montant de 900€ au total et conserver la somme de 900€ pour le service rendu. Ce dernier septique à la réception du chèque contacte la banque qui l'informe que ce dernier est volé. Malgré tout il décide de déposer le chèque sur son compte bancaire et de retirer la somme de 900€ dans la foulée. Il effectue le même jour 3 mandats cash (2x365€ et 1x213€ = 943€). Le lendemain il constate que le chèque n'a bien sûr pas été crédité sur son compte bancaire et qu'il est à découvert de plus de 900€. Il se présente à notre unité pour déposer plainte pour escroquerie. Nonobstant le préjudice dont il a été victime, il est convoqué devant le délégué du procureur de la République (convocation judiciaire) en vue d'un rappel à la loi pour recel de bien provenant d'un usage de chèque falsifié ou contrefait.

Monsieur I 32 ans MEILLY SUR ROUVRES

Manière d'opérer La victime achète un aspirateur sur un site internet. Elle règle le montant par carte bancaire. Quelques jours plus tard, elle n'a toujours pas reçu son achat et le site marchand a disparu.

Mademoiselle O 19 ans NUIITS SAINT GEORGES

Manière d'opérer La victime répond à une annonce de travail consistant à gérer le patrimoine immobilier d'une personne. L'auteur de l'annonce l'informe qu'elle va recevoir un chèque de 1000 euros correspondant à un loyer d'un de ses locataires. Il lui demande de l'encaisser, de lui retourner 750 euros et de garder 250 euros correspondant à son salaire hebdomadaire. Elle encaisse le chèque sur son compte bancaire et lui retourne 750 euros par virement bancaire au moyen d'un RIB communiqué par cet individu. Elle est informée par la suite par sa banque que le chèque qu'elle a encaissé était bien sûr volé. La somme initialement créditée sur son compte est bien sûr ensuite débitée par voie de conséquence. Le préjudice est de 750 euros.

Monsieur R 61 ans CORPEAU

Manière d'opérer La victime souhaite investir ses fonds propres afin de les rentabiliser au mieux. Elle cherche sur internet une solution pour maximiser la rentabilité. Elle jette son dévolu sur une annonce google concernant la société "CAPITAL DIAMOND". Elle prend attache téléphoniquement avec cette société. Son interlocutrice propose à la victime d'investir de l'argent dans des pierres précieuses en lui vantant une forte rentabilité. La victime se laisse convaincre et achète des diamants (3) pour une somme totale de 24720 €. De faux titres de propriété lui ont été communiqués par voie postale. La victime n'a jamais été en possession des pierres. Les contacts courriels et téléphoniques restent sans réponse depuis.

Monsieur G 32 ans LABERGEMENT LES SEURRE

Manière d'opérer La victime à la recherche d'un emploi est contacté par mail par un potentiel employeur qui souhaite l'embaucher comme chauffeur. Il doit encaisser un chèque de 1900 euros sur son compte puis retourner 1300 euros sous forme de coupons trans cash. La victime encaisse le chèque le 31/10/2017 puis se rend dans un bureau de tabac où le buraliste le met en garde. Il fait patienter l'employeur et reçoit ensuite un rejet du chèque par sa banque pour perte. L'escroquerie a été évitée de justesse par la présence d'esprit du buraliste.

Mademoiselle B 19 ans BRAZEY EN PLAINE

Manière d'opérer Le ou les auteurs créent une annonce pour une vente de voiture sur un groupe de vente appelé "CC" sur le réseau social « Facebook », la victime prend contact avec ces derniers par SMS, mais ils l'informent qu'elle doit effectuer un transfert avec Western Union avant d'avoir vu la voiture. La victime, crédule et mise en confiance, exécute les instructions. Le préjudice s'élève à 1300 euros.

Monsieur P 56 ans MEILLY SUR ROUVRES

Manière d'opérer La victime contacte par téléphone un particulier proposant la vente d'une voiture d'occasion via le site "le bon coin". Ils conviennent d'un rendez-vous sur un parking à Dijon. Après l'avoir essayée et s'être mis d'accord sur le prix la victime règle la transaction en numéraire. Le vendeur lui remet alors une déclaration de cession d'un véhicule préalablement remplie. Constatant que l'identité sur la carte grise barrée et sur la déclaration de cession correspond à une personne résidant dans la Loire, la victime lui demande alors des explications. Celui-ci le rassure en lui disant qu'il l'a bien achetée à cette personne et qu'il n'y a aucun problème car de son côté il n'a envoyé aucun document à la Préfecture pour l'immatriculer à son nom. La victime se rend alors dans un garage pour procéder à l'immatriculation. On lui explique alors que c'est impossible car le véhicule est déjà en cession au nom d'une tierce personne.

Monsieur M 30 ans ARCENANT

Manière d'opérer La victime acquiert un véhicule d'occasion pour un montant de 5000 € suite à une annonce trouvée sur le site « le bon coin ». Le véhicule affiche un kilométrage de 168000 kms. Après expertise du véhicule par un concessionnaire Mercedes, le véhicule possède en réalité 306.000 kms.

Madame R 70 ans MOLINOT

Manière d'opérer La victime met en vente sur le site « le bon coin » une scie à ruban à 500 euros. L'auteur demande à la victime de lui envoyer par coupon PCS 150 euros pour s'acquitter d'une "taxe de libre circulation des flux financiers" avant de procéder à la vente. Elle suit les instructions. Préjudice de 150 euros ;

Monsieur B 65 ans MIMEURE

Manière d'opérer TENTATIVE D'ESCROQUERIE . La victime reçoit un mail d'une très bonne amie à lui l'incitant à acheter des coupons NEOSURF suite à la perte de ses documents d'identité, moyens de paiement et téléphone lors d'un déplacement à MENTON. Ce dernier se rend au buraliste de la commune, et achète 5 coupons pour un montant total de 500€. Après les avoir scannés, il cherche à les envoyer par mail mais sans succès. En effet, son amie a pu bloquer son adresse mail, après s'être rendue compte qu'elle avait été piratée.

Monsieur V 44 ans LANTHES

Manière d'opérer TENTATIVE D'ESCROQUERIE . La victime à la recherche d'un emploi reçoit un courriel pour un poste de chauffeur. Après plusieurs échanges de mails le potentiel employeur lui adresse un chèque de 1850 euros à encaisser sur son compte bancaire et il doit retourner la somme de 1350 euros via mandat à la poste pour des frais divers. Il photographie le chèque l'encaisse sur son compte et se présente en gendarmerie. La victime est mise en garde et ne procède à l'envoi d'aucune somme d'argent . Il reçoit ensuite l'opposition du chèque par sa banque.

Monsieur B 43 ans MEURSAULT

Manière d'opérer L'auteur des faits a travaillé comme vendangeur pour une courte période avant de rompre son contrat. Son employeur lui remet un chèque de 212.43 euros correspondant au travail effectif réalisé. L'employeur constate en effectuant la comptabilité de l'entreprise quelques jours plus tard que le chèque débité n'est plus de 212.43 euros mais de 1212.43 euros. EN EFFET UN ESPACE A ÉTÉ LAISSÉ PERMETTANT D' INSERRER LE MILLE et donc la falsification.

Madame F 66 ans SAINT JEAN DE LOSNE

Manière d'opérer Le mis en cause prend contact avec la victime et se fait passer pour un opérateur de chez Bouygues Télécoms. il parvient à obtenir le numéro de carte bleue de la victime ainsi que le cryptogramme de sécurité présent au verso de la carte. Il fait un achat en direct et parvient également à obtenir le code de validation sécurisé que la victime a reçu sur son téléphone portable lui permettant de finaliser la transaction d'achat. Il effectue un achat de 899 euros sur le site C-Discount. **Préjudice de 899 euros pour la victime.**

Monsieur L 27 ans NUIITS SAINT GEORGES

Manière d'opérer La victime sympathise avec une femme sur un site de rencontre, sur internet. Ils se contactent par Skype ou textos. Cette femme est prétendument décoratrice canadienne vivant en FRANCE. Il ne l'a jamais rencontrée. Au bout d'un mois d'échanges, la femme lui explique qu'elle doit partir en Afrique, où son père est mort il y a 3 ans, pour régler la succession. En effet, son père aurait été tué par balle en Afrique dans le cadre de son travail et après 3 ans d'attente, la succession est en passe d'être réglée. Malheureusement et bien sûr, la femme ne peut pas acquitter les frais de succession qui s'élèvent à 10 000 euros. Elle a déjà du payer son billet d'avion, son hôtel et des frais d'hospitalisation, car elle est tombée malade en Afrique. La victime tout à son sentiment amoureux s'en apitoie et paie les 10 000 euros demandés sous forme de cartes de paiement prépayés, en divers versements, s'échelonnant sur une durée de 8 mois. De plus, la femme lui demande de recevoir des colis de vêtements qu'il doit revendre et de lui faire parvenir l'argent récolté, toujours sous forme de cartes de paiement prépayé. Ceci afin d'accélérer la procédure de succession. La victime s'exécute. Enfin et puisque ça marche un chèque de 4800 euros est aussi envoyé à la victime qui doit l'encaisser et renvoyer la somme à son amie en cartes de paiement prépayé. Lors de chaque questionnement de la part de la victime, son amie réussit à lui fournir des explications convaincantes à ses yeux. La victime commence à douter. Il s'aperçoit enfin de la supercherie et donc de l'escroquerie lorsqu'il découvre que la photographie que son amie lui a envoyée ne correspond pas au nom qu'elle lui a donné. Préjudice de plus de dix mille euros

Monsieur P 65 ans COB ARNAY

Manière d'opérer La victime, psychologue est démarchée par courrier et par téléphone par une entreprise spécialisée dans le domaine de la réglementation pour les droits aux personnes à mobilité réduite. La victime reçoit un coup de téléphone de cette entreprise. L'interlocuteur argumente en mettant en avant des notions d'obligations légales, de menaces d'amendes importantes ; si elle ne règle pas dans les 48 heures, la somme de 467€. Sous la crainte de se voir impacter financièrement de façon plus importante, la victime fournit le numéro de sa carte bancaire. L'interlocuteur verrouille l'opération, avec la confirmation du règlement via un code renvoyé par SMS sur le téléphone portable de la victime. Les 467€ correspondraient à des timbres fiscaux selon les dires du mis en cause. De plus, il l'informe qu'elle recevra un courrier par accusé de réception dans les jours prochains à aller récupérer. **Préjudice de 467 euros.**

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

- il importe ainsi de retenir que dès que l'on vous demandera de communiquer des coupons recharges PCS, NEOSURF, TONEO FIRST TRASCASHou 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 motivationsC'est que vous êtes en train de vous faire escroquer.

- Dès 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.

- Dès 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 demande 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 dès 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.