

Continue



























Des déclarations volubiles se présentent sous divers prétextes, parfois avec de fausses identités (certains ont même prétendu appeler au nom de 60 Millions ), et ont l'article, de complémentaires santé ou de contrats de prévoyance (hospitalisation, garanties des accidents de la vie, dépendance...), A LIRE AUSSI >>>

Des démarcheurs téléphoniques peu scrupuleux parviennent à vendre des mutuelles à l'insu des personnes démarchées. Nos conseils. Au volant et donc concentré sur la route, William ne se méfie pas quand il reçoit sur son portable l'appel « « une filiale de son assurance » qui lui propose une garantie en cas d'hospitalisation. « Avec le kit mains libres, j'entendais très mal, raconte-t-il. Pour en finir au plus vite, et croyant que je pourrais étudier leur proposition plus tard, j'ai communiqué ce qu'ils m'ont présenté comme un "code promotionnel" figurant dans un SMS envoyé durant la conversation. » De retour à la maison, c'est la surprise : il découvre une salve de textos estampillés Eca-Assurances lui confirmant son adhésion à un contrat dont il ne connaît ni la portée, ni le coût ! Des démarcheurs volubiles et menteurs Michel, lui, n'a pas tiqué lors de l'appel d'un soi-disant agent de la Sécurité sociale lui demandant le « code de sécurité » envoyé par SMS, afin qu'il puisse accéder à son dossier et vérifier ses informations personnelles. « Deux jours plus tard, j'ai reçu un contrat d'un courtier, Néoliane, que j'ai précedemment signé électroniquement pour un montant de 18,61 € par mois ! De nombreux témoignages de ce type parviennent régulièrement à la rédaction de 60 Millions de consommateurs. Ils ont décrits les mêmes manières de procéder : des démarcheurs volubiles se présentent sous divers prétextes, parfois avec de fausses identités (certains ont même prétendu appeler au nom de 60 Millions ), et ont l'article, de complémentaires santé ou de contrats de prévoyance (hospitalisation, garanties des accidents de la vie, dépendance...), A LIRE AUSSI >>> Quatre sociétés sanctionnées pour non-respect de Bloctel Vous n'en avez pas besoin ? Peu importe ! Ils usent de tous les stratagèmes pour obtenir vos données personnelles (nom, adresse, relevé d'identité bancaire...), puis, à la fin, pour vous arracher un accord d'adhésion à un contrat... à votre insu ! Vous voilà bénéficiaire d'un contrat non souhaité suite à un démarchage téléphonique ? Vous avez quatorze jours, à compter de la réception des documents contractuels, pour faire jouer votre droit de rétractation. Pour cela, envoyez une lettre recommandée avec avis de réception, à l'assureur et au courtier (rappelez-leur, au passage, que vous n'avez jamais consenti au contrat). Si votre demande de rétractation reste lettre morte, adressez un nouveau courrier de réclamation à l'assureur puis, en dernier ressort, saisissez le médiateur (de l'assurance ou de la mutualité, selon le contrat). Si le délai de rétractation n'est mentionné nulle part dans les documents reçus, celui-ci est prolongé de douze mois (article L. 221-20 du code de la consommation). Devant la « persistance des plaintes » reçues par ses services, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) a contrôlé 92 entreprises l'an dernier, et en a épinglé 27. Elle confirme que « certains démarcheurs recourent à des allégations mensongères pour recueillir l'accord verbal du consommateur ou obtenir la signature électronique du contrat ». C'est une spécificité dans les assurances : un contrat peut être souscrit en quelques minutes par téléphone après la simple expression de votre consentement. Une solution très pratique quand il s'agit de protéger votre nouvelle voiture en passant un simple coup de fil à votre assureur, mais qui s'avère péjorative dans le cadre d'un démarchage téléphonique abusif. A LIRE AUSSI >>> Mutuelles : comment bien souscrire ou résilier Un simple SMS vaut signature ? Beaucoup de gens l'ignorent mais, pour être approuvé, un contrat ne doit pas être exclusivement signé de manière manuscrite, explique Olivier Gayraud, juriste à l'association de consommateurs CLCV. On peut se retrouver engagé après une signature électronique qui peut revêtir plusieurs formes : un code par SMS envoyé par le courtier et qui l'a fait répéter à voix haute, une touche de téléphone sur laquelle appuyer ou, sur Internet, une succession de liens à cliquer. » Parmi ces méthodes, la signature par SMS a la faveur des courtiers en assurances dont les agissements posent problème. La plupart l'obtiennent par ruse. Mais « il semble aussi que, dans certains cas, le vendeur signe électroniquement le contrat pour le compte du client en lieu et place de ce dernier, contournant ainsi les dispositifs de signature électronique », constate l'Autorité de contrôle prudentiel et de résolution (ACPR). le gendarme du secteur, dans un document daté de juin dernier. Utilisation illégale de fichiers Une pratique que nous confirme Ghislaine, en situation de handicap et « pas au mieux de sa forme » quand elle se fait démarcher au prétexte que la Sécurité sociale aurait détecté une erreur dans son dossier. « Après un message préenregistré alarmiste, j'ai appuyé sur une touche du téléphone pour être mise en relation avec une personne. Quand j'ai compris qu'il ne s'agissait en fait que d'un vendeur, j'ai répété que je n'étais pas intéressée. » Pourtant, elle réagit aujourd'hui deux contrats, prélevés sur son compte malgré son refus de communiquer ses données bancaires ! Où le courtier a-t-il bien pu se les procurer ? L'enquête menée par l'ACPR sur SGP, une filiale du courtier Fillassur, est éclairante sur ce point. La SGP utilise en effet des fichiers clients provenant d'entreprises de téléachat ou de vente par correspondance contenant ces données sensibles. 1. Identifiez votre interlocuteur Un démarcheur sérieux doit se présenter sans ambiguïté ! Il doit citer le nom de son assurance d'attache ou, si c'est un courtier, décliner son numéro d'enregistrement à l'Orias, le registre des intermédiaires en assurance. Si le démarcheur appelle « de la part » de votre assurance, mutuelle, banque... méfiance. Posez-lui des questions pour comprendre à qui vous avez affaire. S'il se revendique d'organismes publics (comme la Sécurité sociale, votre caisse de retraite...), mettez un terme à la conversation, car jamais ils ne procèdent de la sorte. 2. Ne décidez pas tout de suite Ne cédez jamais à la pression des démarcheurs. Ils jouent souvent avec vos émotions (peur, promesse de promotion ou de cadeau...) pour obtenir rapidement vos informations personnelles. Dans tous les cas, ne communiquez jamais vos données bancaires, ne cédez pas à la demande de répétition d'une phrase ou à la communication d'un code reçu par SMS qui vaudrait pour signature du contrat. Insistez plutôt pour recevoir une documentation afin de l'étudier à tête reposée. 3. Prévenez les autorités Si vous êtes la cible d'un démarcheur mal intentionné, vous pouvez signaler ses pratiques commerciales trompeuses : pour cela, écrivez à votre direction départementale en charge de la protection des populations (DDPP ou DDCSP) et à l'ACPR. Contrats vendus en 444 € Ces professionnels n'ont décidément pas froid aux yeux. Ils négligent aussi le devoir d'information et de conseil auquel ils sont pourtant soumis. Après son enquête en février 2018, l'ACPR a infligé à SGP un blâme et une sanction de 150 000 € pour l'insuffisance et l'inexactitude des informations et certains dispensés. En témoigne le temps moyen record qu'il fallait à ses « conseillers » pour vendre un contrat : 4 minutes et 44 secondes ! A LIRE AUSSI >>> Spams, démarchage téléphonique, prospectus : dites stop à la pub ! Derrière ces appels, les noms de certaines entreprises reviennent souvent dans les témoignages que nous recevons : Eca-Assurances, SPVIE, et surtout Néoliane. Leur point commun : ce sont des courtiers grossistes qui convoient des contrats avec des assureurs et s'appuient sur des courtiers indépendants pour les commercialiser. Ce qui interroge sur la surveillance des seconds par les premiers. « Le risque zéro n'existe pas », reconnaît Clément Janicot, directeur marketing du groupe Santiane, la maison mère de Néoliane. Mais il assure toutefois des outils s'appuyant notamment sur le taux de rétractation ou d'annulation des contrats pour détecter les professionnels qui franchissent la ligne rouge et, dans les cas les plus graves, mettre un terme à leur contrat. Remboursement sur demande Conscient des problèmes de réputation causé par les pratiques des courtiers indécents, les entreprises remboursent rubis sur l'ongle les clients malmenés. A condition qu'ils se manifestent ! Dans le cas d'une signature par SMS avec certains courtiers, Néoliane et SPVIE allongent le délai de rétractation à un mois. La sanction de l'ACPR contre SGP-Fillassur n'est pas pour rien dans le durcissement des contrôles des courtiers par les grossistes. Tout comme l'entrée en vigueur, quelques mois après, de la directive sur la distribution d'assurances qui a amélioré l'information et renforcé la protection des consommateurs. Les contrôles se poursuivent ces jours de vis, les mauvaises pratiques perdurent. « Nos contrôles se poursuivent et se poursuivront, sans nous priver de notre pouvoir de remonter jusqu'aux assureurs », prévient Nathalie Beaudemoulin, directrice du contrôle des pratiques commerciales de l'ACPR. Reste que les téléphones n'ont pas fini de sonner chez les particuliers. Le Parlement est, certes, en train de discuter d'une proposition de loi visant à encadrer plus strictement le démarchage téléphonique. « Les associations de consommateurs plaident pour que, par défaut, il devienne impossible de démarcher un consommateur qui n'a pas donné son accord », explique Olivier Gayraud de la CLCV. Malheureusement, tel ne sera pas le cas, le texte actuel ayant déjà été largement édulcoré... Elodie Toustou Des informations personnelles de 33 millions de Français sont dans la nature après une cyberattaque visant des acteurs du tiers payant. Vigilance ! Votre identité et votre numéro de Sécurité sociale sont peut-être entre de très mauvaises mains. En moins d'une semaine, Viamedis et Almyers, deux entreprises inconnues du grand public, mais stratégiques dans le secteur des remboursements des dépenses de santé, ont officiellement annoncé avoir été victimes d'une cyberattaque. Ces prestataires sont des spécialistes de la gestion du tiers payant entre professionnels de santé et assurances et mutuelles, ce système qui dispense les patients de faire l'avance des frais à leur médecin, leur dentiste, leur opticien, leur pharmacien... Des centaines d'assureurs, mutuelles et courtiers (voir tableau ci-dessous) ont appelé à leurs services. A LIRE AUSSI >>> Vol de données des mutuelles : porter plainte, à quoi ça sert ? Les attaquants ont ainsi mis la main sur les données personnelles de plus de 33 millions de Français, a annoncé la Commission nationale de l'informatique et des libertés (Cnil), qui va « mener très rapidement des investigations ». Leur technicien utilisant les bases de données de professionnels de santé (médecins, pharmaciens, infirmiers, etc.) et d'assurances maladie (être le patient ou l'assuré). Il s'agit du nom, des prénoms, de la date de naissance et du numéro de Sécurité sociale des assurés. Ainsi que le nom de l'assureur, le numéro des contrats et les garanties associées. En revanche, Viamedis a assuré à l'AFP que « ni information bancaire, ni coordonnées postale, ni numéro de téléphone, ni mail ne sont concernés par cet acte malveillant ». Il en est de même pour les détails des remboursements des frais de santé ou les données médicales des patients. Des informations confirmées par la Cnil. A LIRE AUSSI >>> Mutuelle santé : 10 conseils pour bien choisir votre contrat Si des assurés nous ont signalé avoir reçu un mail de la part de leur assurance complémentaire ou de leur mutuelle les informant de ce piratage de données, tous n'y ont pas forcément prêté attention. Tout comme aux messages s'affichant dans leur espace client, s'ils ne s'y sont pas connectés récemment. La Cnil va toutefois veiller à ce que les bénéficiaires concernés soient bien informés individuellement « comme le prévoit le règlement général sur la protection des données (RGPD) ». Le tableau ci-dessous liste tous les organismes touchés (plus d'une centaine), vous pouvez y faire une recherche par nom. Ce vol massif de données doit-il inquiéter ? Évidemment oui, même si les cyberattaquants ne disposent pas des adresses mail, du téléphone, de l'adresse postale ou du RIP des particuliers. Les fuites et les vols de données étant monnaie courante, rien n'est plus facile pour les personnes malintentionnées que de croiser plusieurs bases piratées et de consolider les résultats. Ce qui permettrait, par exemple, de reconstituer les données quasi complètes d'un particulier si son adresse mail contient son nom de famille. A LIRE AUSSI >>> « La Caisse de retraite a-t-elle une erreur dans ma pension, mais ne la corrige pas » Le fait que les cyberattaquants aient en leur possession le numéro de Sécurité sociale des assurés n'est pas très rassurant non plus. Ce numéro pouvant notamment être utilisé pour accéder à une multitude de services en ligne via le service France Connect : impôts, retraite, allocations, chômage, etc.

renouvellement de papiers d'identité, immatriculation d'un véhicule, etc. Vigilance dans les semaines et les mois à venir ! Comment réagir si vous êtes dérobé ? En changeant le mot de passe associé à votre compte d'Assurance maladie (être le patient ou l'assuré). Il s'agit du nom, des prénoms, de la date de naissance et du numéro de Sécurité sociale des assurés. Ainsi que le nom de l'assureur, le numéro des contrats et les garanties associées. En revanche, Viamedis a assuré à l'AFP que « ni information bancaire, ni coordonnées postale, ni numéro de téléphone, ni mail ne sont concernés par cet acte malveillant ». Il en est de même pour les détails des remboursements des frais de santé ou les données médicales des patients. Des informations confirmées par la Cnil. A LIRE AUSSI >>> Mutuelle santé : 10 conseils pour bien choisir votre contrat Si des assurés nous ont signalé avoir reçu un mail de la part de leur assurance complémentaire ou de leur mutuelle les informant de ce piratage de données, tous n'y ont pas forcément prêté attention. Tout comme aux messages s'affichant dans leur espace client, s'ils ne s'y sont pas connectés récemment. La Cnil va toutefois veiller à ce que les bénéficiaires concernés soient bien informés individuellement « comme le prévoit le règlement général sur la protection des données (RGPD) ». Le tableau ci-dessous liste tous les organismes touchés (plus d'une centaine), vous pouvez y faire une recherche par nom. Ce vol massif de données doit-il inquiéter ? Évidemment oui, même si les cyberattaquants ne disposent pas des adresses mail, du téléphone, de l'adresse postale ou du RIP des particuliers. Les fuites et les vols de données étant monnaie courante, rien n'est plus facile pour les personnes malintentionnées que de croiser plusieurs bases piratées et de consolider les résultats. Ce qui permettrait, par exemple, de reconstituer les données quasi complètes d'un particulier si son adresse mail contient son nom de famille. A LIRE AUSSI >>> « La Caisse de retraite a-t-elle une erreur dans ma pension, mais ne la corrige pas » Le fait que les cyberattaquants aient en leur possession le numéro de Sécurité sociale des assurés n'est pas très rassurant non plus. Ce numéro pouvant notamment être utilisé pour accéder à une multitude de services en ligne via le service France Connect : impôts, retraite, allocations, chômage, etc.

renouvellement de papiers d'identité, immatriculation d'un véhicule, etc. Vigilance dans les semaines et les mois à venir ! Comment réagir si vous êtes dérobé ? En changeant le mot de passe associé à votre compte d'Assurance maladie (être le patient ou l'assuré). Il s'agit du nom, des prénoms, de la date de naissance et du numéro de Sécurité sociale des assurés. Ainsi que le nom de l'assureur, le numéro des contrats et les garanties associées. En revanche, Viamedis a assuré à l'AFP que « ni information bancaire, ni coordonnées postale, ni numéro de téléphone, ni mail ne sont concernés par cet acte malveillant ». Il en est de même pour les détails des remboursements des frais de santé ou les données médicales des patients. Des informations confirmées par la Cnil. A LIRE AUSSI >>> Mutuelle santé : 10 conseils pour bien choisir votre contrat Si des assurés nous ont signalé avoir reçu un mail de la part de leur assurance complémentaire ou de leur mutuelle les informant de ce piratage de données, tous n'y ont pas forcément prêté attention. Tout comme aux messages s'affichant dans leur espace client, s'ils ne s'y sont pas connectés récemment. La Cnil va toutefois veiller à ce que les bénéficiaires concernés soient bien informés individuellement « comme le prévoit le règlement général sur la protection des données (RGPD) ». Le tableau ci-dessous liste tous les organismes touchés (plus d'une centaine), vous pouvez y faire une recherche par nom. Ce vol massif de données doit-il inquiéter ? Évidemment oui, même si les cyberattaquants ne disposent pas des adresses mail, du téléphone, de l'adresse postale ou du RIP des particuliers. Les fuites et les vols de données étant monnaie courante, rien n'est plus facile pour les personnes malintentionnées que de croiser plusieurs bases piratées et de consolider les résultats. Ce qui permettrait, par exemple, de reconstituer les données quasi complètes d'un particulier si son adresse mail contient son nom de famille. A LIRE AUSSI >>> « La Caisse de retraite a-t-elle une erreur dans ma pension, mais ne la corrige pas » Le fait que les cyberattaquants aient en leur possession le numéro de Sécurité sociale des assurés n'est pas très rassurant non plus. Ce numéro pouvant notamment être utilisé pour accéder à une multitude de services en ligne via le service France Connect : impôts, retraite, allocations, chômage, etc.

renouvellement de papiers d'identité, immatriculation d'un véhicule, etc. Vigilance dans les semaines et les mois à venir ! Comment réagir si vous êtes dérobé ? En changeant le mot de passe associé à votre compte d'Assurance maladie (être le patient ou l'assuré). Il s'agit du nom, des prénoms, de la date de naissance et du numéro de Sécurité sociale des assurés. Ainsi que le nom de l'assureur, le numéro des contrats et les garanties associées. En revanche, Viamedis a assuré à l'AFP que « ni information bancaire, ni coordonnées postale, ni numéro de téléphone, ni mail ne sont concernés par cet acte malveillant ». Il en est de même pour les détails des remboursements des frais de santé ou les données médicales des patients. Des informations confirmées par la Cnil. A LIRE AUSSI >>> Mutuelle santé : 10 conseils pour bien choisir votre contrat Si des assurés nous ont signalé avoir reçu un mail de la part de leur assurance complémentaire ou de leur mutuelle les informant de ce piratage de données, tous n'y ont pas forcément prêté attention. Tout comme aux messages s'affichant dans leur espace client, s'ils ne s'y sont pas connectés récemment. La Cnil va toutefois veiller à ce que les bénéficiaires concernés soient bien informés individuellement « comme le prévoit le règlement général sur la protection des données (RGPD) ». Le tableau ci-dessous liste tous les organismes touchés (plus d'une centaine), vous pouvez y faire une recherche par nom. Ce vol massif de données doit-il inquiéter ? Évidemment oui, même si les cyberattaquants ne disposent pas des adresses mail, du téléphone, de l'adresse postale ou du RIP des particuliers. Les fuites et les vols de données étant monnaie courante, rien n'est plus facile pour les personnes malintentionnées que de croiser plusieurs bases piratées et de consolider les résultats. Ce qui permettrait, par exemple, de reconstituer les données quasi complètes d'un particulier si son adresse mail contient son nom de famille. A LIRE AUSSI >>> « La Caisse de retraite a-t-elle une erreur dans ma pension, mais ne la corrige pas » Le fait que les cyberattaquants aient en leur possession le numéro de Sécurité sociale des assurés n'est pas très rassurant non plus. Ce numéro pouvant notamment être utilisé pour accéder à une multitude de services en ligne via le service France Connect : impôts, retraite, allocations, chômage, etc.

renouvellement de papiers d'identité, immatriculation d'un véhicule, etc. Vigilance dans les semaines et les mois à venir ! Comment réagir si vous êtes dérobé ? En changeant le mot de passe associé à votre compte d'Assurance maladie (être le patient ou l'assuré). Il s'agit du nom, des prénoms, de la date de naissance et du numéro de Sécurité sociale des assurés. Ainsi que le nom de l'assureur, le numéro des contrats et les garanties associées. En revanche, Viamedis a assuré à l'AFP que « ni information bancaire, ni coordonnées postale, ni numéro de téléphone, ni mail ne sont concernés par cet acte malveillant ». Il en est de même pour les détails des remboursements des frais de santé ou les données médicales des patients. Des informations confirmées par la Cnil. A LIRE AUSSI >>> Mutuelle santé : 10 conseils pour bien choisir votre contrat Si des assurés nous ont signalé avoir reçu un mail de la part de leur assurance complémentaire ou de leur mutuelle les informant de ce piratage de données, tous n'y ont pas forcément prêté attention. Tout comme aux messages s'affichant dans leur espace client, s'ils ne s'y sont pas connectés récemment. La Cnil va toutefois veiller à ce que les bénéficiaires concernés soient bien informés individuellement « comme le prévoit le règlement général sur la protection des données (RGPD) ». Le tableau ci-dessous liste tous les organismes touchés (plus d'une centaine), vous pouvez y faire une recherche par nom. Ce vol massif de données doit-il inquiéter ? Évidemment oui, même si les cyberattaquants ne disposent pas des adresses mail, du téléphone, de l'adresse postale ou du RIP des particuliers. Les fuites et les vols de données étant monnaie courante, rien n'est plus facile pour les personnes malintentionnées que de croiser plusieurs bases piratées et de consolider les résultats. Ce qui permettrait, par exemple, de reconstituer les données quasi complètes d'un particulier si son adresse mail contient son nom de famille. A LIRE AUSSI >>> « La Caisse de retraite a-t-elle une erreur dans ma pension, mais ne la corrige pas » Le fait que les cyberattaquants aient en leur possession le numéro de Sécurité sociale des assurés n'est pas très rassurant non plus. Ce numéro pouvant notamment être utilisé pour accéder à une multitude de services en ligne via le service France Connect : impôts, retraite, allocations, chômage, etc.

renouvellement de papiers d'identité, immatriculation d'un véhicule, etc. Vigilance dans les semaines et les mois à venir ! Comment réagir si vous êtes dérobé ? En changeant le mot de passe associé à votre compte d'Assurance maladie (être le patient ou l'assuré). Il s'agit du nom, des prénoms, de la date de naissance et du numéro de Sécurité sociale des assurés. Ainsi que le nom de l'assureur, le numéro des contrats et les garanties associées. En revanche, Viamedis a assuré à l'AFP que « ni information bancaire, ni coordonnées postale, ni numéro de téléphone, ni mail ne sont concernés par cet acte malveillant ». Il en est de même pour les détails des remboursements des frais de santé ou les données médicales des patients. Des informations confirmées par la Cnil. A LIRE AUSSI >>> Mutuelle santé : 10 conseils pour bien choisir votre contrat Si des assurés nous ont signalé avoir reçu un mail de la part de leur assurance complémentaire ou de leur mutuelle les informant de ce piratage de données, tous n'y ont pas forcément prêté attention. Tout comme aux messages s'affichant dans leur espace client, s'ils ne s'y sont pas connectés récemment. La Cnil va toutefois veiller à ce que les bénéficiaires concernés soient bien informés individuellement « comme le prévoit le règlement général sur la protection des données (RGPD) ». Le tableau ci-dessous liste tous les organismes touchés (plus d'une centaine), vous pouvez y faire une recherche par nom. Ce vol massif de données doit-il inquiéter ? Évidemment oui, même si les cyberattaquants ne disposent pas des adresses mail, du téléphone, de l'adresse postale ou du RIP des particuliers. Les fuites et les vols de données étant monnaie courante, rien n'est plus facile pour les personnes malintentionnées que de croiser plusieurs bases piratées et de consolider les résultats. Ce qui permettrait, par exemple, de reconstituer les données quasi complètes d'un particulier si son adresse mail contient son nom de famille. A LIRE AUSSI >>> « La Caisse de retraite a-t-elle une erreur dans ma pension, mais ne la corrige pas » Le fait que les cyberattaquants aient en leur possession le numéro de Sécurité sociale des assurés n'est pas très rassurant non plus. Ce numéro pouvant notamment être utilisé pour accéder à une multitude de services en ligne via le service France Connect : impôts, retraite, allocations, chômage, etc.

renouvellement de papiers d'identité, immatriculation d'un véhicule, etc. Vigilance dans les semaines et les mois à venir ! Comment réagir si vous êtes dérobé ? En changeant le mot de passe associé à votre compte d'Assurance maladie (être le patient ou l'assuré). Il s'agit du nom, des prénoms, de la date de naissance et du numéro de Sécurité sociale des assurés. Ainsi que le nom de l'assureur, le numéro des contrats et les garanties associées. En revanche, Viamedis a assuré à l'AFP que « ni information bancaire, ni coordonnées postale, ni numéro de téléphone, ni mail ne sont concernés par cet acte malveillant ». Il en est de même pour les détails des remboursements des frais de santé ou les données médicales des patients. Des informations confirmées par la Cnil. A LIRE AUSSI >>> Mutuelle santé : 10 conseils pour bien choisir votre contrat Si des assurés nous ont signalé avoir reçu un mail de la part de leur assurance complémentaire ou de leur mutuelle les informant de ce piratage de données, tous n'y ont pas forcément prêté attention. Tout comme aux messages s'affichant dans leur espace client, s'ils ne s'y sont pas connectés récemment. La Cnil va toutefois veiller à ce que les bénéficiaires concernés soient bien informés individuellement « comme le prévoit le règlement général sur la protection des données (RGPD) ». Le tableau ci-dessous liste tous les organismes touchés (plus d'une centaine), vous pouvez y faire une recherche par nom. Ce vol massif de données doit-il inquiéter ? Évidemment oui, même si les cyberattaquants ne disposent pas des adresses mail, du téléphone, de l'adresse postale ou du RIP des particuliers. Les fuites et les vols de données étant monnaie courante, rien n'est plus facile pour les personnes malintentionnées que de croiser plusieurs bases piratées et de consolider les résultats. Ce qui permettrait, par exemple, de reconstituer les données quasi complètes d'un particulier si son adresse mail contient son nom de famille. A LIRE AUSSI >>> « La Caisse de retraite a-t-elle une erreur dans ma pension, mais ne la corrige pas » Le fait que les cyberattaquants aient en leur possession le numéro de Sécurité sociale des assurés n'est pas très rassurant non plus. Ce numéro pouvant notamment être utilisé pour accéder à une multitude de services en ligne via le service France Connect : impôts, retraite, allocations, chômage, etc.

- format of petty cash book in excel
- wujigo
- http://studioingenegeneramot.com/userfiles/files/18984425979.pdf
- is where the red fern grows a banned book
- doyeha
- what is hydraulic test of boiler
- shell shockers aimbot apk
- homedics 531 scale battery replacement
- what day is it in act 3 scene 3 roméo and juliet