الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م ا م

LETTRE D'INFORMATION : BON A SAVOIR (N°14)

La conformité : Compliance Officer, RCSI et RCCI

Définition

La compliance, en français conformité, tire sa source de la règlementation bancaire et financière : les travaux de Bâle II repris par le Règlement 97-02 du Comité de la Règlementation Bancaire et Financière, applicable aux établissements de crédit et aux entreprises d'investissement ; les Directives européennes, dont la Directive MIF (Marchés d'Instruments Financiers) transposée par le Règlement Général de l'Autorité des Marchés Financiers (AMF).

La fonction de conformité est une fonction indépendante qui identifie, évalue, et contrôle le risque de non-conformité de l'établissement, défini comme le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative, ou d'atteinte à la réputation, qui naît du non respect de dispositions propres aux activités bancaires et financières, qu'elles soient de nature législatives ou règlementaires, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions de l'organe exécutif.

Le responsable de la conformité a également un rôle d'information, de formation et de conseil, tant vis-à-vis des collaborateurs que vis-à-vis de la direction de l'établissement.

Le champ de compétences de la conformité est donc très large.

Organisation

Dans les banques la fonction est confiée à un Directeur de la Conformité, dans les entreprises d'investissement elle est confiée à un Responsable de la Conformité des Services d'Investissement (RCSI) ou à un Responsable de la Conformité et du Contrôle Interne (RCCI) selon que l'on se trouve chez un prestataire de services d'investissement au sens large (transmission et exécution des ordres de bourse, conservation de titres, investissement pour compte propre etc…) ou bien dans une société de gestion de portefeuille.

Ces différences sémantiques qui désignent peu ou prou une même fonction et une même réalité, tiennent à la diversité tant des règlementations que des autorités de supervision bancaires et financières ainsi qu'à leur histoire.

Dans les grands établissements, aux activités souvent multiples, la fonction est remplie par un Département de la Conformité, doté d'un personnel nombreux.

Dans des établissements de plus petite dimension, elle est souvent remplie par une seule et unique personne qui cumule les fonctions de déontologue, contrôleur interne, responsable de la lutte anti blanchiment avec celle de responsable de la conformité.

Enfin dans les plus petites entités elle peut être concentrée entre les mains d'un dirigeant, qui peut en déléguer l'exécution à un prestataire externe. Cette délégation peut même, dans certains cas, être encouragée, voire imposée, par l'Autorité des Marchés Financiers, qui y voit une assurance de professionnalisme et d'indépendance.
Les fonctions de contrôle interne et d'audit sont très proches. Si dans bien des cas les fonctions de contrôle interne et de conformité peuvent être regroupées, il en va différemment de l'audit, ou de l'inspection, qui doivent être indépendantes, de façon à pouvoir contrôler toutes les activités de l'entreprise, y compris la conformité.
La fonction de conformité est distincte de la fonction juridique à proprement parler, en cela qu'elle traite de l'application au sein de l'établissement et dans son activité de l'ensemble de règles qui régissent la profession ; mais sans interférer dans le règlement des litiges qui peuvent opposer la société à des tiers, ni dans les différends d'ordre contractuels. Cependant il n'est pas impossible de regrouper la fonction juridique avec la conformité, bien, qu'à notre sens, cette dernière soit de nature complètement différente, en raison de sa dimension de contrôle.
Enfin la fonction de conformité est incompatible avec la réalisation d'opérations comptables, commerciales, ou financières.
En termes de hiérarchie, elle doit, lorsqu'elle n'est pas confiée à un membre de l'organe exécutif, être rattachée directement à la direction générale de l'entreprise, ou tout au moins à un niveau d'autorité suffisant pour assurer son indépendance vis-à-vis des autres services.

Le compliance officer

Le compliance officer, ou le responsable de la conformité, a non seulement un rôle d'identification de la règlementation financière, du code de bonne conduite et des bonnes pratiques professionnelles à suivre ainsi que de contrôle de leur application ; mais aussi un rôle de conseil, d'information et de formation.

Définition et application des règles

Le responsable de la conformité identifie les règles applicables et met en place les procédures visant à leur respect par l'ensemble de personnel.
Il identifie les conflits d'intérêts potentiels et met en place des règles de gestion lorsqu'ils ne peuvent pas être évités, comme la tenue d'un registre des conflits d'intérêts. Il met en place des procédures connues sous le nom de « Murailles de Chine », afin de prémunir la société contre la circulation indue d'informations confidentielles.
Bien que le terme ait disparu du vocabulaire règlementaire, il est aussi déontologue : il définit les règles déontologiques, identifie le personnel concerné et fixe les restrictions en matière de transactions personnelles.
Il dresse la liste du personnel dont les conversations téléphoniques peuvent être enregistrées et est compétent pour procéder à leur écoute.

Contrôle

Rôle de contrôle : le responsable de la conformité effectue des contrôles de second niveau, réguliers, afin d'identifier les violations des règles que nous venons de citer. Parmi ces contrôles nous pouvons citer :

- Le contrôle du respect des procédures par les services opérationnels ainsi que l'exécution des contrôles de premier niveau.
- Dans une société de gestion de portefeuilles le respect des contraintes d'investissement
- Dans une entreprise d'investissement, quelque soit son métier, le respect par le personnel, des règles de transaction pour son propre compte, et, plus généralement du code de déontologie.

- Le contrôle de la prévention des abus de marché…

Ces contrôles donnent lieu à un reporting à la Direction, mais aussi, dans certains cas comme dans celui de l'abus de marché, à l'autorité de supervision.

Information et Conseil

Il conseille la direction pour la mise en place de produits nouveaux et s'assure à cette occasion que l'ensemble des mesures destinées à prévenir le risque de non-conformité ont bien été identifiées. De façon plus générale il conseille le management de l'entreprise sur l'application de la règlementation, par exemple en cas de communication de crise.

Il informe et forme le personnel sur tous les sujets de sa compétence. Il est par exemple de bonne pratique que tout nouvel entrant dans la société se voit expliquer par le responsable de la conformité les règles déontologiques en vigueur. Cette information est renouvelée à destination de l'ensemble du personnel à chaque évolution de la règlementation.

Il est responsable de la lutte anti-blanchiment et contre le financement du terrorisme et s'assure de l'existence de procédures dans ce domaine ainsi que de leur respect.

Il est le correspondant attitré des autorités de supervision, et, à ce titre leur soumet des rapports réguliers sur son activité. En France, RCCI et RCSI se voient attribuer une carte professionnelle par l'AMF, tandis que la nomination et le départ du Directeur de la Conformité, dans les banques, doivent être notifiés à la Commission Bancaire. De même, en cas d'externalisation, l'AMF autorise le recours à un prestataire après s'être entretenu avec ce dernier et le responsable de l'entreprise, sur la nature et l'étendue de sa mission.

Il va sans dire que le Responsable de la Conformité doit disposer de moyens en rapport avec l'étendue de ses tâches. Ces moyens autonomes et suffisants incluent des outils informatiques ad-hoc.

Lorsque ces moyens sont partagés avec d'autres services, comme par exemple, le juridique ou le contrôle interne, le partage doit être clairement identifié et des mécanismes de coopération mis en place.

Il est destinataire des alertes des membres du personnel sur les éventuels dysfonctionnements dont ils peuvent être témoins. Ce dispositif, connue sous le nom de « droit d'alerte » a été mis en place dans la réglementation française à la suite de la transposition de la MIF et est inspiré du « whistle blowing » de la loi Sarbanes-Oxley (Sox).

Conclusion

Les évènements que nous avons vécus ces dernières années, comme les affaires Enron et World com ont conduit les législateurs à durcir les obligations de contrôle interne : loi Sox aux Etats-Unis et loi de Sécurité Financière (LES) en France, par exemple. Les travaux du Comité de Bâle et les Directives Européennes ont insisté sur l'obligation de mettre en place une fonction de conformité indépendante et dotée de moyens suffisants. En France, cette obligation a été transposée dans la loi (Code Monétaire et Financier) ainsi que dans la règlementation bancaire et financière (CRBF et RGAMF).

Les développements récents de l'actualité sont symptomatiques d'une absence de conformité aux règles déontologiques et aux bonnes pratiques professionnelles, comme celle qui consiste, pour une banque, à ne pas pousser ses clients emprunteurs au surendettement, ou à proposer des produits financiers complexes inadaptés aux besoins des investisseurs.

Le compliance officer est un élément essentiel de la protection de son établissement contre le risque opérationnel, il joue également un rôle dans la protection de l'intégrité

des marchés et est garant de la primauté des intérêts des clients. Son autorité sortira vraisemblablement renforcée de la crise actuelle des institutions financières.

Le métier de Compliance Officer

Qu'est-ce qu'un Compliance Officer ?

Le Compliance Officer – également connu sous le nom de Gestionnaire KYC (Know Your Customer) – est avant tout un professionnel de l'éthique. Son rôle principal est de détecter les transactions suspectes dans les établissements bancaires. Il s'agit en particulier de vérifier l'origine des fonds, l'identité des personnes intéressées ainsi que la cause du transfert.

Cet expert s'assure ainsi de la conformité des transactions aux différentes réglementations bancaires et aux législations en vigueur. Il assume également le rôle de conseiller et de formateur auprès des responsables de l'institution financières qui l'emploie.

Quelles sont les qualités nécessaires pour réussir le métier de Compliance Officer

Ce professionnel de l'éthique doit être doté d'une forte personnalité et d'un excellent relationnel, car il est amené à se mettre en relation avec plusieurs intervenants. D'ailleurs, il est l'interlocuteur direct du régulateur.

D'autre part, une grande probité est l'une des qualités indispensables pour mener à bien les missions qu'on lui confie. Le Compliance Officer doit aussi être curieux, du fait qu'il doit s'informer sur l'évolution des réglementations.

Quelles sont les difficultés rencontrées par le Compliance Officer ?

Le Responsable de Conformité est souvent obligé de travailler à des horaires flexibles, ce qui est assez éprouvant. Il doit aussi être capable de gérer le stress, étant donné qu'il doit faire face à de nombreuses pressions suite à des décisions qu'il a prises (clôture de compte d'un client douteux ou refus de collaboration avec un opérateur économique suspect).

Contrôle Anti-blanchiment d'Argent (AML/CTF)

Le contrôle et le suivi des transferts d'argent, le comportement des capitaux et des clients sont, de nos jours, devenu extrêmement important pour les organisations financières qui tentent de protéger leurs affaires. Les réglementations des pays sont devenues plus strictes pour assurer une activité financière irréprochable et pour prévenir le blanchiment d'argent et assurer la provenance des fonds.

Aperçu

La solution Contrôle Anti-Blanchiment d'Argent est une solution verticale, se servant des meilleures pratiques de la branche et d'une technologie unique conçue pour aider les institutions financières à se conformer aux normes de lutte contre le blanchiment d'argent. Peut être déployée à part des autres solutions, ou parfaitement intégrée avec le système existant de la Banque.

La solution AML se concentre sur le profil Know Your Customer (KYC) ainsi que sur la notation du client de et son Historique, en fournissant également la Liste de Gestion de Suivi AML contre de nombreuses listes de surveillance et, la Recherche d'Activités Suspectes par le moyen de l'Analyse Transactionnelle du Comportement du client.

Caractéristiques

- Puissant moteur KYC relié aux mécanismes proactifs de contrôle de risques
- Paramétrisations des alertes selon de nombreuses dimensions qualitatives et quantitatives
- Suivi et notation du comportement transactionnel et social du client au moyen de questionnaires
- Listes locales, globales et manuelles d'assistance à la surveillance
- Traitement des données transactionnelles concernant les transactions à valeur élevée et les activités excessives pour les clients
- Vérification en ligne des clients et contrôle des Transferts de Fonds par rapport aux listes de surveillance en présence
- Génération d'alertes en ligne et par lot pour renforcer le suivi et l'investigation

Avantages

- Protège votre entreprise
- Surveille les transactions à tout moment
- Renvoi dans les listes de surveillance internationales
- Être informé par des alertes pour toutes anomalies de comportement

IBAN, BIC :

IBAN et BIC sont 2 sigles qu'il vous faut connaître avant d'effectuer (ou recevoir) un virement à l'étranger.

IBAN :

L'International Bank Account Number est un numéro de compte bancaire européen standardisé, utilisé pour les paiements transfrontaliers (zone E.E.E.).

Il est opérationnel dans tous les pays qui ont choisi d'utiliser cet identifiant bancaire.

L'IBAN se compose du code pays ISO, d'un nombre de contrôle de 2 chiffres et du numéro de compte national existant.

Il est obligatoire de mentionner l'IBAN. De plus il permet un acheminement plus rapide avec une tarification adaptée.

BIC :

Le Bank Identifier Code est l'identifiant normalisé international de banque**.**

Il est également connu sous la dénomination « adresse SWIFT » et il est mondialement utilisé.

Il peut être représenté sous 2 versions :

- identification de la banque en 8 caractères (siège social de la banque), exemple : AGRIFRPP,
- identification de la banque en 11 caractères (succursale de la banque), exemple : AGRIFRPP810

Les trois derniers caractères ne doivent pas être des X.

Info pratique : Attitude à adopter en cas de réception d'un e-mail étrange voire douteux

Vous recevez un e-mail étrange voire douteux, vous craignez être victime d'une arnaque ? Apprenez à les identifier et adoptez une attitude visant à contribuer à la destruction de ces réseaux.

Vous avez certes, la possibilité de nous contacter [en cliquant ici] pour que nous vous assistions dans les démarches nécessaires à la défense de vos intérêts, mais vous

trouverez ci-dessous, en plus des différentes formes d'arnaques, les organismes à contacter.

Les arnaques les plus courantes sont appelées les #Arnaques à la Nigériane ou #Scam 419. Ce n'est pas parce que les attaques viennent principalement du Nigéria que ces attaques s'appellent les attaques à la nigériane. Pour preuve, en terme d'origines d'attaques, le Nigéria arrive en troisième position loin derrière les états-unis d'Amérique et le royaume uni, mais parce que le Nigéria a été le premier pays d'Afrique à réagir face à la recrudescence de ces types d'attaques en modifiant son code pénal et en y ajoutant une section 4-1-9 traitant un type d'arnaque détaillé ci dessous. Le mot SCAM, quant à lui, est un terme argotique anglais désignant « arnaque ».

Différentes formes d'arnaques

L'arnaque à la loterie (le plus ancien)

Ca commence souvent par un e-mail de la part d'une « Fondation Microsoft » dont le siège social serait opportunément en Afrique ? ou d'une marque rassurante comme Coca Cola ou Heineken avec le nom d'un huissier ou d'un avocat à contacter d etoute urgence pour retirer son gain. Il y a aussi parfois des termes incitatifs du type « Avis de gains » ou « Réclamation ». Attiré par l'aubaine, vous répondez, vous recevez alors un autre mail expliquant les modalités du concours, expliquant comment votre mail est ainsi sorti du chapeau. Après vient une autre surprise. L'interlocuteur demande de régler au préalable un certain nombre de frais : avocats, gestions, douanes le plus souvent via Western Union, Money Gram ou même par mandats cash récupérer les sommes en liquide. S'il propose un virement, c'est pour crédibiliser sa démarche, des « contraintes techniques le ramèneront vers vous pour revenir aux mandats.

L'arnaque aux mandats cash

Un « propriétaire très altruiste » met en location un bien dans un quartier plutôt prisé de n'importe quelle ville, à un prix défiant toute concurrence. Le tout sous couvert de « il ne veut pas le laisser vide, il n'a pas besoin de cette source de revenus en plus… » Bien entendu, il vous demande une photo pour preuve du dépôt du mandat en vous spécifiant de cacher le code…sauf que le numéro resté visible suffit pour aller retirer l'argent. Il est important de signaler que ces arnaques existent aussi bien pour des annonces de location immobilière, d'achat de véhicule, d'achat d'immobilier…

Sites de vente de particulier à particulier (LeBonCoin.fr, EBay et Adoos).

Dans ce type de formats, l'escroc, le plus souvent par le biais de sites de petites annonces en ligne tentera de vous faire croire qu'il cède gracieusement un certain nombre d'affaires. Véhicules animaux, high-tech… tout y passe. Mais les frais sont à la charge de la victime potentielle. La mécanique de l'escroquerie est assez simple. Dans le meilleur des cas, la victime obtient un faux de mauvaise qualité. Mais la plupart du temps, il s'agit d'amener la cible, souvent une personne recherchant une voiture, à régler un certains nombre de frais.

Arnaque à la mise sous pli

La personne vous offre un emploi en or : vous devez juste envoyer des mails ou mettre sous pli des brochures. Le tout pour un salaire attractif bien sûr. « L'employeur » essaye alors d'endormir la méfiance en citant des soi-disant articles de loi insistant sur la légalité de la procédure et indique même des démarches à faire pour vous déclarer si vous dépassez un seuil de revenus. La seule chose qu'elle vous demande en contre partie : envoyer une somme, souvent petite pour le kit de démarrage. Après un échange de mail plus ou moins long, on vous annoncera qu'il

faut payer par mandat cash. Dès que la personne vous aura délesté de votre argent, vous pouvez être sûr qu'elle disparaîtra dans la nature.

Offres de prêts aux personnes en difficulté

Ces arnaques se sont développées sur le dos de la crise économique. Elle vise les personnes en difficulté financière qui y verraient une opportunité intéressante de se refaire une santé à moindre frais. Le principe est archi-simple. Un particulier vous contacte par mail pour vous proposer des offres de prêts à des conditions sans concurrence possible. Elle vous invite à remplir un formulaire pour postuler. Cela implique notamment de fournir vos coordonnées bancaires. En retour, un mail invite le postulant à régler des frais de dossier. Au mieux, l'argent des frais disparaît, au pire, le compte en banque de la victime est vidé. A noter que des escrocs des Pays de l'Est pratiquent des arnaques similaires. Prêt juste et honnête et fiable. Alors si vous avez besoin de prêt n'hésitez pas à me contacter pour en savoir plus sur mes conditions. Veuillez me contacter directement par Email : vince438@hotmail.com

DuplicoSite

Prenez un site très prisé, RueduCommerce.com par exemple, transformez-le un tout petit peu, en RDCommerce.com, et les internautes s'y perdent très vite. Un internaute avait acheté une couette à 100 euros qui n'est jamais arrivée. « Pour moi c'était le même site, c'était Rueducommerce. Les couleurs étaient identiques, tout comme le logo. Il y avait une très bonne promotion donc je me suis dit c'était une affaire », raconte-t-il. Et pour se faire rembourser, c'est le parcours du combattant. Si bien que ces sites frauduleux en profitent. Le temps qu'une victime s'aperçoive de la supercherie, envoie des courriers recommandés, fasse appel à des associations et porte plainte et le temps que des dizaines de plaintes débouchent enfin sur une enquête, puis sur un jugement au tribunal, il peut très vite s'écouler un an. Souvent, les fraudeurs sont basés à l'étranger, ils sont quasiment intouchables.

Appel à la générosité ou aux dons

Cette technique particulièrement opportuniste consiste à faire appel à la générosité des internautes pour les grandes causes : catastrophes naturelles, guerres, famines… Ils ont été particulièrement actifs après le séisme en Haïti. Les escrocs aux commandes de ce type d'opération sont particulièrement réactifs, s'adaptant très rapidement à l'actualité. Sinistrés d'Haïti, Ebola, aider un enfant à terminer ses études…

Petites livraisons

Idem à la mise sous pli mais les personnes escroquées étant, bien malgré elle, rendues complices de l'escroquerie. « Sous de faux noms d'entreprises tels Total Success World ou Flashvision-, plusieurs réseaux recruteraient depuis 2009 des employés dont ils feraient par la suite des complices de vols ». Des petites annonces postées sur Internet font miroiter aux demandeurs d'emploi un salaire de 1000 euros à 2500 euros par mois pour une mission simple : réexpédier des colis en Afrique. Sauf que les colis sont parfois des achats réalisés avec des cartes bancaires volées. « Ces organisations se servent de leurs coordonnées postales, obtenues grâce à un faux contrat de travail, pour effectuer des achats sur Internet. Les colis sont ensuite envoyés chez la victime, qui doit les réexpédier en Afrique, où sont basés ces réseaux. » Et bien entendues, elles ne sont jamais payées…

Chantage à la WebCam

Dans ce type de format, une femme ou un homme contacte sa victime via un site de rencontre ou un réseau social, dans les mêmes circonstances qu'une accroche de « Romance » ou « Love Scam ». Là encore, les identifiants sont là pour rassurer la cible, les images pour la séduire, tirées de catalogues ou volées à un autre compte. L'escroc, toujours un homme, demande rapidement à son interlocuteur de passer sous

messagerie classique, en l'occurrence MSN. Pourquoi MSN ? Parce qu'une fonctionnalité peu ou mal connue des usagers permet à l'une des parties d'enregistrer les images diffusées via la webcam. L'escroc prend alors le temps de prendre un maximum d'informations sur sa victime, données qui pourront par ailleurs être utilisées pour ferrer une autre cible. Il propose alors des jeux plus « chauds ». Chacun des partenaires doit se livrer à des jeux sexuels devant la caméra. La victime a droit à un film le plus souvent pioché sur des sites pornos. Elle est alors en confiance pour se donner elle-même en spectacle. L'escroc enregistre puis se dévoile, menaçant sa victime de diffuser la vidéo auprès de vos familles et amis, dont il a pris les coordonnées. Dans certaines variantes, pas incompatibles avec la première, l'escroc se fait passer pour un service de police pour réclamer le paiement d'une amende pour attente aux bonnes mœurs, pédophile ou tout autre accusation destinée à pousser la victimes dans ses retranchements. Ce type de chantage a mené des personnes fragiles au suicide.

L'usurpation d'identité

Cette infraction, d'après Christophe Naudin, criminologue à l'université de Paris-II, est en hausse, elle atteignait en 2011 la 2ème place des infractions globales derrière le vol de voiture. Elle peut prendre plusieurs formes (emploi, logement…), mais à chaque fois invariablement on vous demande d'envoyer vos papiers d'identité. (les copies couleurs de votre carte vitale, carte d'identité et permis de conduire, ainsi que la photocopie d'un justificatif de domicile). C'est un cas flagrant de tentative de vol d'identité. Avec ces papiers en main, les arnaqeurs peuvent : – Ouvrir un compte en banque, – Vider votre compte en banque, – Réaliser des fraudes à l'assurance maladie, – Contrefaire un permis de conduire et c'est vous qui recevrez les amendes.

Phishing, ou tentative d'hameçonnage

Sous le terme générique de phishing, ou tentative d'hameçonnage, se cache toute une gamme d'escroqueries en provenance d'Afrique ou d'Europe de l'Est. La technique consiste à faire croire à la victime qu'elle se trouve en face du document officiel en provenance d'une banque, d'une administration, d'un fournisseur d'accès internet, d'un prestataire de carte de paiement… Ce document à en-tête, en général émis d'une adresse non conforme, et rarement exempt de fautes d'orthographe, n'a pour but que de vous amener à transmettre à l'escroc des données confidentielles, soit dans un champs proposé en complément, soit sur une page web falsifiée.

Les PaySafeCards

La PaySafeCard est un système européen de cartes prépayées dédiées à Internet. Pas besoin de compte bancaire ou de carte de paiement pour régler en ligne, il suffit d'acheter une PaySafeCard dont les valeurs vont de 10 à 100 euros. L'arnaqueur vous demande simplement d'acheter des PaysafeCards, que vous pouvez trouver chez votre buraliste, pour le régler. Vous ne verrez simplement ni la couleur de l'objet ni de l'argent et ni de l'arnaqueur.

Arnaques aux sentiments : LoveScam

Femme ou homme charmant, des liens s'établissement, la personne originaire de n'importe quel pays vit en afrique (souvent en cote d'Ivoire). Des liens se tissent et va essayer de vous arnaquer le plus vite et la plus grosse somme possible par différentes méthodes faisant appel aux sentiments : Aider à payer son loyer, son hôtel, ses factures d'électricité ou d'internet, victime d'une agression, est tombée malade et il faut régler des frais d'hospitalisation, d'opération… avec de faux certificats… Demande de payer le billet d'avion pour venir vous rejoindre en et devra payer un chèque voyage pour avoir le droit de sortir du pays. Elle se verra refuser l'embarquement pour trafic quelconque et se verra infliger une fore amende. Elle peut

vous signer une reconnaissance de dettes et vous régler même une avance par chèque (volé…).

Qui veut ~~gagner~~/hériter des Millions ?

Vous recevez un e-mail d'une riche personne qui pour récupérer l'argent de l'héritage a rapidement besoin d'une personne qui dispose d'un compte bancaire. Il s'agit systématiquement d'une grosse somme d'argent à récupérer et en échange de cette aide, elle offre un pourcentage sur la somme qui sera transférée, en général par la « voie diplomatique ». Si la victime accepte, on lui demandera petit à petit d'avancer des sommes d'argent destinées à couvrir des frais imaginaires (notaires, entreprises de sécurité, pots-de-vin…) avant que le transfert ne soit effectif ; bien entendu, ce transfert n'aura jamais lieu. Le record à ce jour est détenu par Janelia Spears a perdu 400 000 $ dans un scam nigérian lui promettant des millions. Elle a vidé le fond de retraite de son mari et a hypothéqué sa maison. Elle a emprunté des sommes colossales. Tout cela à durée deux ans.

L'ami en détresse

Les auteurs parviennent à pirater la boîte mail d'un ou une de vos amies ou contact. Ils utilisent ensuite sa liste de contacts pour envoyer un message d'alerte volontairement alarmiste. La personne affirme être bloquée dans un pays étranger, sans ressource après un problème quelconque (agression/maladie/perte de moyens de paiement), et sollicite une aide financière urgente pour s'en sortir. Cette aide doit être envoyée via un compte à l'inévitable Western Union. Beaucoup réagissent en téléphonant à l'ami en question pour se rendre compte que tout va bien. Dans la précipitation, certains envoient de l'argent. Lequel disparaît dans la poche des escrocs. Tout ceci est de l'Ingénierie sociale (l'art du tirer les vers du nez), afin de nuire, arnaquer, convaincre…

Signalez un contenu douteux ou illicite

Internet est un espace de liberté où chacun peut communiquer et s'épanouir. Les droits de tous doivent y être respectés, pour que la « toile » reste un espace d'échanges et de respect.

C'est pourquoi les pouvoirs publics mettent un site internet à disposition des citoyens. Sur ce site Internet, en cliquant sur le bouton « SIGNALER », vous pourrez transmettre des signalements de contenus ou de comportements illicites auxquels vous vous seriez retrouvés confrontés au cours de votre utilisation d'Internet. 25 mai 2016.

Lien : https://www.lenetexpert.fr/info-pratique-attitude-adopter-en-cas-reception-dun-e-mail-etrange-voire-douteux/

Que sont le Smishing et le Vishing ?

Le Smishing et le Vishing sont tous deux l'équivalent du Phishing (hameçonnage) sur Internet.

Smishing

Smishing est la contraction de SMS et de Phishing. On l'appelle également Hameçonnage par SMS.

Tout comme le phishing, un message à caractère urgent est envoyé à un utilisateur pour qu'il entreprenne une action. Lors d'un Smishing, c'est un message texte qui est envoyé à un utilisateur sur son téléphone. Le texte du message demande généralement à l'utilisateur d'appeler un numéro de téléphone ou de se rendre sur un site Internet pour effectuer une action précise. La plupart du temps, lorsque vous composez ce numéro de téléphone, vous êtes automatiquement redirigé vers un serveur vocal

interactif. Il est demandé à l'utilisateur de fournir des informations personnelles (mot de passe) ou bancaires (numéro de carte bancaire).
Ne cliquez jamais sur les liens contenus dans ces messages et ne rappelez jamais ces numéros.

Vishing

Vishing est la contraction de Voice et de Phishing. On l'appelle également Hameçonnage par téléphone.
On parle de Vishing lorsqu'un fraudeur utilise un serveur vocal interactif pour appeler des utilisateurs dans le but de leur dérober des informations personnelles. L'intention est la même que lors d'un phishing par email ou d'un phishing par SMS. L'appel est souvent à caractère urgent et demande à l'utilisateur d'agir rapidement. Ne fournissez jamais aucune information lors de la réception de pareils appels. Gardez également à l'esprit qu'il est facile pour une personne malveillante d'usurper un numéro appelant et ainsi de se faire passer pour quelqu'un d'autre.
Si vous n'êtes pas en mesure d'authentifier l'origine de l'appel, ne fournissez jamais aucune information personnelle ou bancaire.

Lien : https://aide.homelidays.com/articles/Que-sont-le-Smishing-et-le-Vishing

Gare au vishing, la nouvelle arnaque par téléphone

Compte tenu de la méfiance des internautes face au hameçonnage - dit "phishing" - de leurs données personnelles sur internet, les escrocs utilisent désormais le "vishing", une arnaque qui consiste à passer un coup de téléphone en se faisant passer notamment pour un employé de la banque de la future victime afin de lui demander ses données personnelles.
La palette des escrocs se cachant derrière une machine ne cesse de s'étendre. Après le phishing (faux emails) et les ping calls (arnaque à l'appel en absence), voici le "vishing" (en anglais, vishing : combinaison de voice et phishing). Il s'agit d'une technique de hameçonnage qui consiste à obtenir frauduleusement, via un appel téléphonique, des informations personnelles : mots de passe, numéros de comptes bancaires, codes etc.
Le procédé est toujours le même : sous prétexte d'un problème lié à son compte bancaire (opérations inhabituelles par exemple) ou au règlement d'une facture, la victime est invitée, lors d'un appel par un serveur vocal, à composer rapidement un numéro de téléphone. Une fois en ligne, elle est mise en relation avec un système automatisé - ou avec une personne qui se fait passer pour un employé de sa banque - lui demandant de fournir ses identifiants bancaires, son numéro de carte bancaire ou son numéro de compte, ainsi que d'autres informations personnelles (cryptogramme, dates de validité de la CB). Ces données seront ensuite utilisées par le fraudeur pour accéder à son compte bancaire ou faire des achats sur internet.
Mot d'ordre : ne pas rappeler !
"Dans tous les cas, il est impératif de ne jamais donner d'informations bancaires, personnelles ou tout autre renseignement par téléphone", rappelle la Police nationale.
Pour se protéger du "vishing", les particuliers doivent se méfier des messages vocaux du type "Nous suspectons une transaction non autorisée sur votre compte, rappelez le numéro....". En présence d'un tel message, il est préférable d'appeler immédiatement sa banque pour prévenir de la situation, et ce même en cas de doute.

Ceux qui auraient été victimes de ce type d'escroquerie peuvent déposer une plainte au commissariat ou à la gendarmerie la plus proche. 13/09/16

Lien : **http://www.leparticulier.fr/jcms/p1_1613915/gare-au-vishing-la-nouvelle-arnaque-par-telephone**

Cette nouvelle arnaque téléphonique risque de faire de nombreuses victimes...

Les internautes le savent désormais : le phishing est courant. Ça ne les empêche pas de régulièrement tomber dans le panneau et de donner à des pirates leurs données personnelles. Mais maintenant, c'est dans la vie réelle que ça se passe, et par téléphone. Le principe est le même, le nombre de victimes risque d'exploser.

Le vishing : un appel pour vous voler vos données bancaires

Le nom de cette nouvelle arnaque est tout un programme : vishing, pour "voice phishing". Comme le phishing, l'idée est de se faire passer pour un organisme, typiquement votre banque, pour vous demander des données personnelles, notamment bancaires. Sauf que cette fois, c'est par téléphone que les malfrats frappent. De quoi inquiéter les autorités, car on a plus tendance à faire confiance à une personne réelle qu'à un simple mail.

Les escrocs vous appellent et une voix enregistrée vous prévient que votre banque soupçonne une utilisation frauduleuse de votre compte bancaire. La voix vous demande d'appeler immédiatement un numéro, ce que vous faites car vous paniquez. Là, une personne réelle, ou bien une autre voix enregistrée, vous demande des données personnelles, soi-disant pour vérifier votre identité et vos transactions.

En fait, avec ces données, les pirates vont tout simplement se faire plaisir et accéder à vos comptes ou acheter sur Internet.

Ne jamais donner vos données personnelles par téléphone et ne pas rappeler

À moins que vous ne soyez certain à 100 % de votre interlocuteur, le mot d'ordre est le même : gardez vos données personnelles pour vous. Une banque, surtout, ne vous demandera pas votre numéro de carte ou votre cryptogramme, car... elle n'en a pas besoin pour vérifier vos comptes !

Surtout, rappelez-vous qu'en cas d'utilisation frauduleuse de votre carte bancaire (avant ou après cette arnaque, si vous en avez été victime), votre banque est tenue de vous rembourser l'intégralité des sommes.

Si vous avez reçu ce type d'appel, prévenez votre banque, qu'elle puisse prévenir ses clients. Et si vous êtes tombé dans le panneau, portez plainte ! 14/09/2016

Lien : **http://news.radins.com/actualites/attention-a-cette-nouvelle-arnaque-telephonique-qui-va-faire-nombreuses-victimes,27756.html**

Appels frauduleux en masse, attention au "vishing" !

En pleine période de paiement de l'impôt sur le revenu, de nombreux Français ont été victimes d'une arnaque téléphonique visant à récupérer leurs données bancaires. Explications.

Cette arnaque qui avait fait de nombreuses victimes outre-Manche il y a quelques mois sévit désormais en France. Le "vishing" (hameçonnage par téléphone), qui

consiste notamment à voler les données bancaires, se développe en effet fortement dans l'Hexagone, en particulier depuis plusieurs semaines avec le paiement de l'impôt sur le revenu.
Selon le journal Nord Littoral, il y a quelques jours, "un certain nombre d'habitants du Pas-de-Calais se sont plaints d'avoir reçu des appels téléphoniques frauduleux de la part des impôts". Concrètement, des malfaiteurs profitent du calendrier fiscal pour appeler leurs victimes en se faisant passer pour l'organisme et en demandant leurs données bancaires. Dans le but évidemment de les utiliser à des fins malveillantes.

Signalez la tentative d'escroquerie

Cette escroquerie ressemble fortement à celle du "phishing", une arnaque que de nombreux internautes ont déjà reçue au moins une fois dans leur boite mail. Celle-ci consiste pour les escrocs à envoyer un courrier électronique dans lequel ils se font passer pour une banque, un site de commerce ou encore un particulier afin de demander un service ou prétexter un problème de paiement et ainsi récupérer les données bancaires de leurs victimes.
Il est évidemment important de rappeler que l'administration fiscale ne demande jamais de tels renseignements par téléphone. Dans le cas où vous seriez victime d'une tentative d'escroquerie, vous pouvez la signaler sur le site internet-signalement.gouv.fr ou en composant le numéro (gratuit) 0 805 805 817.

Lien : **http://www.planet.fr/actualites-appels-frauduleux-en-masse-attention-au-vishing.1176521.1557.html**

Le «smishing» une nouvelle vague d'arnaques par SMS

En France, les stratagèmes d'escroquerie par téléphone ne changent pas beaucoup, mais les arnaqueurs réussissent toujours à trouver des victimes. Pour cela, aujourd'hui on ira présenter un type d'escroquerie qui n'a pas, pour l'instant, été mentionnée sur Tellows mais qui fleurie de nouveau – en France, mais aussi dans d'autres pays comme la Suède. C'est le smishing. Le mot « smishing » se compose du mot SMS et du mot « phishing » respectivement « vishing » que veut dire hameçonnage par téléphone. Le but de toutes ces variantes d'arnaques est le même : obtenir et abuser des informations sensibles telles que vos dates bancaires.
Lors du « pishing » la victime reçoit un courriel que, apparemment, provient de votre banque, compagnie d'électricité ou du Trésor publique et ainsi de suite. De plus, le mail contient un lien qui mène à un site qui ressemble, par exemple, au site de votre banque. Comme vous ne voyez pas de différences (sauf dans l'url !) vous y entrez vos coordonnées et l'arnaqueur a beau jeu.
Le « vishing » diffère du « pishing » par le fait que l'internaute, après réception du courriel, n'est pas invité à cliquer sur le lien et à entrer ses dates, mais il est tenu de rappeler un certain numéro qui lui est indiqué dans le courriel.
Maintenant alors le « smishing » : Cette méthode d'arnaque ne se sert plus du courriel, mais consiste en envoyer un SMS à la victime indiquant un numéro à rappeler et puis la victime doit entrer un code ou un mot-clé que lui est communiqué par ce texto. Les numéros à partir desquels ces SMS sont envoyés sont, dans las plupart des cas, générés par un ordinateur et ne sont pas attribués à un particulier ou une société. Les numéros indiqués pour le rappel sont avec peu d'exceptions des numéros surtaxés.

Dans une autre entrée dans notre blog nous avons déjà décrit un des cas connus d'arnaque par SMS :
Attention! Nouvelle méthode d'arnaque téléphonique découverte
Le procédé du « smishing », que certains parmi vous ont vécu et dont ils ont témoigné, pourrait également être le suivant :
Le cible reçoit un SMS. Le message reçu semble provenir d'un ami ou bien d'une personne que l'on connaît plus ou moins bien car le langage est d'une certaine façon personnalisé pour que la victime soit rassurée et rappelle un des numéros indiqués. Or, ces numéros sont des numéros surtaxés et la communauté leur a attribué un Score de 9. 0899465500 et 0899464400 sont des numéros dont il est question dans les témoignages.
Si le destinataire du texto rappelle ce numéro l'arnaqueur obtiendra ce qu'il voulait. Alors : Supprimez le texto si vous en recevez et n'appelez surtout pas. Ainsi vous ne courrez pas le risque de vous faire avoir.
Lien : **https://blog.tellows.fr/2012/12/le-%C2%ABsmishing%C2%BB-une-nouvelle-vague-darnaques-par-sms/**

Les pirates du web, rois du phishing ?
Qu'est-ce que le phishing ?

Le phishing est défini comme une méthode utilisée par les cyber-pirates pour obtenir des renseignements personnels dans le but d'extorquer des fonds aux victimes. Les renseignements peuvent concerner un mot de passe, un numéro de carte de crédit ou encore une date de naissance. Cette technique d'ingénierie sociale consiste à exploiter la faille humaine et non une faille informatique. Le phishing fonctionne grâce au risque de confusion sur l'émetteur du courriel ou sur l'url communiqué par la personne ciblée. C'est une arme massive pour les pirates du web qui envoient leur mail à énormément d'individus dans le but qu'une poignée d'entre eux mordent à l'hameçon. Le principe même du phishing repose sur l'adresse email de l'émetteur du courrier. Pour troubler le destinataire, l'émetteur utilisera les adresses classiques telles que gmail ou yahoo. Mais avec l'arrivée de la nouvelle extension de nom de domaine en .email, il pourra effectuer des dépôts de noms de domaines basés sur des similitudes orthographiques entre l'entreprise et l'usurpateur. Et c'est sur ce point que beaucoup se posent des questions sur cette nouvelle extension dont nous ne manquerons pas de suivre les évolutions.

Phishing et autres arnaques

Une étude de Ponémon en 2012 a montré qu'une attaque phishing coûte en moyenne 241 000$ à l'entreprise qui en est victime. 5 techniques de phishing ont actuellement été identifiées : la confirmation de données, le « tirage au sort », le changement de site, le harponnage sentimental et la menace. De nouvelles méthodes basées sur le phishing ont vu le jour ces dernières années. Tout d'abord, le spear phishing (ou harponnage) qui est une variante du phishing classique. Dans ce cas, l'attaque est ciblée sur une personne ou un groupe ciblé d'utilisateur. L'email contient des informations très précises et personnelles sur l'individu pour endormir sa vigilance. Cette nouvelle méthode semble cibler particulièrement les entreprises pour leur soutirer des informations sensibles. Que ce soit du point de vue de la propriété intellectuelle, pour des informations à forte valeur ajoutée ou encore espionner la concurrence, le spear phishing jouera sur la corde sensible de l'humain. Lorsque l'attaquant insère un code dans une page qui aura pour fonction d'ouvrir un pop-up

pendant votre navigation, on appelle cela du in-session phishing. Deux dernières méthodes commencent à se répandre, le smishing (phishing par sms) et le vishing (phishing vocal).

Bien se protéger du phishing

Il existe des techniques préventives permettant de protéger ses données d'une attaque phishing. Il faut minimiser au mieux le risque de faille humaine. Cela passe par des campagnes de communication internet et de la formation, principalement pour les personnes manipulant des données sensibles. Ensuite, il ne faut jamais cliquer directement sur un lien contenu dans un mail mais le saisir manuellement l'url. Il est également nécessaire de se méfier des formulaires demandant des informations secrètes telles que des informations bancaires. Sachez qu'une banque ne vous demandera jamais de communiquer votre numéro de compte et/ou votre mot de passe par mail ou par téléphone. Dans le doute, n'hésitez pas à contacter votre agence. Pour finir, avant de saisir des informations sensibles, assurez-vous que votre navigateur est en mode sécurité (url en https et présence d'un petit cadenas). Enfin, munissez-vous d'une solution email efficace contre le spam et le phishing telle que MailSecurity+ pour votre boîte email, renseignez-vous auprès de Nom-domaine.fr.

Lien : http://blog.nom-domaine.fr/les-pirates-du-web-rois-du-phishing.html

Cybercrime : Le vishing (hameçonnage vocal), Gare aux appels frauduleux !

Le hameçonnage par téléphone (en anglais, *vishing*: combinaison de *voice* et *phishing*) est une technique utilisée par des escrocs via un appel téléphonique pour obtenir frauduleusement vos informations personnelles: mots de passe, numéros de comptes bancaires, codes etc.

Comment reconnaître une tentative de vishing ?

Deux types d'appels sont possibles. Les victimes sont contactées par téléphone soit par un automate soit par une personne physique.

L'appel d'un automate (enregistrement sonore)

Un problème quelconque de compte bancaire peut être évoquer lors de cet appel par un serveur vocal. La victime est alors invitée à composer rapidement un numéro de téléphone.

Lorsque ce numéro est appelé, elle est mise en relation avec un système automatisé lui demandant de fournir ses identifiants bancaires, son numéro de carte bancaire ou son numéro de compte, ainsi que d'autres informations personnelles (cryptogramme, dates de validité de la CB).

Un problème lié à son compte bancaire (opérations inhabituelles par exemple) ou au règlement d'une facture peut aussi être évoqué lors de l'appel.

Ces informations seront ensuite utilisées par le fraudeur pour accéder à son compte bancaire, faire des achats sur Internet.

Attention, dans certains cas, le premier appel de l'automate sera relayé par une personne physique.

L'appel d'une personne physique

Une personne appelle la potentielle victime et se fait passer pour un employé d'un département de sécurité bancaire ou un employé de sa propre banque.

Elle lui signale un problème sur son compte ou avec sa carte de crédit, une éventuelle utilisation frauduleuse pour des achats sur internet par exemple.
Le fraudeur demande ensuite de lui communiquer les informations de sa carte bancaire afin de vérifier qu'elle est toujours en sa possession.
Ce scénario peut prendre plusieurs variantes.

Les bons réflexes

Dans tous les cas, il est impératif de ne jamais donner d'informations bancaires, personnelles ou tout autre renseignement par téléphone.
Les établissements bancaires ne vous demanderont jamais d'informations par téléphone ou par courrier électronique.
Se méfier des messages vocaux de type « Nous suspectons une transaction non autorisée sur votre compte, rappelez le numéro....»
Les fraudeurs utilisent le stress et la peur pour obtenir les informations personnelles des victimes en leur faisant croire qu'elles ont fait l'objet d'une escroquerie.
Si un message vous demande de rappeler un numéro, ne le composez pas.
Appelez immédiatement votre banque pour prévenir de la situation, même en cas de doute.

Que faire si j'ai déjà donné mes informations ?

Contactez le plus rapidement possible votre banque pour les informer de votre situation.
Allez déposer une plainte au commissariat ou à la gendarmerie la plus proche.

Lien : http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/Le-vishing-hameconnage-vocal-gare-aux-appels-frauduleux

Le "vishing", La nouvelle escroquerie par téléphone qui peut coûter cher

Environ 30 millions d'euros (24 millions de livres) ont été escroqués au Royaume-Uni en 2014 par le "vishing", selon le quotidien britannique The Guardian. Une nouvelle méthode qui consiste à voler les données bancaires par téléphone.
Il y avait le "phishing", il faudra désormais également faire attention au "vishing". Cette nouvelle escroquerie, qui consiste à passer un coup de téléphone en se faisant passer pour un employé de la banque de la future victime afin de lui demander ses données personnelles, fait des ravages au Royaume-Uni, selon le *Guardian*. Une arnaque qui ne s'arrête pas là puisque les malfaiteurs demandent également de transmettre l'argent sur un autre compte. 24 millions de livres (environ 30 millions d'euros) ont ainsi déjà été escroqués cette année outre-Manche.
Cette nouvelle escroquerie ressemble fortement à celle du "phishing", une arnaque que de nombreux internautes ont déjà reçue au moins une fois dans leur boite mail. Celle-ci consiste en effet pour les escrocs à envoyer un courrier électronique dans lequel ils se font passer pour une banque, un site de commerce ou encore un particulier afin de demander un service ou prétexter un problème de paiement et ainsi récupérer les données bancaires de leurs victimes.

Plus efficace sur les personnes âgées

"La montée de l'hameçonnage vocal peut être due en partie à la baisse de l'escroquerie de type 'phishing' (…) Cela parce que l'hameçonnage vocal est plus efficace sur une cible démographique précise - les personnes âgées - ou encore parce que les

escroqueries par 'phishing' autrement convaincants sont toujours compromises par la grammaire pauvre de leurs expéditeurs", explique le journaliste du *Guardian*.
Pour faire face au problème, l'organisme en charge de la prévention des fraudes sur les moyens de paiement (Financial Fraud Action UK), a lancé une campagne d'avertissement, précise *L'Express*.
Lien : **http://www.planet.fr/conso-le-vishing-la-nouvelle-escroquerie-par-telephone-qui-peut-couter-cher.745156.1404.html**

Vishing :
La nouvelle escroquerie par téléphone

le **Phishing**, pour rappel, c'est **l'**extorsion de vos coordonnées bancaires et/ou mots de passe par l'entremise d'emails**.**
Le **Vishing** (contraction *de voice* + *phishing*), c'est la même chose, mais par téléphone **!**
Cette méthode existe en fait depuis 2008, mais c'est vraiment depuis cette année qu'elle se développe, pour l'instant surtout en dehors de l'hexagone, mais les frenchy sont en train de succomber **!**
La raison principale de ce développement soudain étant que le Phishing rapportant de moins en moins**,** les internautes étant (enfin !) de moins en moins crédules, ces personnes mal intentionnées n'ont pas d'autre choix que de changer de tactique.
Bon, je ne vous le cache pas, je trépignais en écrivant cet article, et pour ceux qui ne me connaissent pas, je peux vous dire que c'est un spectacle.
Ben oui, je trouve déjà exaspérant que comme je le dis souvent, les consommateurs sont de plus en plus prudents, limites paranoïaques, mais totalement incohérents dans leurs actes dans certaines circonstances.
En effet, pour donner un exemple, dans la rue ils cachent la saisie de leur code secret aux Distributeurs automatiques, redoublent de vigilance aux caisses des supermarchés, mais, arrivés chez eux devant leur ordinateur cliquent sur n'importe quel mail ou lien et donnent volontiers leurs coordonnées bancaires aux premiers venus !!!
Alors le Vishing**,** c'est encore plus énorme, un inconnu se faisant passer pour une institution officielle, souvent une banque, vous appelle et vous demande de confirmer vos coordonnées bancaires et beaucoup les donnent !!!
Donc, si je tape à votre porte demain matin, vous me donnerez spontanément le numéro de votre carte ?
Soyons cohérents, à moins que vous ayez gagné au Loto ou que vous ayez un découvert problématique, un banquier ne vous appellera jamais personnellement.
Il y a une deuxième variante à ne pas négliger encore plus sournoise : l'automate téléphonique.
La machine compose de manière aléatoire des numéros.
En décrochant, la personne entend un message préenregistré.
Ce message, censé provenir de sa Banque, l'informe par exemple que des opérations inhabituelles avaient été détectées sur son Compte Bancaire.
La victime potentielle est ensuite invitée à composer un numéro de téléphone (très souvent surtaxé) pour soit-disant contrôler son compte bancaire.
Elle aboutit sur une boîte vocale qui lui demande de saisir tous les numéros de sa carte bancaire ainsi que sa date de validité et parfois même le cryptogramme !

Les fraudeurs utilisent le stress et la panique pour parvenir à leurs fins, en provoque un faux sentiment d'urgence.
Beaucoup ne réalisent pas sur le moment qu'ils sont en train de divulguer des informations confidentielles et facilement réutilisables.
Comme je le disais plus haut : gardez à l'esprit que les banques ne demandent pas de transmettre par mail ou par téléphone des informations aussi précieuses !
Pour info, environ 30 millions d'euros ont déjà été escroqués au Royaume-Uni cette année avec cette méthode, elle est donc très efficace.
Et surtout, ne vous dites pas que cela ne pourrait pas vous arriver, les méthodologies d'approche sont de plus en plus sophistiquées et élaborées !
Alors restez vigilants, la meilleure arme contre ces agressions c'est le bon sens.
La meilleure façon de l'éradiquer c'est d'en parler avec son entourage, faites circuler l'info !
Vous voilà prévenus !
Lien : http://sospc.name/vishing-la-nouvelle-escroquerie-par-telephone/

Attention aux arnaques aux faux colis par SMS

De plus en plus de particuliers reçoivent sur leurs téléphones portables ou leurs smartphones de faux avis de passages de colis avec un numéro surtaxé à rappeler. Des conseils pour réagir face à ce fléau.
Lorsqu'un téléphone sonne plusieurs fois sans que le destinataire n'ait réussi à décrocher, il retrouve parfois un message vocal ou SMS lui indiquant qu'un colis est à sa disposition dans un point relais. On lui propose alors de téléphoner à un numéro commençant par 0899 pour récupérer son bien.
Bien que le réflexe de certains soit souvent de rappeler aussitôt, mieux vaut ne pas céder à la tentation, surtout si la personne n'a rien commandé depuis quelques temps. Car, en réalité, non seulement le colis n'existe pas mais encore pire le numéro à rappeler est surtaxé !
Si le préjudice individuel n'est souvent que quelques euros, le Réseau anti-arnaques ainsi que la DGCCRF (Répression des fraudes) recommandent de ne pas donner suite à ces messages et, lorsqu'il s'agit d'un SMS, préconisent de les faire suivre au 33700. Ce numéro correspond à la plate-forme de signalement de SMS abusifs.
Lien : http://www.leparticulier.fr/jcms/p1_1531639/attention-aux-arnaques-aux-faux-colis-par-sms

Protégez-vous des ping calls, ces arnaques à l'appel en absence !

Les « ping call », une technique d'escroquerie consistant à pousser un abonné téléphonique à rappeler un numéro surtaxé, reviennent sur le devant de la scène, ces derniers mois. Face à leur recrudescence, les autorités appellent à la vigilance. Des conseils pour éviter ce type d'arnaque au portable
Qui n'a jamais été tenté de rappeler le numéro de téléphone affiché sur son portable, lorsqu'il n'a pas eu le temps de décrocher ? Attention, il s'agit parfois d'un ping call, une technique de "spam vocal" qui consiste à appeler un numéro de téléphone en ne laissant sonner qu'une seule fois. Naïvement, le destinataire, n'ayant pas eu le temps

de prendre l'appel, rappelle le numéro qui évidemment est surtaxé. Il tombe alors sur un opérateur qui lui annonce qu'il a gagné un bon d'achat ou un cadeau. Si les call ping existent depuis plusieurs années, les escrocs ont amélioré leur technique au point que ces arnaques par téléphone se développent à grande vitesse ces derniers mois. "Pour ne pas susciter la méfiance de leurs victimes, les usurpateurs passent désormais leurs appels depuis des numéros en 01, 02, 04 etc... plutôt que des 0 899", souligne le ministère de l'Intérieur.

Pour lui faire passer un maximum de temps au téléphone, le client doit patienter sur une musique d'attente facturée à prix d'or, avant d'être mis "soi-disant" en contact avec le bon service.

Mieux vaut ne pas rappeler

Numéro inconnu, aucun message sur le répondeur... Face à ces indices, mieux vaut ne pas rappeler, même si le numéro semble "normal ".

Pour lutter contre ces spams vocaux, les consommateurs victimes peuvent envoyer gratuitement un SMS au 33 700 avec le texte « Spam vocal 01 XX XX XX XX » en précisant le numéro de téléphone suspect. Son signalement sera transmis aux opérateurs.

Lien : http://www.leparticulier.fr/jcms/p1_1595290/protegez-vous-des-ping-calls-ces-arnaques-a-l-appel-en-absence

Ping calls : 2 sociétés condamnées pour fraude aux numéros surtaxés

Après enquête de la Répression des fraudes, deux sociétés et leur gérant viennent d'être condamnés à de lourdes amendes pour avoir émis des "ping calls". Cette escroquerie consiste à émettre des appels en absence pour pousser à rappeler un numéro surtaxé. Bercy appelle les particuliers à la plus grande vigilance.

Deux sociétés, 123soleil.com et holding123mediacorp, viennent d'être condamnées pour avoir utilisé la technique frauduleuse des "ping calls". Chaque mois, les escrocs émettaient des appels en absence auprès de millions de numéros de téléphone en ne laissant sonner qu'une seule fois. Naïvement, les destinataires, n'ayant pas eu le temps de prendre l'appel, rappelaient le numéro affiché à l'écran - 3247, 3287, 3684, 3687 et 3261 - qui évidemment était surtaxé, à leur insu.

Le piège se refermait ensuite sur les appelants qui, sous un prétexte fallacieux (gain d'un cadeau, faux impayé...), étaient incités à passer un maximum de temps en ligne, avant d'être "soi-disant" mis en contact avec le bon service. Le tout sur une musique d'attente facturée à prix d'or ! La totalité des frais liés à ces communications frauduleuses était ensuite encaissée par les escrocs.

Après l'enquête menée entre 2013 et 2015 par les agents de la DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes), les deux sociétés ont été condamnées à des amendes respectivement de 300 000 et de 500 000 €. Leur gérant a, quant à lui, été sanctionné par une peine de deux ans de prison avec sursis et une amende de 250 000 €.

Vérifier le numéro avant d'appeler

Tout en félicitant l'efficacité des contrôles menés par la DGCCRF, Martine Pinville, secrétaire d'État chargé de la consommation, appelle les utilisateurs à faire preuve de vigilance face aux sollicitations reçues par téléphone émanant de numéros inconnus, et à recourir aux dispositifs publics existants. Ils sont notamment invités à consulter

l'annuaire inversé des numéros SVA (Services à valeur ajoutée). Cet outil permet ainsi de vérifier si un numéro surtaxé est utilisé frauduleusement en identifiant à partir du numéro, le professionnel et le tarif de ses appels.
Pour lutter contre ces spams vocaux, les consommateurs victimes peuvent envoyer gratuitement un SMS au 33 700 en précisant le numéro de téléphone suspect. Son signalement sera transmis aux opérateurs. 03/08/16
Lien : **http://www.leparticulier.fr/jcms/p1_1611848/ping-calls-2-societes-condamnees-pour-fraude-aux-numeros-surtaxes**

Le Tabnabbing, une attaque par Phishing évoluée

Le **Tabnabbing** est une attaque par phishing qui profite de votre utilisation insouciante des onglets pour vous pirater.
C'est une technique qui n'est pas récente (elle date de 2010) mais qui a presque été oubliée. Oubliée seulement de notre côté, mais pas tout à fait du côté des pirates… Voici donc la définition de cette attaque, et comment s'en protéger efficacement.
Le nom « tabnabbing » a été donné par le chercheur et designer pour Firefox Aza Raskin qui l'a mise au point et expliquée afin d'alerter les internautes.
Qu'est-ce que le « tabnabbing » ?
Un site pirate utilise un bout de code permettant de détecter le changement d'onglet.
Lorsque vous le visitez, vous voyez du contenu normal probablement lié à ce que vous cherchiez.
Seulement, au bout de quelques secondes après avoir changé d'onglet, le site pirate change subitement son titre et sa « favicon » (l'icône du site web qui apparaît dans chaque onglet).
Lorsque la victime retourne sur l'onglet, elle pense dans l'exemple précédent revenir sur son onglet Gmail précédemment ouvert. Ce même onglet qui contient une copie frauduleuse de Gmail et qui piratera la victime si elle ne fait pas attention. Si vous êtes comme moi avec 40 onglets ouverts en permanence, vous êtes d'autant plus ciblé(e) par cette attaque**.**
Comment s'en prémunir ?
C'est le type d'attaque plutôt bête mais très rusée qui nous attrape facilement si l'on ne fait pas attention. La prudence est de mise, l'idéal est de bien vérifier l'URL des onglets (à défaut de se souvenir des onglets ouverts).
Notons que cette attaque pourrait prendre des tournures différentes en se faisant passer pour d'autres sites qu'on a l'habitude d'utiliser.
Bien entendu les meilleures défenses contre les attaques par Phishing sont la vigilance et la sensibilisation**.** Si on ne sait pas que ça existe ou ne fait pas attention, et on est toujours perdant.
Lien : **http://www.leblogduhacker.fr/le-tabnabbing-une-attaque-par-phishing-evoluee/**

Tabnabbing : comment le reconnaitre et se protéger ?

Le Tabnabbing (ou TabJacking) est une nouvelle forme de piratage de type "phishing" particulièrement sournoise qui utilise la navigation par onglet pour tromper les internautes et dérober leurs identifiants de comptes et autres informations sensibles.

Lorsque plusieurs onglets sont ouverts simultanément, une page piégée laissée ouverte en arrière plan déclenche son rechargement ou sa redirection pour afficher une page imitant un site populaire ou habituellement utilisée par l'utilisateur. Cela peut être une page de connexion à un organisme bancaire ou de paiement, un site de réseau social (twitter, facebook...), un compte email (Hotmail, Yahoo, Gmail...) etc... L'utilisateur croit ensuite se connecter à son site habituel mais livre ses identifiants et mots de passe à un site piégé.

Démonstration

Pour que cela paraisse bien clair, prenons un exemple concret. Il s'agit d'une tentative de piratage de compte Facebook mais le fonctionnement resterait le même pour tout site de banque, réseau social, email etc...

Durant la navigation, lors d'un clic sur un lien depuis n'importe quelle page web, l'internaute consulte une page d'apparence classique traitant d'un sujet quelconque :

L'internaute visite ensuite un autre onglet et laisse le précédent ouvert. La page laissée ouverte en arrière plan se recharge, ce qui est le comportement normal de certaines pages web, l'internaute n'y prête pas attention.

La page en arrière plan a changé son apparence pour afficher une icône de favori (favicon) immitant un site populaire. D'un coup d'oeil, l'internaute croit reconnaitre l'emplacement de sa page web habituelle.

L'internaute clique sur l'onglet et s'aperçoit qu'il doit se connecter à son compte puis rentre machinalement ses identifiants sur la page piégée sans prêter attention à l'url de la barre d'adresse.

Le pirate n'a plus qu'a récupérer ses identifiants de compte ou de carte bancaire pour les utiliser.

Comment se protéger du Tabnabbing ?

Tout comme pour le phishing, le meilleur moyen de ne pas devenir victime de tabnabbing est de vérifier systématiquement que l'url de la barre d'adresse correspond bien au site sur lequel on veut se connecter ou sur lequel on veut saisir des informations sensibles (numéro de comptes et de cartes bancaires etc...).

D'autres astuces et outils peuvent aider à se protéger, du moins contraignant au plus contraignant :

- Utiliser des barres d'outils ou des logiciels de sécurité permettant d'évaluer les sites (WOT, SiteAdvisor...)
- Prendre le réflexe de fermer systématiquement les onglets des sites que l'on connait peu.
- Désactiver Javascript
- Utiliser deux fenêtre de navigateurs, chacune avec plusieurs onglets. Une sera reservée à vos sites favoris.
- Revenir à une navigation sans onglet et configurer son navigateur pour ouvrir les liens dans une seule et même fenêtre

Lien : **http://forums.cnetfrance.fr/topic/171356-tabnabbing--comment-le-reconnaitre-et-se-proteger/**