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 ع إ م

LETTRE D'INFORMATION : BON A SAVOIR (N°31)

Arnaques sur Internet

Nous allons tenter de cerner le phénomène de la «fraude commise à l'aide de l'informatique», communément appelée «fraude sur Internet». Tout le monde en a entendu parler, que ce soit par le biais de connaissances, des médias, de collègues, etc. Certains d'entre vous en ont peut-être déjà été victimes, etc. Ce phénomène toujours très en vogue, profitant de la crédulité de ses victimes et de l'ingéniosité de certains stratagèmes mis en place par les escrocs, a encore de beaux jours devant lui, etc. Internet offre en effet la possibilité d'atteindre un grand nombre de victimes potentielles, rapidement et à très faible coût.

Arnaques dans les enchères ou ventes en lignes "Auction Fraud"

Les sites de ventes ou d'enchères par Internet sont de plus en plus prisés par le grand public. A tel point que de plus en plus de sociétés vendent également leurs marchandises par ce biais. C'est ce que l'on appelle l'e-commerce.

Revers de la médaille, les escrocs de tout poil y sévissent aussi. Soit ils vendent des marchandises inexistantes, soit ils achètent de vraies marchandises mais sans les payer. Pour ce faire, ils utilisent diverses techniques telles que les faux sites de tiers de confiance, de faux sites de transport, le piratage de comptes existants, le paiement par faux chèques, le paiement par transfert d'argent (via Western Union ou Web Money par exemple), l'utilisation de faux noms, de fausses qualités, etc.

Les montants réclamés sont en général assez réduits au départ mais peuvent s'accumuler et atteindre des sommes considérables (plusieurs dizaines de milliers d'euros). De plus, pris globalement, les réseaux organisés peuvent ainsi brasser des centaines de milliers d'euros, voire plusieurs millions pour les plus gros !

Arnaque à la vente

Le vendeur est malhonnête, il ne livre pas ce qui a été payé. Certains vendeurs réussissent à se fabriquer des profils très positifs grâce à des réseaux, ou en ouvrant des comptes différents avec des adresses IP différentes. Ils fabriquent de fausses boutiques attrayantes et de faux sites Internet.

Le vendeur vend des biens volés ou des contrefaçons: en moyenne près de 50% des produits neufs trouvés à prix concurrentiels sur les sites de ventes sont des contrefaçons ou des objets volés.

Le vendeur est malhonnête, il cherche à se procurer des coordonnées bancaires pour mieux pouvoir piller le compte de l'acheteur en effectuant des transactions de quelques dizaines d'euros.

Comment les détecter ? Une demande de paiement par virement bancaire pour des petits objets ou des objets onéreux ou rares, demande de paiement par chèque (qui contient toutes les coordonnées bancaires et la signature qui peut être scannée).

Le vendeur est malhonnête et cherche à réaliser une vente frauduleuse sur des objets qui n'existent pas ou ne lui appartiennent pas. Ces pratiques touchent l'immobilier (la

mine d'or au Brésil) ou des automobiles, mais aussi téléphones, ordinateurs, montres, chaussures, instruments, vêtements, vins, etc.
Le vendeur ne livre qu'une partie de l'objet commandé.
Cas typique : l'ordinateur sans système d'exploitation (Windows ou Vista).
Généralement, il s'empresse de le proposer à prix très compétitif. Si l'acheteur accepte, il reçoit une copie piratée.
Usurpation de noms et qualité du vendeur. Le vendeur usurpe le profil d'un vendeur disposant d'une bonne notation. Souvent, les données d'identité ont été dérobées par l'accès illicite aux données mail du vendeur.

Arnaque à l'achat ou au paiement

Utilisation de faux sites de paiement, de faux certificats de paiement, de faux avis de transferts d'argent.
Utilisation de moyens de paiement frauduleux: fausse carte de crédit, faux compte de tiers de confiance, compte tiers de confiance piraté, faux certificats de paiement (ou lettres de crédit ou chèques de banques très fréquemment), fausse monnaie (c'est plus fréquent qu'on ne croit), faux chèque.
Le paiement est complexe et doit passer par plusieurs intermédiaires.

Arnaques à la carte bancaire

La carte de paiement (VISA, Amex, Eurocard, etc.) est devenue un moyen de paiement très courant. C'est d'ailleurs le mode de paiement le plus utilisé pour les transactions en ligne sur Internet.
Mais ce système de paiement a ses failles : sa simplicité peut se retourner contre le titulaire d'une carte. En effet, sur de très nombreux sites de ventes en ligne, il suffit de taper son numéro de carte de crédit avec son nom et son prénom ainsi que la date d'expiration de la carte pour régler ses achats.
Comme à ce jour, de nombreux sites marchands ne sont pas sécurisés (par l'utilisation du protocole sécurisé « https » par exemple), les données transmises entre l'acheteur et le vendeur circulent en clair sur le Net et peuvent aisément être « sniffées » (lues) par des personnes mal intentionnées ! Les escrocs ont vite compris tout le potentiel que représentait ce moyen de paiement. C'est facile et la victime ne se rend compte de l'escroquerie qu'au moment où elle reçoit son relevé de compte !

Les chèques contrefaits

L'auteur envoie à sa victime un chèque en bois, volé ou contrefait, généralement tiré d'une grande banque étrangère. Le «bénéficiaire » dépose la formule à sa banque mais la vérification de la solvabilité de l'émetteur prend un certain temps (de l'ordre de plusieurs jours), temps qui est mis à profit par l'auteur pour demander l'envoi rapide de la marchandise «achetée». Cette technique est également appelée «Counterfeit cashier's check» (US).
Variante : L'auteur envoie un chèque d'un montant supérieur au montant demandé par la victime et lui demande le remboursement de la différence. Le préjudice peut ainsi être nettement plus important, à savoir la marchandise et l'argent ! Cette technique est principalement utilisée dans le cadre des ventes de véhicules par Internet.

Charité, dons, collectes de fonds - "Charity, donation, fundraising"

De nombreux escrocs ont bien compris que les grandes causes humanitaires parvenaient à rassembler d'énormes fonds. Partant du même principe, ils utilisent la technique du «spamming» pour tenter de convaincre les internautes de verser de l'argent pour une cause déterminée. Ils peuvent soit utiliser une cause réelle (tsunami, famine, etc.), soit en inventer une de toutes pièces.

Escroqueries dites « nigérianes»

Connue depuis les années 1980, cette arnaque a refait surface avec l'avènement d'Internet. Elle connaît de multiples variantes, est souvent rédigée en anglais mais des versions « locales » existent, notamment en français.
Voici son principe de fonctionnement : un soi-disant homme d'affaire, un orphelin ou une veuve sollicite votre aide pour transférer des millions de dollars bloqués dans son pays en raison des problèmes politiques qui y sévissent (cela dépend souvent de l'actualité internationale du moment).
L'escroc vous demande alors de lui prêter une certaine somme pour soit payer l'entreprise de gardiennage qui détient le coffre à millions, soit rémunérer le notaire local afin de pouvoir transférer cet argent sur votre compte, à charge pour vous de le transférer ensuite à son « légitime propriétaire» moyennant bien entendu une substantielle commission pour vos efforts (de l'ordre de 5 à 10% du montant total)…
Bien évidemment, tous ces transferts d'argent se font via des sociétés spécialisées dans les transferts d'argent en cash, comme par exemple «Western Union», «Web Money» ou «Moneygram».
Le ou les auteurs utilisent de faux documents (factures de gardiennage, passeports, etc.) et n'hésitent pas non plus à menacer leur victime lorsqu'elle arrête de payer.

Fausses loteries

Les internautes reçoivent par e-mail un avis qui leur indique qu'ils ont gagné le gros lot à une loterie ou un jeu de hasard. Cette loterie est toujours située à l'étranger. Sur la toile aussi, beaucoup de messages circulent dans des variantes les plus diverses mais il existe toujours un point commun : Pour recevoir son prix, le gagnant doit d'abord verser une certaine somme d'argent pour les frais engendrés (authentification, transfert bancaire, représentation par un avocat, gardiennage, etc.).
Le délai pour réclamer son lot est très court, de sorte que la victime n'a normalement pas le temps de venir chercher son gain et doit déléguer (via faux avocat).Les fausses loteries les plus répandues sont : fausse loterie espagnole du style « El Gordo », fraude à l'Euromillions.

Variantes:

Le « sweepstake » : un e-mail informe la victime qu'elle vient de gagner un magnifique séjour aux Seychelles ou un voyage de rêve aux Caraïbes. Pour toucher son prix, la victime devra payer uniquement les taxes… Évidemment, il s'agit d'un autre subterfuge pour soutirer quelques milliers d'euros dont la victime ne reverra jamais la couleur.

Les investissements « exotiques » : toujours par e-mail, les internautes reçoivent des messages avec des propositions alléchantes pour des projets exotiques (tourisme, pétrole, cuivre...). La présence de mots chocs du type « gains certains » promettant des bénéfices astronomiques en peu de temps, « poussent » les victimes à répondre et à rentrer dans l'engrenage des escrocs. Cette escroquerie est aussi connue dans les pays anglo-saxons sous la dénomination « Ponzi Scheme » du nom de Charles Ponzi, de Boston, instigateur de cette méthode.

Fausses rencontres ou "friendship fraud"

Via des e-mails ou des sites web spécialisés dans les rencontres, l'escroc demande à sa victime de l'aider à payer son voyage pour le rejoindre et ainsi pouvoir se rencontrer.
Les e-mails sont souvent très chargés émotionnellement (forts sentiments de l'un envers l'autre, amour grandissant, possibilité de vie commune…) afin de mieux appâter la victime. Bien entendu, la victime paye pour divers frais (passeport, cadeaux, billets de voyage, etc.) mais l'escroc ne vient jamais.
De nombreux cas sont recensés avec des filles des pays de l'Est, du Sud-est asiatique et de l'Afrique.

On peut certes trouver de vraies filles qui font cela pour gagner facilement de l'argent mais on rencontre aussi de véritables réseaux bien organisés où les filles ne sont présentes que pour les séances de webcam ! Le but étant d'obtenir un maximum d'argent venant d'un maximum de personnes, une même fille peut aussi avoir plusieurs « contacts » en même temps, chacun croyant être le seul en relation avec la fille.

Le keylogging : le piratage de clavier

Un enregistreur de frappe ou keylogger peut être assimilé à un matériel ou à un logiciel espion qui a la particularité d'enregistrer les touches frappées sur le clavier sous certaines conditions et de les transmettre via les réseaux ou via des ondes électromagnétiques. Par exemple, certains enregistreurs de frappe analysent les sites visités et enregistrent les codes secrets et mots de passe lors de la saisie. Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur.

Fausses réservations d'hôtels, de voyages, de locations de villas ...

L'escroc prend contact avec un hôtel, une agence de voyage ou un «tour operator » afin de passer une réservation généralement assez conséquente (grand luxe, nombre de personnes prévues élevé, séminaire, etc.). Ces contacts se passent par e-mails, par les sites web des victimes (réservations en ligne) ou par (e-) fax. Pour ce faire, l'escroc communique un numéro de carte de crédit. Ce numéro de carte peut avoir été subtilisé à l'insu de son titulaire, généré au moyen d'un programme informatique, ou tout simplement provenir d'une carte volée.

Quelques jours avant l'arrivée prévue, l'escroc signale qu'il désire annuler pour un motif quelconque. Il demande donc le remboursement rapide des frais engagés moins les frais d'annulation. La victime rembourse donc la différence à l'escroc via des sociétés telles que Western Union ou WebMoney avant que la banque ne signale que la carte utilisée n'était pas valable et ne réclame le montant crédité.

Ventes pyramidales

La vente pyramidale est une forme d'escroquerie dans laquelle le profit ne provient pas vraiment d'une activité de vente comme annoncé, mais surtout du recrutement de nouveaux membres. Dans la vente pyramidale, seuls les initiateurs du système en profitent en spoliant les membres de la base. Ce système se camoufle fréquemment derrière les termes de «marketing multiniveaux » ou «commercialisation à paliers multiples» (en anglais multi-level marketing ou «MLM»), bien que des différences fondamentales existent, qui permettent à certains pays d'interdire la vente pyramidale alors que la vente multiniveau reste permise (notamment en France grâce au statut de vendeur indépendant à domicile).

Internet connaît ses propres versions de systèmes pyramidaux, notamment avec le fameux spam «MMF» (Make Money Fast).

La caractéristique primordiale est que le bénéfice d'un membre est fondé principalement sur le recrutement de nouvelles personnes, qui payent pour entrer dans le système ; des ventes réelles peuvent exister et fournir un appoint et, surtout, un camouflage. Le plus souvent, cette caractéristique fondamentale est dissimulée à l'aide de différentes techniques :

Vente d'un produit futur : produit miracle dont la commercialisation va commencer « bientôt », ou encore un voyage qui ne peut être fait que lorsqu'un groupe a été recruté, etc.

Tromperie sur la marchandise : la pyramide prétend vendre un produit, en fait elle en vend un autre, par exemple une promesse de ce produit (promesse qui constitue,

elle-même, un produit, mais bien sûr très différent de ce à quoi elle se rapporte) ; la matière financière est particulièrement propice à ce genre de tromperie.
Chaque membre d'un tel réseau paie pour rentrer dans le système, et son recruteur reçoit une part de ce droit d'entrée, une autre part étant répartie dans la chaîne des recruteurs successifs. La forme et la part qui reviennent aux membres déjà dans le réseau (recruteur, recruteur du recruteur, etc.) dépend de la pyramide.
L'escroquerie dans le principe de bénéfice caché sur le recrutement est que, tôt ou tard, le système ne parvient plus à recruter assez de nouveaux pour alimenter les participants (ou leur foi dans le système). Les initiateurs (et éventuellement les premiers arrivés), ont alors largement amorti leur mise de départ, mais les membres plus récents perdent leur investissement.

Offres de prêts frauduleuses ou "Advance fee loans"

Un courriel non sollicité (spam) vous propose de régler tous vos problèmes financiers, d'obtenir de nouvelles cartes de crédit ou encore de regrouper tous vos prêts et ce, même si les autres banques ont refusé. Pour ajouter à la vraisemblance, on vous fait valoir de nombreux contacts avec les différentes agences de recouvrement. Après quelques échanges, on vous réclame des sommes pouvant atteindre plus de 1.000 euros pour enclencher les procédures. Une fois l'argent versé, les fraudeurs disparaissent évidemment dans la nature.
Ce procédé est très utilisé depuis la crise des «subprimes» aux Etats-Unis et ses conséquences dans le monde!

Arnaques aux paiements par Western Union

Beaucoup de victimes d'escroqueries sur Internet paient leurs achats via Western Union (ou Moneygram, dans une moindre mesure). Il suffit de remplir un formulaire et de présenter une pièce d'identité pour transférer de l'argent à l'étranger. Si le système est acceptable lorsqu'il s'agit d'envoyer de l'argent à un membre de sa famille par exemple, il est par contre très risqué de l'employer au bénéfice d'un inconnu.
«Un inconnu vous demande de régler un achat sur Internet via le service Western Union ? Refusez !»

Pharming

Le « pharming » est une technique d'arnaque qui consiste à rediriger le trafic Internet d'un site Web officiel vers un autre site lui ressemblant à s'y méprendre. Le but étant de collecter vos informations personnelles (nom d'utilisateur et mot de passe principalement) dans la base de données du site factice. Généralement dirigées contre des sites bancaires ou financiers, ces attaques visent à obtenir des données confidentielles afin d'accéder au compte bancaire des victimes, d'usurper leur identité («Identity Theft») ou de commettre des délits en se faisant passer pour elles.
Si le «pharming», ou utilisation de sites Web factices, peut sembler similaire au «Phishing», cette technique est toutefois plus insidieuse car vous pouvez être redirigé vers un faux site Web en toute bonne foi. Vous saisissez l'adresse web (URL) de votre site bancaire et cette adresse est redirigée vers le faux site. Les pirates utilisent une méthode appelée «empoisonnement DNS» en vue d'accéder aux gigantesques bases de données qu'utilisent les fournisseurs d'accès Internet pour acheminer le trafic Web et effectuer sur le champ, les modifications nécessaires pour rediriger les victimes vers le site frauduleux avant même qu'elles n'accèdent au site voulu.

Vols de données personnelles - "Phishing" / "Spoofing"

La technique dite du «Phishing» consiste en l'envoi de faux e-mails provenant soit disant de grandes banques ou de grands services de paiement en ligne afin d'induire l'internaute en erreur sur le contenu de l'email. En effet, ces e-mails, souvent rédigés en anglais, annoncent que le compte de l'internaute a rencontré un problème

quelconque et que ce dernier doit cliquer sur un lien qui va le diriger vers un faux site ressemblant à s'y méprendre au vrai site web («spoofing»). S'il ne s'exécute pas, l'Internaute verra son compte désactivé.
Ce faux site peut être hébergé sur un serveur qui a été préalablement piraté («hacké») par l'auteur, par un cheval de Troie, ou une faille de sécurité et donc à l'insu du propriétaire légitime de cet ordinateur.
Sur ce faux site, l'escroc va demander toutes les informations de l'utilisateur (coordonnées, numéro de carte, codes secrets, etc.) et pourra ainsi s'en servir de diverses manières : acheter des marchandises via l'Internet et payer avec les données ainsi piratées ; effectuer des transferts d'argent du compte de la victime vers un autre compte (généralement celui d'une « mule », c'est-à-dire d'un intermédiaire).

Arnaques aux propositions d'emplois ou "Work-at-Home Plans"

Via des petites annonces sur Internet, des sites d'offres d'emploi (vrais ou faux sites) ou des spams par courriels, l'escroc propose à sa future victime un travail à domicile de quelques heures par jours seulement, avec la possibilité d'obtenir de gros gains.
Exemple n° 1 : la victime est contactée par un individu, le plus souvent par un représentant d'une fausse société internationale, qui doit effectuer des transferts importants d'argent entre ses filiales. La victime doit ouvrir un compte bancaire dans une banque précise ; elle communique son numéro de compte à l'escroc ; ce dernier verse des sommes sur ledit compte et lui demande de prélever l'argent en liquide, moins une commission de l'ordre de 5 à 10% ; cet argent doit être transféré par la victime à un destinataire à l'étranger via des systèmes de payement « anonymes » tels que Western Union ou MoneyGram.
Exemple n° 2 : une offre d'emploi propose au destinataire du courriel de devenir le collaborateur d'une soi-disant société financière internationale ou même d'une ONG.
Cette société est active en Europe mais ne souhaite pas créer de filiale en Belgique ou en France, car son activité est trop limitée. Elle cherche donc des collaborateurs pour l'aider à finaliser les paiements en rapport avec les contrats qu'elle obtient ou en rapport avec les dons perçus. Si le candidat potentiel demande plus de détails, il recevra - toujours par e-mail quelques détails dans lesquels on lui expliquera qu'il recevra des fonds sur son compte bancaire et que le «travail» consistera à sortir ces fonds et à les transférer vers un autre compte.
Pour donner du poids à son offre, le correspondant joint même un projet de contrat de travail. De plus, l'intermédiaire recevra une commission sur chaque transaction.
La personne qui accepte ce genre de proposition devient le maillon d'une escroquerie, et/ou plus pratiquement le co-auteur d'un blanchiment d'argent.
En fait, l'utilisation de mules permet de résoudre un problème crucial rencontré par les criminels : récupérer en cash les fonds illégalement acquis. Puisque les virements internationaux sont très surveillés et laissent des traces, la solution consiste à recruter une mule qui effectuera les virements via Western Union. Les pistes seront ainsi brouillées.
Le meilleur conseil que l'on puisse donner, c'est de ne jamais répondre à des sollicitations qui proposent de se faire de l'argent rapidement. Si quelqu'un a néanmoins réagi en toute bonne foi à ces e-mails, il lui sera conseillé de déposer une plainte auprès d'un service de police.

Arnaques «Pump and Dump»

Le «pump and dump» (également appelé «stock dump») est une fraude financière. La fraude consiste à faire « gonfler » le prix d'une action ordinaire, en faisant courir des rumeurs positives, qui sont bien évidemment inventées de toutes pièces. Ainsi, une demande artificielle surélevée est créée, le «pumping». Quand le prix des actions est

très haut, les fraudeurs les vendent, avant que la valeur ne tombe de manière naturelle, le «dumping». Les autres porteurs d'actions n'ont ensuite plus que des actions de faible valeur.
L'exécution de cette fraude a été facilitée par l'apparition d'Internet et plus particulièrement des moyens de communication en masse comme l'e-mail. En effet, en utilisant des techniques comme le mass mailing, les fraudeurs peuvent répandre des fausses rumeurs très rapidement.

Arnaques "Spamming"

On entend généralement par les mots «spam» ou «spamming» les courriers électroniques (e-mails) publicitaires non sollicités. Entrent également dans cette catégorie, les SMS, MMS ou autres publicités non sollicités, reçus sur son GSM. Les courriers électroniques doivent comprendre une mention permettant au destinataire de refuser de continuer à recevoir des e-mails publicitaires.
Si un «spam» vous semble suspect (origine hors d'Europe, caractères bizarres, etc.), ne cliquez surtout pas sur le lien vous permettant de vous «désabonner» : dans beaucoup de cas, ce lien va juste confirmer que vous avez bien reçu le «spam» et donc vous risquez fort de recevoir encore plus d'e-mails non sollicités.

Arnaques aux faux sites de tiers de confiance - «Escrow Sites»

Un «tiers de confiance» ou «escrow site» en anglais est un intermédiaire entre l'acheteur et le vendeur. En effet, le problème lors d'un achat ou d'une vente, surtout lorsque l'on traite avec l'étranger, c'est d'être certain de recevoir sa marchandise ou son argent. C'est à cette fin qu'ont été créés les « tiers de confiance ». L'acheteur paie son achat non pas directement au vendeur mais à un intermédiaire «neutre». Ce dernier informe le vendeur qu'il a bien reçu l'argent et qu'il peut donc livrer sa marchandise à l'acheteur. Dès que l'acheteur confirme la bonne réception de la marchandise, l'intermédiaire paie le vendeur.
Évidemment, les escrocs ont vite compris l'intérêt de créer de faux sites de tiers de confiance dont l'unique but est de mettre en confiance la victime (vendeur ou acheteur) et ainsi de mieux l'arnaquer. Les sites sérieux d'enchères en ligne proposent d'ailleurs une liste des tiers de confiance approuvés et reconnus...mais souvent la future victime se laisse abuser par l'escroc et se rend sur de faux sites ! Il existe plusieurs milliers de faux sites de tiers de confiance dont plusieurs centaines sont toujours en activité. Il s'en crée tous les jours…

Arnaques «Vishing»

Le vishing utilise les mêmes principes que le phishing ; c'est la méthode de contact qui change.
Le phishing utilise le courrier électronique pour vous attirer sur de fausses pages web et pour vous faire remplir un formulaire dans lequel vous communiquerez des informations confidentielles.
Le vishing utilise quant à lui la téléphonie pour arriver au même résultat. Qu'il s'agisse d'ailleurs de votre ligne fixe ou d'un logiciel de téléphonie par Internet comme Skype, par exemple. Le vishing est donc la contraction de VoIP et de phishing. Au lieu d'être dirigé vers une page web, la victime est invitée à appeler un numéro de téléphone et là, une personne ou un serveur vocal va lui demander de communiquer son numéro de compte bancaire, le code secret, le mot de passe ou autres données personnelles sensibles.
La raison invoquée est toujours liée à un problème informatique ou de sécurité. De plus, l'interlocuteur annoncera à la victime que, si elle ne fournit pas les informations demandées, son compte sera évidemment clôturé.

Une autre variante d'arnaque consiste à envoyer des e-mails à des personnes, les invitant à communiquer, par téléphone, des informations privées. Les escrocs poussent parfois le vice jusqu'à faire appeler un numéro surfacturé (jusqu'à 25 euros minute). Une fois en possession des données personnelles de la victime, il ne restera plus aux escrocs qu'à initier des opérations financières en son nom.

Évitez l'escroquerie à la « loterie Microsoft »

Message d'alerte de Microsoft sur son site : Évitez les arnaques qui utilisent le nom Microsoft de manière frauduleuse.
Certains de nos clients ont récemment été la cible de cette arnaque, qui utilise de faux messages électroniques promettant les gains de « La loterie Microsoft ».
Malheureusement, ces clients n'ont rien gagné à la « Loterie Microsoft », parce qu'il n'existe pas de « Loterie Microsoft ».
Ces messages frauduleux ont pour unique but d'initier un dialogue afin d'extorquer argent, informations personnelles ou d'inciter à cliquer sur un lien vers un site Web malveillant.
Il s'agit donc d'une arnaque de phishing appelée « fraude aux avances sur commission». Sa forme la plus répandue est un message électronique annonçant le gain d'une forte somme d'argent ou le paiement d'une forte somme en rétribution d'une aide ou d'un service.
Cette arnaque est également connue sous le nom de « Lettre nigériane » ou arnaque «419 » en raison de son pays d'origine et du numéro d'article du code nigérian qu'elle viole.
Régulièrement, depuis des années, des spams parviennent dans les boîtes aux lettres, annonçant que vous avez gagné une forte somme à une loterie organisée par Microsoft.
La somme gagnée augmente d'année en année. Elle était de 100.000 € en 2008. Elle est passée à 250.000 € en 2013.
Pour toucher cette somme, vous devez simplement donner vos références bancaires pour que le virement soit effectué, et payer de menus frais aux avocats, notaires et huissiers qui prennent en charges votre dossier de gagnant / gagnante.
Une fois que vous aurez été soulagée de 5.000 à 10.000 € de " menus frais ", vous n'entendrez jamais plus parler de ces escrocs (généralement, c'est une seule personne qui utilise plusieurs noms, plusieurs titres (totalement usurpés, bien sûr), plusieurs boîtes email, etc. ...). L'escroc " travaille " dans un cyber café, au Nigéria (ou ailleurs dans le monde) et ne peut être tracé ni retrouvé.
Comme le cybercriminel aura toutes vos informations bancaires et toutes vos informations personnelles, il pourra voler votre identité et effectuer toutes transactions en votre nom, jusqu'à vider complètement vos comptes et même utiliser vos découverts autorisés que vous aurez à combler.

Autres arnaques utilisant le nom de Microsoft

- Vous recevez un courrier de Microsoft qui vous « demande vos détails de carte de crédit pour valider votre copie de Windows ». Microsoft demande que votre copie de Windows soit légitime avant de vous permettre d'obtenir des programmes du Centre de téléchargement Microsoft ou de recevoir des mises à jour de Microsoft Update. Le processus en ligne qui effectue cette validation se nomme le Genuine Advantage Program (Programme d'avantage légitime). Cela se passe d'ordinateur à

ordinateur et vous n'êtes pas sollicité. Microsoft ne demande jamais vos détails de carte de crédit au cours du processus de validation**.** En fait, Microsoft ne collecte aucune information qui puisse être utilisée pour vous identifier comme votre nom, votre adresse email ou autres détails personnels. Microsoft n'envoie JAMAIS de courrier. Arnaque !

- Vous recevez un message de « Microsoft » avec des mises à jour de sécurité, à exécuter, en pièces jointes. N'ouvrez pas les pièces jointes. Ce sont des virus ou pire encore. Lorsque Microsoft publie des informations sur la mise à jour sécuritaire d'un logiciel ou sur un incident de sécurité, Microsoft n'envoie d'emails qu'aux abonnés au canal de communication sur la sécurité, et ces emails ne contiennent JAMAIS de pièce jointe. Les communications légitimes de Microsoft ne contiennent jamais de mises à jour de logiciels en pièce jointes (ni de logiciel, tout court). Microsoft n'attache jamais de mises à jour de logiciels à ses communications sur la sécurité.

Microsoft préfère renvoyer ses clients sur son site Web pour l'information complète sur la mise à jour des logiciels ou l'incident de sécurité. Des cybercriminels exploitent ce canal de communication en envoyant des communications fictives sur la sécurité qui semblent venir de Microsoft. Certains messages attirent les destinataires sur des sites Web pour télécharger des logiciels espions ou d'autres logiciels malveillants.
D'autres comprennent un fichier en pièces jointe qui contient un virus. Microsoft n'envoie JAMAIS de courrier. Arnaque !

- Vous recevez un appel téléphonique d'une personne qui se prétend du « Support Technique Microsoft » et vous appelle pour réparer votre ordinateur.

Raccrochez sans explication ni discussion - ce n'est pas " grossier ", cette personne tente de vous arnaquer. Vous avez en face de vous un professionnel de la manipulation par ingénierie sociale, ne tentez pas de discuter, vous perdrez. Dans ce type d'escroquerie, les cybercriminels vous appellent et prétendent appartenir au Support Technique de Microsoft. Ils vous proposent d'aider à résoudre vos problèmes d'ordinateurs. Une fois que les escrocs ont gagné votre confiance, ils essayent de vous voler et d'endommager votre ordinateur avec des logiciels malveillants dont des virus et des logiciels espions. Comme les forces de l'ordre peuvent suivre les numéros de téléphones, les escrocs utilisent des cabines téléphoniques, des téléphones portables jetables ou des numéros de téléphones portables volés. Il vaut mieux éviter d'être trompé que d'essayer de réparer les dommages ensuite car la personne va vous demander de télécharger quelque chose : ce sera un virus (ou pire encore). La personne va vous demander de passer en mode de télémaintenance et prendra le contrôle à distance de votre ordinateur. Toutes vos données seront révélées et votre ordinateur deviendra un zombie dans un botnet. Microsoft ne fait pas d'appels téléphoniques non sollicités pour vous aider à réparer votre ordinateur. Microsoft n'appelle JAMAIS personne. Arnaque **!**

http://assiste.com/Loterie_Microsoft_Escroquerie.html

Blanchiment d'argent et arnaques liées à la réexpédition

Les candidats seraient bien avisés de se rappeler de l'expression : « l'argent sale recherche toujours le chemin le plus facile », lorsqu'ils effectuent des recherches dans le cyberespace – un marché d'emploi et de données personnelles de faible interaction.

Lorsque le crime organisé et les petits escrocs cherchent à transférer des fonds et des biens volés et à soutirer de l'argent à des complices involontaires, les sites de recrutement sur Internet sont des supports de plus en plus utilisés.
Une attention particulière est toutefois portée sur le blanchiment d'argent et les arnaques liées à la réexpédition, car ils peuvent tromper les candidats et les transformer en criminels.
Malgré la surveillance des publications des offres d'emploi, les candidats doivent savoir se protéger par eux-mêmes.

Où sont les arnaques

Les candidats doivent savoir reconnaître les arnaques les plus souvent utilisés sur Internet pour piéger des complices involontaires et des victimes. Certains argumentaires frauduleux sont publiés sous forme d'offres d'emploi. D'autres escrocs envoient à leur victime un e-mail non-sollicité, contenant le plus souvent de nombreuses fautes d'orthographe. Par exemple : « Nous avons consulté votre CV sur [site d'offres d'emploi reconnu] et avons décidé de vous proposer un poste au sein de notre entreprise. » Ils utilisent parfois une technique appelée **spoofing** (usurpation d'identité). Cette arnaque vise à faire apparaître un e-mail contenant un lien vers une offre frauduleuse comme un véritable e-mail provenant d'un site de recrutement reconnu.

Escroqueries liées au blanchiment d'argent

Le blanchiment d'argent sur Internet « est un énorme problème » déclare Susan Grant, Directrice de la surveillance de la cybercriminalité (Internet Fraud Watch) de la ligue nationale de protection des consommateurs (National Consumers League) à Washington, DC. « Dans le cas des arnaques aux faux chèques, les personnes perdent plusieurs milliers de dollars en un clin d'œil. »
Les blanchisseurs d'argent créent souvent des publications d'offres d'emploi indiquant qu'ils recrutent des citoyens américains pour « effectuer des paiements » ou « faire des virements », car étant étrangers, ils ne peuvent pas le faire eux-mêmes. Ces communications contiennent parfois des erreurs de grammaire, mais peuvent également contenir des parties très bien rédigées provenant d'offres publiées par des employeurs légitimes.
Si le candidat répond à l'annonce frauduleuse, l'escroc répondra immédiatement, affirmant au candidat qu'il est la personne idéale et lui proposera un poste. L'escroc demandera ensuite à sa victime son numéro de compte bancaire ou d'autres données personnelles. « Aucune personne légitime ne vous embaucherait pour utiliser vos compte bancaire personnel pour effectuer ces démarches » dit S. Grant.
Si les victimes coopèrent, leur compte bancaire personnel sera utilisé pour transférer des chèques volés ou frauduleux. Elles espèrent ainsi conserver un pourcentage sur les paiements en suivant les instructions de l'escroc. Si l'arnaque implique des fonds légitimes, les victimes ne pourront jamais garder les fonds. En fait, les victimes de blanchiment d'argent pourraient être tenues responsables par leur propre banque de remises de chèques sans provision.
« L'argent transférée par les victimes provient presque toujours d'un vol, et par conséquent, ces personnes commettent un délit de vol », écrit Pam Dixon dans un rapport pour le forum de confidentialité mondiale (World Privacy Forum).

Réexpédition frauduleuse

Pour les réexpéditions, ou renvois postaux, les victimes d'arnaques se sont généralement vu offrir un travail à domicile, impliquant le ré-emballage de biens volés -- souvent des produits électroniques – et leur réexpédition, en dehors des Etats-Unis la plupart du temps. Les escrocs demandent à leurs victimes de payer eux-

mêmes les frais d'expédition, et les remboursent avec compensation, à l'aide d'un chèque sans provision.
Non seulement les victimes ne seront pas remboursées, mais elles pourront être poursuivies pour arnaque à la réexpédition, être obligés de rembourser les frais d'expédition voire même le coût des biens achetés en ligne avec la carte de crédit volée.
Comment les victimes peuvent être pénalement responsables ? Pour commencer, elles ont manipulé des biens volés et suivi les instructions des escrocs pour faire de fausses déclarations sur le formulaire des douanes américaines, si elles ont réexpédié ces colis à l'étranger.

Si vous êtes impliqué

Pensez-vous que vos données personnelles ont été volées ou être impliqué dans une arnaque de blanchiment d'argent ou de réexpédition frauduleuse ? Fermez tous vos comptes bancaires et créditeurs susceptibles d'être compromis, demandez régulièrement votre rapport de solvabilité et rapportez vos suspicions aux autorités et au site de recrutement utilisé par les escrocs. Si une action ou une omission de votre part vous a amené à enfreindre la loi, prenez conseil auprès d'un avocat.

L'argent Magique :
Comment l'arnaque «PUMP AND DUMP» vide vos poches!

Pump and Dump :

Type de fraude financière qui consiste à promouvoir des stocks d'actions en bourse à un prix surévalué afin de réaliser une forte plus-value avant de la revendre.
Le «Pump and dump» est une forme de fraude qui consiste à gonfler artificiellement le prix d'une action détenue par des déclarations fausses et trompeuses positives, afin de vendre l'action bon marché acheté à un prix supérieur. Une fois que les opérateurs du régime « dump » la vente de leurs actions surévaluées, les prix baissent et tous les investisseurs, mais particulièrement ceux qui les ont acheté au prix fort perdent leur argent.
Le systeme «Pump and dump» gagne de l'argent sur la création et l'éclatement des bulles financières. Selon mes recherches, cette pratique est non seulement juridique, elle est endémique. Et cette manipulation non seulement se passe avec les actions, mais cela se passe dans toutes sortes de marchés, y compris avec les monnaies elles-mêmes. Pendant ce temps, la tromperie économique touche un grand nombre de créduls économiques, au péril de leur fonds de retraite, leurs maisons et leurs vies.

Pump and Dump
Escroqueries financières aux cours de bourses

La technique repose sur le spam et est dénommée "Pump and Dump". Elle consiste, pour l'escroc, à investir, en bourse, sur les titres de petites sociétés inconnues et ne valant rien.
Ensuite, l'escroc spam en masse la planète en recommandant l'achat de ces valeurs - il argumente pour cela en annonçant n'importe quoi (dépôt de brevet révolutionnaire, découverte minière, contrat mirobolant en cours de signature etc. ...).

En quelques jours il y a suffisamment de gogos qui tombent dans le panneau pour que les cours de ces valeurs grimpent mécaniquement.
L'escroc vend alors au plus haut, il ramasse ses billes et se sauve ailleurs pour recommencer.
Selon Sophos, le Pump and Dump arrivait en quatrième position dans les spams en circulation avec 8,5 % des messages circulants sur le Net.