Arnaque aux faux virement : Vol de 15 millions d’euros à Intermarché | Le Net Expert Informatique

Arnaque aux faux virement : Vol de 15 millions d’euros à Intermarché

Après Ryanair et de centaines d’autres entreprises, c’est au tour d’Intermarché d’être victime de l’arnaque dite « au président », une escroquerie aux faux ordres de virement internationaux (FOVI). 15 millions d’euros auraient été dérobés par ce biais.

Tout a commencé par une prise de contact avec un salarié au siège du groupe fin avril, situé dans le XVe arrondissement de Paris, en se faisant passer pour le PDG. Les cyber-escrocs sont alors parvenus à le convaincre d’opérer plusieurs virements vers des comptes bancaires étrangers, situés en Pologne.
D’après les informations de l’enquête en cours, les escrocs ont ainsi pu détourner plus de 15 millions d’euros en l’espace de quelques jours en s’en prenant à l’enseigne de grande distribution Intermarché. Une fois la supercherie découverte, l’enseigne a tenté de récupérer ses fonds mais en vain. Une enquête a été ouverte par le parquet de Paris avant d’être confiée à la direction centrale de la police judiciaire (DCPJ).
De nombreuses investigations sont actuellement en cours afin d’interpeller les auteurs de cette arnaque au « président » mais cela est complexe du fait que la coopération entre états est obligatoire et décisive.
Rappelons que ce type d’escroquerie a fait plus de 700 victimes en France durant les trois dernières années, pour un préjudice estimé à 350 M€.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.undernews.fr/banque-cartes-bancaires/arnaque-aux-faux-virement-vol-de-15-millions-deuros-a-intermarche.html

---

Alerte ! Des escrocs se font

passer pour des techniciens en informatique | Le Net Expert Informatique

Alerte ! Des escrocs se font passer pour des techniciens en informatique

Mercredi, une habitante de Saint-Pal-de-Mons a subi une tentative d'escroquerie par des cybercriminels. Elle a reçu un appel téléphonique d'une personne parlant anglais se présentant comme employée d'une célèbre entreprise d'informatique. Selon les dires de son interlocuteur, son ordinateur serait infecté d'un virus. L'appel a été transmis à un second présumé technicien qui, toujours en anglais, a proposé à la San-palouse de prendre la main sur la machine.

La femme a alors eu la puce à l'oreille lorsqu'on a lui a demandé ses coordonnées bancaires. Elle a raccroché et s'est rendue dans une entreprise spécialisée. Des fichiers de son ordinateur ont été endommagés.
Elle a ensuité déposée plainte auprès des gendarmes de la communauté de brigades de Saint-Didier-en-Velay.
Selon nos informations, les premiers éléments tendraient vers une escroquerie depuis l'étranger, l'indicatif « 00221 » au moment de l'appel étant celui du Sénégal.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.leprogres.fr/faits-divers/2015/03/13/cybercriminalite-ils-se-font-passer-pour-des-techniciens-en-informatique

---

Un réseau de fraudeurs cybercriminels démantelé au Mali

Malijet La Un réseau de fraudeurs cybercriminels démantelé au Mali

Dans le cadre de la lutte contre la délinquance économique dans le domaine des télécommunications, la section de cybercriminalité de la Brigade d'investigation judiciaire (BIJ), dirigée par l'inspecteur divisionnaire, Papa Mambi Kéita, a démantelé, le 23 février 2014, un réseau de fraudeurs sur les communications mobiles d'Orange Mali en provenance de l'international. Les deux frères fraudeurs, Seydou Mahamadou Touré et Sidi Touré, ont été pris dans le bureau à l'ACI 2000 en possession de 276 puces Orange, une unité centrale et un SIMBOX.

Après un passage remarquable à la Brigade de recherche du 3ème arrondissement, Papa Mambi Kéita plus connu sous le sobriquet « L'Epervier du Mandé » continue à faire parler de lui à la section cybercriminalité de la Brigade d'investigation judiciaire.
Car, il vient, en collaboration avec Orange Mali, de mettre le grappin sur les deux pirates. Selon Papa Mambi Kéita, le mode opératoire des délinquants consistait à masquer les appels extérieurs effectués à l'international entrants sur le réseau Orange Mali en les contournant de leur voie normale.
Selon un responsable de la société, la fraude a causé un énorme manque à gagner à la société Orange Mali et à l'Etat malien auquel la société paye des taxes et des impôts.
Pour elle, le crime ne résulte aucunement d'une défaillance quelconque de la société qui a toujours su repérer et localiser les menaces centre son réseau. En effet, la pratique utilisée est le bypass téléphonique, connu également sous le nom de SIMBOX.
Il s'agit d'un dispositif frauduleux qui permet de contourner la voie normale des appels internationaux entrants. Selon le chef de la section cybercriminalité de la BIJ, Papa Mambi Kéita, les fraudeurs ont reconnu leur crime et disent travailler pour un camerounais basé aux Etats-Unis pour une somme de 200 000 F CFA par mois.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://malijet.com/les_faits_divers_au_mali/124118-cybercriminalite_au_mali_la_brigade.html
Par Youssouf Z KEITA

Cybercriminalité : Une stagiaire dérobe 1 million de FCFA à son patron

Cybercriminalité : Une stagiaire dérobe 1 million de FCFA à son patron

Mardi 17 février 2015-Kadija Koné stagiaire dans une agence Rechercher agence de transfert d'argent a été épinglée par la Police de Lutte contre la Cybercriminalité (PLCC), pour escroquerie Rechercher escroquerie , faux et usage de faux Rechercher faux et usage de faux portant sur la somme d'un 1000 000 FCFA dérobé à son patron.

En effet, et pour subvenir aux soucis financiers de son ex compagnon, la stagiaire en question a frauduleusement retiré la somme de 1 581 550 FCFCA, sur le compte géré par son patron entre septembre 2014 et janvier 2015. Le patron ayant constaté les faits a avisé la PLCC Rechercher PLCC et porter plainte contre X.
Après enquêtes, la PLCC Rechercher PLCC a fini par mettre le grappin sur Kadija Koné, qui d'ailleurs ne mettra aucune difficulté pour reconnaitre les faits qui lui sont reprochés.
« Je voulais octroyer un prêt à usure à mon ex copain. J'ai retiré 1 000 000 FCFA sur le compte géré par mon patron. En retour et comme convenu j'ai reçu en récompense un acompte de 450 000 FCFA, ensuite mon ex devait me rembourser à hauteur de 1 200 000 FCFA », aurait-elle révélé dans les locaux de la PLCC. La stagiaire a été déférée devant le parquet pour escroquerie, faux et usage de faux.
Selon la nouvelle loi sur la cybercriminalité, cette dernière risquerait une peine allant jusqu'à 20 ans de prison ferme, et une amende de 40 millions de FCFA.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://koaci.com/cote-divoire-cybercriminalite-stagiaire-derobe-million-fcfa-patron-pour-aider-copain-elle-risque-prison-98895.html
Par Donatien Kautcha, Abidjan

Côte d’Ivoire : Deux caissières d’une agence Western Union épinglée

Côte d’Ivoire : Deux caissières d’une agence Western Union épinglée

L’équipe de la PLCC a épinglé récemment Dames Wamien Ahou Chantal et Oulobo Ahou Véronique, toutes deux caissières d’une maison de transfert d’argent de la place.
L’interpellation fait suite à l’exploitation d’une information anonyme selon laquelle ces dames se sont rendues complices d’un cybercriminel au fait de recevoir de ce dernier par SMS, des codes de transaction. Et ce, en vue de retirer des fonds. La contrepartie de ce concours frauduleux serait qu’elles prendraient 10% et expédieraient le reliquat au cybercriminel via orange money.

Après interrogatoire, les nommées WAMIEN AHOU CHANTAL ET OULOBO AHOU AHOU VERONIQUE ont reconnu sans ambage avoir rencontré un certain nommé GYPY ainsi que les faits qui leur sont reprochés.
De l’acte délictueux, elles ont avoué avoir retiré quatre (04) mandats Western-Union d’un montant total de 1 225 207 FCFA. De cette somme, elles ont également fait l’aveu d’avoir pris 106 000 FCFA et expédié le reste au cybercriminel par orange money.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.connectionivoirienne.net/106570/cote-divoire-cybercriminalite-deux-caissieres-dune-agence-western-union-epinglee

---

44,8% des avis en ligne sont biaisés selon la DGCCRF

44,8% des avis en ligne sont biaisés selon la DGCCRF

La Direction Générale de la concurrence, de la consommation et de la répression des fraudes s'est penchée sur les commentaires en ligne et les pratiques autour de ce phénomène. Et son constat est sans appel : les dérives sont nombreuses dans le domaine.

Le monde impitoyable des commentaires en ligne vient de prendre un coup dans l'aile : selon la DGCCRF, 44,8% des commentaires sont biaisés. Ce chiffre est tiré d'une étude menée par les services de la DGCCRF au cours de l'année 2013 et vient aggraver les premières tendances de l'étude de 2010 qui plaçait ce chiffre à 28,8% rapporte NextInpact.

Modération partout, vérité nulle part

Des faux avis conso ? La réalité n'est pas aussi simple que cela, explique la DGCCRF, qui détaille par la suite les différentes pratiques mises en place par les entreprises pour s'assurer une forme de contrôle sur les flux de commentaires. Cela ne signifie pas en substance que 45% des avis publiés sur le web sont faux, simplement que ceux-ci ne sont pas toujours honnêtes et présentent ce que la direction nomme avec une certaine délicatesse « des anomalies ».

Première source « d'anomalie » : la modération parfois extrêmement partiale des avis publiés sur des plateformes en ligne. Il y a bien sûr des sites qui ne s'embarrassent pas de finesse et qui se contentent de supprimer les avis négatifs, relève la direction de la concurrence. Une méthode radicale mais qui a le mérite d'être assez claire et facile à repérer.

Plus insidieux en revanche : le traitement différencié. Un avis positif passera comme une lettre à la poste, mais un avis négatif déclenchera alors un processus de médiation entre le client mécontent et l'entreprise. Avec en bout de course et si le processus de médiation aboutit, la suppression de l'avis en question. Une pratique qui pourrait être louable du point de vue du consommateur, mais que la DGCCRF qualifie de « problématique » car ces médiations se font hors de la vue du grand public et laissent donc l'utilisateur lambda ignorant des éventuels problèmes rencontrés par les autres utilisateurs.

En plein dans la zone grise

Moins discutables, la rédaction de faux avis fait aussi partie des pratiques recensées par la DGCCRF. Elle décline en deux grandes catégories : d'une part la rédaction d'avis par les professionnels ou leur entourage, souvent partiaux et encensant le produit, ou par des sous traitants qui vont alors rédiger de faux avis à la gloire du client sur différentes plateformes web contre espèces sonnantes et trébuchantes.

Plus pervers, l'instrumentalisation d'internautes lambda, invités à écrire des commentaires positifs sur la marque en échange de contreparties financières ou matérielles, ce qui jette évidemment un discrédit sur leur objectivité.

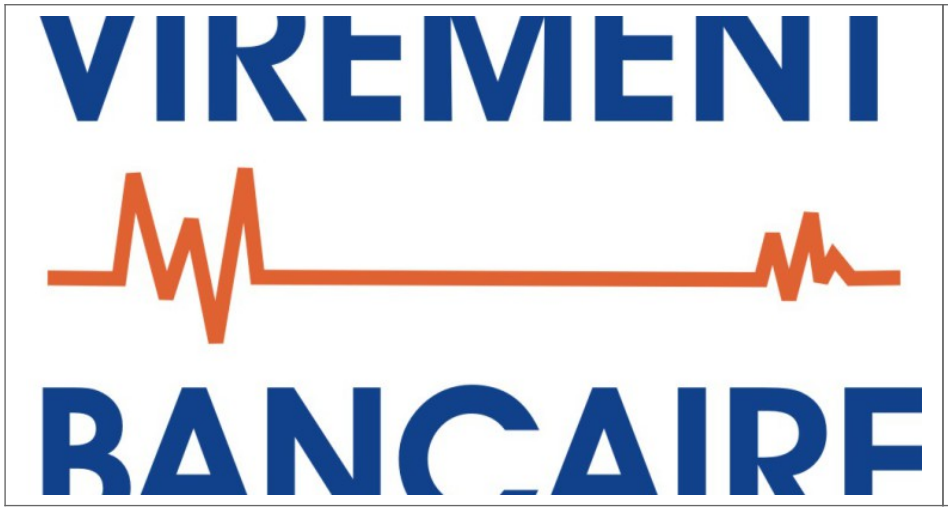
Plus étonnant mais loin d'être anodin, la direction s'inquiète du phénomène des billets sponsorisés qui fleurissent sur les blogs et sites d'informations en ligne. Si la pratique ne pose pas de problème lorsqu'elle est déclarée, elle devient contestable dès lors que l'utilisateur n'est pas informé de l'arrangement entre la marque et l'éditeur du contenu. Si on s'éloigne ici des avis de consommateur, la DGCCRF n'hésite pas à faire une petite remise au point sur les règles de déontologie traditionnelle.

Face à ce triste constat, la DGCCRF compte sur plusieurs actions afin de renforcer les droits des consommateurs, notamment par une norme internationale sur l'e-réputation, « qui comprendra un volet sur l'avis en ligne ». Une mesure qui peut faire sourire, la DGCCRF mentionnant dans le même rapport que de nombreux sites web n'hésitaient pas à se déclarer en conformité avec la norme NF Z74-501 qui pose des limites sur les pratiques autour des avis en ligne. Autre mesure avancée : des demandes de coopérations européenne autour des réglementations déjà en place.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/448-des-avis-en-ligne-sont-biaises-selon-la-dgccrf-39804407.htm
Par Louis Adam

Virements bancaires frauduleux, découvrez les dernières techniques d’escroquerie



Virements bancaires frauduleux, découvrez les dernières techniques d’escroquerie

Les entreprises sont de plus en plus souvent victimes d'escroqueries bancaires, en particulier celles touchant les virements internationaux. C'est ainsi près de 250 millions d'Euros qui sont détournés, le plus souvent au profit d'organisations criminelles. 16% des entreprises reconnaissent ainsi avoir été touchées. A côté de la classique escroquerie qui consiste à usurper la signature d'un dirigeant de l'entreprise visée, puis à transmettre un ordre de virement falsifié à la banque, trois autres sont principalement utilisées.

Jean-Marc Souvira, commissaire principal à l'Office central de la répression de la grande délinquance financière révèle dans une vidéo (ci-dessous) destinée à sensibiliser les responsables d'entreprises sur les risques encourus qui sont chaque jours plus grands. Ces fraudes touchent tous les secteurs d'activité, elles visent majoritairement le commerce, en raison du très grand nombre de transactions réalisées dans ce secteur. Il faut rappeler aussi l'exposition des fraudes a la carte bancaire comme nous en parlions ici.

Prévenir les escroqueries aux ordres de virements internationaux dans les entreprises

Virements bancaires frauduleux : les nouvelles techniques des escrocs
La première d'entre elles est appelée «escroquerie à la nigériane»: L'escroquerie à la nigériane, ainsi appelée car les auteurs procèdent depuis l'Afrique de l'ouest, consiste à envoyer un mail informant la société destinataire d'un changement de coordonnées en raison de dysfonctionnements. Les auteurs y expliquent que le paiement des prochaines factures devra s'effectuer sur un nouveau compte bancaire, mieux sécurisé. Elle touche principalement les entreprises exerçant dans le secteur du commerce, les escrocs se faisant passer pour leurs sous-traitants asiatiques.

virements bancaires frauduleux
Une autre technique l'«escroquerie au président» : L'escroquerie au Président consiste à obtenir un virement en se faisant passer pour le PDG de l'entreprise, en arguant d'une quelconque urgence pour qu'il soit immédiat. Une personne de l'entreprise est appelée par le prétendu P-DG, qui explique qu'il est en déplacement et a besoin d'un virement pour une opération confidentielle, telle qu'une OPA ou un contrôle fiscal. Très compliquée puisqu'elle nécessite une bonne connaissance de l'entreprise et de ses codes, ainsi qu'un certain aplomb, cette escroquerie est très lucrative : les sommes détournées peuvent atteindre plus d'un million d'euros pour chaque ordre.
La dernière arnaque en vogue est celle qui profite de la norme Sepa : Plus récemment, une nouvelle escroquerie exploite les failles de la norme SEPA. Les escrocs contactent les entreprises, en se faisant passer pour un informaticien de leur banque, afin de les convaincre de se connecter sur un site pour des mises à jour ou des tests de sécurité. Ce faux site leur permet de prendre le contrôle à distance du réseau interne de l'entreprise. Des ordres de virement sont alors passés, sans surveillance puisque les banques ne vérifient plus si l'ordre émane bien de l'entreprise.

La Chine, principale plateforme de réception
Pour faire face à ces arnaques, il faut avant tout du « bon sens ». Mais il faut aussi ne pas tarder à se rendre compte de l'arnaque, car les opérations de virement ne peuvent être annulées après un délai, très court. Dans leur grande majorité c'est en Chine que l'on trouve l'origine des escrocs et vers ou l'argent est ensuite versé. La police et de la justice françaises doivent d'ailleurs très prochainement rencontrer leurs homologues chinois pour étudier ce problème qui ne touche pas seulement la France mais l'ensemble de l'Europe.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesnewseco.fr/techniques-escroquerie-virements-bancaires-01609.html

Michelin victime de « l’arnaque au président », Banque – Assurances

Michelin victime de « l’arnaque au président »

Le fabricant de pneumatiques s'est fait dérober 1,6 million d'euros au moyen de l'arnaque dite « du président ».

L'arnaque est désormais bien rodée, et Michelin en est la dernière victime. Le fabricant de pneumatiques s'est fait dérober 1,6 million d'euros via une escroquerie reposant sur de faux ordres de virement, a-t-il indiqué lundi à l'AFP, confirmant une information du journal « Le Parisien ». La méthode employée est celle de « l'arnaque au président », qui sévit de plus en plus dans les entreprises.

Modus operandi

Un individu se fait généralement passer pour le président ou l'un des directeurs d'une société ou d'un groupe, et appelle un comptable de niveau assez bas dans hiérarchie, à qui il demande, dans le cadre d'une opération soi-disant très confidentielle, un virement urgent vers un pays étranger. Bien souvent, il s'agit de la Chine, ou de Chypre, mais cette fois, le pseudo directeur financier a réclamé que les règlements soient effectués sur le compte d'une banque en République tchèque. « Cet homme connaissait parfaitement la procédure à suivre et la personne à contacter au sein du groupe Michelin pour pouvoir effectuer cette modification en toute discrétion », a rapporté une source proche de l'affaire. Une enquête a été ouverte et confiée à la police judiciaire de Clermont-Ferrand.

Michelin n'est pas le premier groupe à être victime d'une telle escroquerie, « la plus redoutable » et qui requiert « une autorité naturelle, un certain aplomb et […] un don pour la comédie », expliquait récemment aux « Echos » le SRPJ de Clermont-Ferrand. Pour le service régional de police judiciaire, ces arnaques sont de trois types : outre « l'arnaque au président », on trouve l'escroquerie « à la nigériane » ou encore le détournement de la nouvelle norme Sepa , l'espace de paiement unique européen.

La fédération française bancaire a récemment mis en ligne une vidéo afin de prévenir les escroqueries aux ordres de virement :

Selon l'Office central pour la répression de la grande délinquance, quelque 700 faits ou tentatives ont ainsi été recensés entre 2010 et 2014. Le montant des préjudices atteignait, en août dernier, plus de 250 millions d'euros. Le cabinet KPMG (audits et expertises comptables) avait révélé cette année en avoir été victime, pour un préjudice de 7,6 millions d'euros.

Denis JACOPINI et son équipe vous propose des formations pour sensibiliser les salariées à ce type de pratiques cybercriminelles.

N'hésitez pas à me contacter pour organiser une session de formation. (Denis JACOPINI)

Source :

http://www.lesechos.fr/finance-marches/banque-assurances/0203910698411-michelin-victime-de-larnaque-au-president-1060501.php

---

Arnaques sur Internet : 30% des sites sont dans l'illégalité

Arnaques sur Internet : 30% des sites sont dans l'illégalité

Les arnaques sur internet se multiplient. De faux sites imitent les couleurs et le logo d'autres sites fiables, pour attirer les internautes.

Le mauvais habit qui arrive, les délais de garantie non-respectés ou encore des soldes avec des prix gonflés… Tous ces litiges du commerce sur Internet représentent la moitié des cas traités par le site Lesarnaques.com. Attention aussi au vol de vos coordonnées bancaires et à une nouvelle arnaque, plus inattendue, le faux nom de site internet.

Une copie conforme d'un site connu

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.

Comment éviter les arnaques

« Ce n'est parce que vous avez un site web où tout est écrit en français, que forcément il est basé en France. Il faut regarder les conditions générales. Si vous n'avez pas d'adresses ou d'information sur le site, il ne faut pas faire d'achats », conseille Joël Guillon, président du site Lesarnaques.com.

Pour vérifier la fiabilité d'un site, « pensez à les appeler sur la fiabilité d'un produit. Si le téléphone sonne dans le vide, c'est déjà qu'il y a un vrai service derrière », ajoute-t-il. Autre conseil : au moment où l'on fait un achat sur un site web, une page s'ouvre pour demander le numéro de carte bleue. « À ce moment-là, en haut de votre page à gauche, avant le nom de domaine se trouve « https » qui correspond à 'secure' ».

Par Anaïs Bouissou

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://www.rtl.fr/culture/web-high-tech/arnaques-sur-internet-30-des-sites-sont-dans-l-illegalite-7775018016

Alerte : Arnaque par téléphone d'un agent Microsoft

Alerte : Arnaque par téléphone d'un agent Microsoft

Depuis quelques temps, une arnaque au cours de laquelle un agent vous appelle afin de résoudre avec vous vos soucis d'informatique prend de l'ampleur à la Police.

Le principe?
De nombreuses personnes témoignent à présent du même mode opératoire : vous êtes appelé par un opérateur à l'accent anglophone, se faisant passer pour un employé de « Microsoft », ou bien de son service client « Customer Care Center ».
Selon cet opérateur, des messages d'erreur leur seraient parvenus via votre ordinateur, et pour y remédier, il vous suffit d'accéder, avec un code, à une page web « infosis.net » ou bien « logme120.com ». Ces noms changent régulièrement, c'est pourquoi c'est essentiellement le mode opératoire qui doit vous alerter.
L'agent vous demande alors d'installer un logiciel pour voir votre écran et commencer un tutoriel afin que vous puissiez résoudre ensemble votre problème informatique. Vous l'avez compris: ce programme n'est autre qu'un espion informatique chargé de s'introduire dans des relations bancaires ou des données de cartes de crédit.
Que faire?
Important :La société Microsoft a déjà réagi dans de nombreux pays, en précisant qu'elle ne contacte jamais les usagers, sans que ceux-ci ne l'aient préalablement sollicitée. De plus, l'aide de spécialistes de dépannage Microsoft ne vous est jamais facturée ainsi en ligne !
Afin de protéger un ordinateur contre diverses formes d'escroquerie, il est conseillé d'utiliser un outil de suppression de logiciels espions fiables.
Si vous n'avez pas reçu un faux appel de téléphone mais cela ne signifie pas que vous êtes protégé contre d'autres types d'escroquerie, c'est pourquoi il est conseillé d'utiliser un programme de prévention de spyware.
Dans le doute, passez en revue tous les programmes de votre ordinateur en vérifiant la fonctionnalité de chacun d'entre eux, de détecter les éventuels programmes « espions » afin de les supprimer.
Vous pouvez également signaler ces messages à la police judiciaire via Pharos : www.internet-signalement.gouv.fr
N'oubliez pas le numéro « Info Escroqueries » 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile)
! SOYEZ VIGILANT !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Arnaque-via-un-appel-d-un-agent-Microsoft