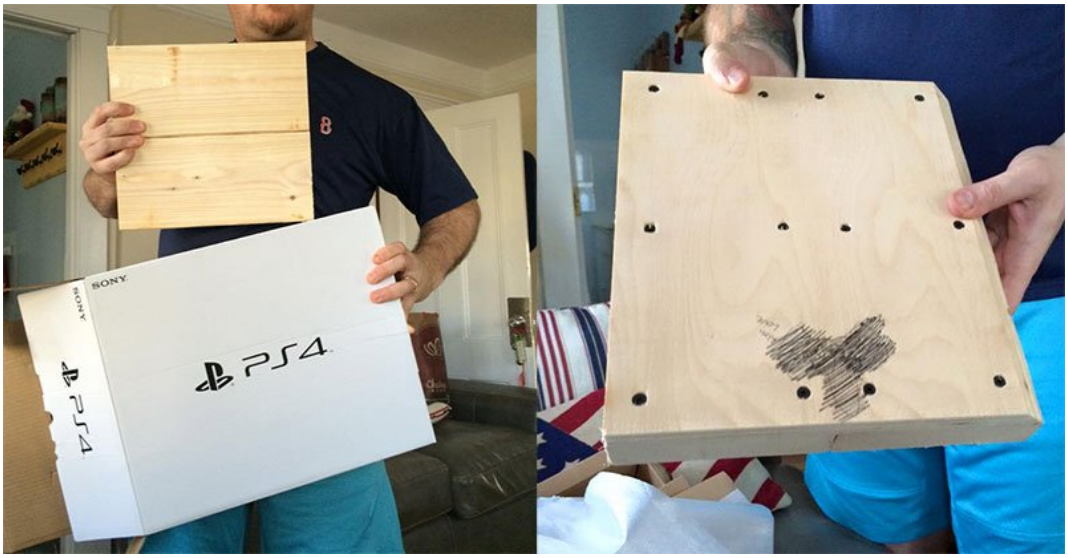
Il commande une PS4 pour Noël et reçoit à la place un morceau de bois

Il commande une PS4 pour Noël et reçoit à la place un morceau de bois

Un père de famille a fait l'acquisition d'une PS4 en boîte dans un magasin Target, en vue des fêtes de Noël. Lorsque son fils a déballé la console le 25 décembre, ils ont découvert un bloc de bois en forme de PS4 à l'intérieur.



Ah, la magie de Noël… parfois certains cadeaux laissent de marbre, tandis que d'autres font un carton. Par contre, la PlayStation 4 en bois était jusque-là inédite… jusqu'à ce que la famille Lundy, résidant dans le Massachusetts aux Etats-Unis, décide de faire l'acquisition d'une console dans le magasin Target de sa ville. Le cadeau est destiné à Scott Lundy, 9 ans. Fou de joie en découvrant son cadeau le 25 décembre, il demande à son père de l'installer sur la télévision. Seulement, au moment d'ouvrir la boite, Brian Lundy découvre à l'intérieur un bloc de bois taillé dans la même forme que la console.
Cerise sur le gâteau, un dessin sexuel, doublé d'un message insultant avait été rajouté sur la surface du bois par le voleur. On imagine assez facilement la déception du garçon de 9 ans, dont le Noël a été ruiné, mais également celle des parents qui ont dépensé plusieurs centaines de dollars pour un bout de bois assorti d'un dessin de pénis.
PS4 en bois
L'histoire s'est cependant bien terminée, puisque le magasin Target incriminé a échangé la fausse console contre une vraie, assortie de 100 dollars de bon d'achat et de la compilation Uncharted : The Nathan Drake Collection. Néanmoins, les responsables du magasin ont expliqué que « c'est quelque chose qui arrive de temps à autre ». Un voleur inventif et un peu de malchance peuvent « ruiner l'esprit de Noël », a résumé auprès de la chaîne Fox 25 la belle-mère de l'enfant. On peut malgré tout reconnaître que le faussaire a particulièrement soigné sa copie en bois : on est bien loin de la photo de la Xbox One qu'un père de famille avait reçu pour Noël 2013, après s'être fait avoir par une annonce frauduleuse sur eBay !

Réagissez à cet article

Source : *Il achète une PS4 pour Noël et se retrouve avec un morceau de bois*

Augmentation de la cybercriminalité encore prévu pour 2016

	**Augmentation de la cybercriminalité encore prévu pour 2016**

Le nombre de piratages informatiques a substantiellement augmenté en 2015, une tendance qui devrait encore s'affirmer en 2016. Chefs d'Etat, groupes industriels, médias, banques, petites entreprises ou particuliers, personne n'est à l'abri de la menace.

Si les cyber-attaques (attaques informatiques, ndlr) ont augmenté durant l'année 2015 en France et dans le monde, la tendance ne semble pas près de s'atténuer en 2016. C'est la mise en garde prononcée par de nombreux organismes, dont le Cercle européen de la sécurité et des systèmes d'information. Cet organe, qui fédère les professionnels du secteur de la sécurité informatique, redoute un cyber-sabotage de grande ampleur en 2016.
Difficile cependant de cerner le danger car il vient de partout, emploie des formes diverses et peut toucher tout le monde, directement ou pas. A grande échelle, une attaque déclenchée à distance peut viser des objectifs affectant des bassins entiers de population : réseau électrique, distribution de l'eau, contrôle de la circulation, trafic aérien. Ou encore s'en prendre à des organismes gouvernementaux avec les conséquences que cela implique.

Des attaques en forte hausse

L'Allemagne a eu affaire à ces deux types d'attaques ces douze derniers mois: la mise hors service par deux fois d'un haut-fourneau dans la Sarre et le piratage de l'ordinateur personnel d'Angela Merkel. En France, l'exemple le plus spectaculaire remonte au printemps dernier quand la chaîne francophone TV5Monde (257 millions de foyers à travers le monde) a carrément cessé d'émettre durant plusieurs heures après une attaque perpétrée par Daech.

TV5 Monde avait été ouvertement ciblée par Daech. REUTERS/Benoit Tessier

A moyenne échelle, les malfaiteurs peuvent s'en prendre à une entreprise pour lui voler des données ou gripper son système informatique. Le cabinet PricewaterhouseCoopers révélait en octobre dernier que les cyber-attaques contre les entreprises avaient progressé de 38 % en un an dans le monde et de 51 % en France alors que les pertes financières s'élevaient à 3,7 millions d'euros par entreprise victime d'attaque en moyenne. Il faut noter que plus d'un tiers des sources d'incident provient d'employés de la compagnie attaquée.
A plus petite échelle, les particuliers sont touchés par des escroqueries en tout genre, à la carte de crédit par exemple. Ainsi, un rapport récent de Norton/Symantec révélait qu'un Français sur cinq s'était fait dérober ses données bancaires après un achat en ligne. Le phénomène est tellement répandu que les banques ont peut-être trouvé la parade, du moins provisoirement : le cryptogramme dynamique qui change toutes les 20 minutes, un identifiant qui va commencer à figurer au dos des cartes de crédit en 2016.

De plus en plus sophistiqués

Les hackers, remarquent les professionnels, utilisent des méthodes de plus en plus sophistiquées pour fracturer les systèmes informatiques de leurs cibles. Dans un rapport récent, l'entreprise de sécurité informatique roumaine Bitdefender identifiait des évolutions notables pour 2016. La première touchait aux systèmes de monétisation publicitaires et en particulier les systèmes de blocage de publicité qui pourraient être utilisés par les pirates informatiques pour développer de nouvelles souches de logiciels malveillants.
D'après Bitdefender, le monde de l'entreprise va être encore plus touché en 2016 à travers des attaques ciblées visant essentiellement le vol d'informations. Mais les individus aussi seront plus vulnérables, en partie du fait de la multiplication des objets connectés qui recèlent de nombreuses failles de sécurité exploitables par les cybercriminels. Même des systèmes d'exploitation réputés plus sûrs, comme le Mac OS X d'Apple, ne seraient plus à l'abri d'être percés par les malfaiteurs en ligne, selon Bitdefender.

Réagissez à cet article

Source : *La cybercriminalité devrait encore augmenter en 2016 – France – RFI*

Vtech vend une tablette éducative tout en sachant qu’elle est défectueuse

Vtech vend une tablette éducative tout en sachant qu’elle est défectueuse

Lorsque la fille de 6 ans de Jade a développé son cadeau, le soir du réveillon de Noël, la joie a rapidement cédé la place à la déception.

«Un jouet complètement inutile», «une arnaque». C'est en ces mots que cette mère décrit la tablette Innotab max de Vtech, qui se décrit comme le chef de file mondial en jeux éducatifs électroniques pour enfants.
Le fabricant a confirmé, un peu tard aux yeux de nombreux parents, qu'il s'agissait là d'une conséquence de l'importante cyberattaque dont il a fait l'objet il y a plus d'un mois.

Depuis Noël, la page Facebook de la compagnie a été prise d'assaut par des parents déçus et frustrés de ne pas avoir été mis au courant des problèmes avec la tablette d'apprentissage qu'ils ont payée 120$.
«Quelle déception!», écrit Mélyssa Guay. «Ils auraient dû faire preuve d'honnêteté depuis le début et retirer le produit ou s'assurer que les magasins publient un avertissement», renchérit Samantha Taylor.
«Comme ça coûte cher, c'était le seul cadeau pour ma fille et elle ne peut pas l'utiliser», soupire Jade, avec qui La Presse s'est entretenue. «Il y a des choses pires que ça dans la vie, mais c'est une arnaque de vendre un produit qu'on sait défectueux.»
À mi-novembre, la base de données contenue dans le «Learning Lodge» de VTech, ou «Explor@ Park» en français, a été piratée. Explor@ Park est une plateforme sur laquelle les clients téléchargent les jeux et les vidéos. Ce n'est que deux semaines plus tard, le 30 novembre, que l'entreprise établie à Hong Kong a confirmé le piratage de millions de comptes clients et de profils d'enfants.
Les noms, les dates d'anniversaire des enfants ou les mots de passe et adresses courriel des parents ont été piratés. Mais selon le site Motherboard, du groupe Vice, le pirate a aussi mis la main sur des photos des enfants et des messages. VTech n'a toujours pas confirmé ou démenti cette dernière assertion.

Pas de compte, pas de jeux

La plateforme Explor@ Park a donc depuis été suspendue, ce qui rend impossible l'utilisation de certaines applications pour les tablettes InnoTV, InnoTab MAX, InnoTab. De plus, les nouveaux clients ne peuvent créer de compte. Sans ce compte, le WiFi, les vidéos et les jeux ne sont pas accessibles, ont confirmé des parents à La Presse.
«Je savais qu'il y avait eu une brèche informatique, mais nulle part on ne m'a dit que le produit ne fonctionnerait pas», déplore Jade.
Rachelle Lowry, de Red Deer en Alberta, a acheté une tablette VTech sur le site Amazon le 27 novembre et s'est aperçue il y a deux semaines que rien ne fonctionnait.
«Je leur ai écrit à propos du problème deux semaines avant Noël et je n'ai pas reçu de réponse», a-t-elle expliqué à La Presse. Elle s'est résignée à acheter de nouveaux cadeaux à ses trois enfants pour éviter de les décevoir. «Le service à la clientèle n'a rien fait pour m'aider depuis un mois. Ce n'est qu'à Noël qu'ils ont répondu à mon message Facebook […] C'est très frustrant.»
Le 14 décembre, plus d'un mois après l'attaque informatique, VTech Canada avait écrit sur sa page Facebook un message en anglais pour s'excuser de cet «inconvénient». Le 24 décembre, le fabricant a réitéré ses excuses, ajoutant cette fois une version française.
«Nous nous excusons des inconvénients que cette cyber-attaque et la suspension temporaire à Explor@ Park ont pu vous causer», peut-on lire. Il offre maintenant une solution de rechange, soit le téléchargement d'une mise à jour de programme permettant «de débloquer certaines fonctionnalités encore bloquées sur votre tablette et de bénéficier de 3 JEUX que nous vous offrons pour nous excuser des désagréments rencontrés».
Trop peu trop tard, selon Jade, qui croit qu'un avertissement aurait dû se trouver en magasin. Au commerce Toys'R'Us où elle a acheté le jeu, une préposée lui a affirmé le 26 décembre qu'elle n'était pas au courant du problème. Dans les grandes surfaces où nous nous sommes rendues, la tablette ne se trouvait plus. «Ça s'est beaucoup vendu cette année», a indiqué une vendeuse.

Aucun avertissement

Sur les sites internet de différents détaillants, aucun avertissement n'apparaît. Un message se trouve bien sur le site de VTechkids, mais pas sur la page du produit.
La chaîne Toys'R'Us n'a pas rappelé La Presse hier, pas plus que VTech.
Sur son site internet, le fabricant affirme qu'il espère que certaines des fonctionnalités importantes de la plateforme seront utilisables vers la mi-janvier. Rachelle et Jade attendent toujours que la compagnie leur envoie la carte SD pour effectuer la première mise à jour.
«Mais sur Facebook, j'ai lu que certaines personnes se plaignaient que ça ne fonctionnait pas et je n'ai pas beaucoup d'espoir. Je n'ai plus trop confiance», soupire Jade.

Réagissez à cet article

Source : *Vtech vend une tablette éducative qu'il sait défectueuse | Annabelle Blais | Actualités*

Deux escrocs sur Leboncoin iront en prison

Deux escrocs sur Leboncoin iront en prison

Un couple d'escrocs avait mis au point une combine simple mais redoutable sur Leboncoin. Après avoir reçu le paiement d'un client, aucune commande n'était envoyée. La justice vient de les condamner.

Dans la Somme, un couple s'était spécialisé dans l'escroquerie en utilisant le site de petites annonces Leboncoin comme plateforme. Leur technique était simple. Un client payait sa commande mais ne recevait rien en échange. La gamme de produits vendus était des plus larges, allant des aspirateurs aux jantes automobiles.

Les escrocs tablaient sur le fait qu'aucun client ne viendrait porter réclamation. Le couple avait tenté de vendre des produits plus chers, comme des voitures, mais avait éveillé les soupçons, et s'était rabattu sur des produits moins onéreux. C'est pourquoi, selon le site d'informations locales *lepaysdauge*, le couple est passé entre les mailles du filet.

Pendant près d'une année et demie, le couple a donc sévi dans le département du Calvados. En situation de surendettement, ces trentenaires justifiaient leurs détournements par le fait qu'ils avaient eux-mêmes déjà été victimes de tels actes.

La justice les a toutefois condamnés à une peine de 8 mois de prison ferme. Le fait que leurs casiers judiciaires étaient déjà remplis n'a pas joué en leur faveur. La sanction du tribunal est également assortie d'une obligation d'indemniser les victimes d'un montant total de 5 666 euros.

Réagissez à cet article

Source : *Deux escrocs sur Leboncoin iront en prison*

Prix barrés sur Internet : un vaste enfumage

	**Prix barrés sur Internet : un vaste enfumage**

Gare aux promotions trop alléchantes en ligne. Derrière les « -25 % » vantés par les vendeurs, l'UFC-Que Choisir a constaté que les rabais étaient bien inférieurs… ou même inexistants.

À 399 euros au lieu de 699, ce téléviseur est une excellente affaire. Tel est le levier d'achat que veulent actionner les e-commerçants en affichant le prix supposé être d'origine, et en le barrant d'un grand trait rouge quasi-exutoire. Sauf que ce prix, selon l'UFC-Que Choisir, est la plupart du temps totalement bidon.

En mars 2015, la réglementation encadrant les réductions de prix en ligne a été assouplie. Et comme il fallait s'y attendre, les e-marchands n'ont pas attendu pour en abuser. L'association de défense des consommateurs a mené une enquête et analysé 966 promotions. Selon elle, la totalité des rabais promotionnels de dix sites de commerce sur Internet : Auchan, Boulanger, But, Carrefour, Conforama, Connexion, Fnac, MisterGoodDeal, Topachat et Webdistrib. Et pour trois familles d'électroménager : lave-linge, réfrigérateurs et téléviseurs.

Son constat : *« 0 % des sites étudiés indique la justification des prix barrés sur les pages des promotions. »*

Une règlementation vidée de sa substance

Avant la nouvelle règlementation, le fameux prix barré – celui de référence – devait être le tarif le plus bas proposé par le vendeur depuis les 30 derniers jours, offrant une vraie base de comparaison pour le client.

Or, selon la nouvelle règle, *« toute annonce de réduction de prix est licite sous réserve qu'elle ne constitue pas une pratique commerciale déloyale au sens de l'article L. 120-1 du code de la consommation. »*

Pour avoir plus de précisions, il faut se référer à l'article L. 121-1, selon lequel *« une pratique commerciale est trompeuse (…) lorsqu'elle repose sur des allégations, indications ou présentations fausses ou de nature à induire en erreur et portant sur (…) le prix ou le mode de calcul du prix, le caractère promotionnel… »*

Dans les faits, en neuf mois de pratiques, l'UFC-Que Choisir a eu le loisir de constater que les e-marchands font à peu près ce qu'ils veulent, qualifiant la situation de *« grand bazar des prix de référence »*. *« Sur les pages des promotions que nous avons analysées, aucun des sites ne donne d'indication sur la justification du prix de référence »* dénonce l'association. Alors elle a tenté de trouver elle-même l'origine de ces prix.

Des rabais gonflés artificiellement

Le bilan est accablant. Ces tarifs sont justifiés dans moins d'un cas sur cinq. C'est-à-dire que dans plus de 80 % des situations – sur le panel de produits étudié – les promotions ne sont pas recevables. Plusieurs cas de figures se présentent. Le principal : dans plus d'un tiers des cas, le prix de référence sur lequel se base la supposée promotion correspond au tarif le plus élevé chez les concurrents au cours des six derniers mois.

Aux yeux de l'association, ceci a *« évidemment pour effet de gonfler artificiellement le montant du rabais »*. Enfin dans 41 % des cas, ajoute l'UFC, *« aucune justification logique n'a été trouvée »*. Alors que les rabais annoncés sont de l'ordre de 25 %, en réalité, le vrai bénéfice pour le consommateur est souvent de… 1 %. Sur les TV chez Topachat, c'est pire : derrière la promesse d'une baisse de 26 %, se cache une hausse de 0,5 % !

Crédit : UFC-Que Choisir

Réagissez à cet article

Source : *Prix barrés sur Internet : un vaste enfumage*

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews

---

Plus de 2 millions de personnes doivent recevoir ces jours-ci une prime de Noël de la part de la Caf et Pôle emploi. Des escrocs profitent de l'occasion pour envoyer de faux mail provenant soi-disant de ces organismes. Objectif : vous soutirer des données personnelles.

La prime de Noël est versée à partir de ce mercredi 16 décembre 2015. La période parfaite pour des cyber-escrocs de tenter de vous soutirer des informations personnelles en se faisant passer pour des administrations ou des grands organismes. Leur objectif : usurper votre identité voire se servir sur vos comptes bancaires.

La police nationale alerte en effet sur les faux mails prétendument envoyés par la Caf ou Pôle emploi, qui sont chargés de verser cette aide à plus de 2 millions de bénéficiaires. Cette technique est appelée phishing, ou hameçonnage. Pour mieux la reconnaître et donc ne pas tomber dans le piège, voici en quoi elle consiste et comment réagir :

Logos qui semblent vrais ⇒ Vous recevez un courrier électronique qui reprend les intitulés, les couleurs et les logos bien connus pour ne pas éveiller vos soupçons.

Liens vers des sites piégés ⇒ Ce mail mail comporte un lien ou une pièce jointe. En cliquant dessus, vous êtes redirigé sur un site piégé qui vous invite à saisir des données personnelles (login, mot de passe, numéro de compte client, coordonnées bancaires…) soi-disant pour confirmation ou une vérification.

Fautes d'orthographe ⇒ Ne cliquez pas si vous avez un doute. Un indice : ces faux messages comportent souvent des fautes d'orthographe. Sachez également qu'aucun opérateur ou organisme ne vous demande de venir vérifier sur leur site des informations confidentielles en vous les faisant retaper en ligne. Vous pouvez si vous le souhaitez signaler l'email douteux **ici** sur la plateforme Pharos.

Réagissez à cet article

Source : *Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews*

La menace du phishing plane sur les PME : trois étapes pour éviter le pire

La menace du phishing plane sur les PME : trois étapes pour éviter le pire

Les attaques informatiques ciblant de grands groupes, comme TV5monde, font régulièrement la une des journaux. Selon le rapport 2014 PwC sur la sécurité de l'information, 117 339 attaques se produisent chaque jour au niveau mondial.

Depuis 2009, les incidents détectés ont progressé de 66%.
Cependant, ce type d'attaques, très répandue, cible en grande partie les PME. Selon un rapport de l'ANSSI, 77% des cyber-attaques ciblent des petites entreprises.
Les conséquences peuvent être désastreuses pour ces structures à taille humaine, n'ayant pas forcément la trésorerie suffisante pour assurer leur activité en attendant le remboursement de leur assurance. Le coût d'une attaque peut s'avérer très élevé et la crédibilité de l'entreprise visée peut également en pâtir.
Suite à une attaque informatique du type « fraude au président », la PME française BRM Mobilier a ainsi perdu cet été 1,6 M€ et se trouve aujourd'hui en redressement judiciaire.
En mai dernier, le PMU a effectué un test grandeur nature en envoyant un faux email, proposant de gagner un cadeau, avec une pièce jointe piégée. Résultat : 22% des salariés ont téléchargé la pièce jointe et 6% ont cliqué sur le lien contenu dans l'email et renseigné leurs données personnelles.

Comment éviter que ce type de scénario ne vire à la catastrophe ?
1 – Connaitre le déroulé d'une attaque Le phishing, également appelé hameçonnage, est une technique employée par les hackers pour obtenir des données personnelles, comme des identifiants ou des données bancaires.
Le déroulement est simple : le hacker envoie un email en usurpant l'identité d'un tiers de confiance, comme un partenaire, un organisme bancaire, un réseau social ou encore un site reconnu.
L'email contient une pièce jointe piégée ou un lien vers une fausse interface web, voire les deux.
Si le subterfuge fonctionne, la victime se connecte via le lien, et toutes les informations renseignées via la fausse interface web sont transmises directement au cybercriminel.
Autre possibilité : la pièce jointe est téléchargée et permet ainsi à un malware d'infester le réseau de l'entreprise.

2 – Comprendre la dangerosité d'une attaque pour l'entreprise
Pour les entreprises, le phishing peut s'avérer très coûteux. Il est bien évidemment possible que le hacker récupère les données bancaires pour effectuer des virements frauduleux.
Puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites, les informations recueillies sont parfois réutilisées pour pirater d'autres comptes, comme une messagerie, un site bancaire, ou autre.Mais – puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites – il est aussi possible que le hacker réutilise les informations recueillies pour pirater une boite mail, ou un compte cloud.
Le cybercriminel peut ainsi consulter l'ensemble de la boîte mail, ou des comptes de sauvegarde cloud, et mettre la main sur des documents confidentiels, comme des plans ou des brevets, pouvant nuire à l'entreprise.
Enfin, les hackers profitent du piratage des boîtes mails pour envoyer à tous les contacts un nouvel email de phishing. La crédibilité de l'entreprise peut ainsi être touchée et ses clients pourraient subir à leur tour des pertes.

3 – Se préparer et éduquer avant qu'il ne soit trop tard
Les emails de phishing ont bien souvent une notion « d'urgence », qu'il s'agisse d'une demande pressante de la part d'un organisme ou d'un partenaire, ou d'une participation à un jeu concours « express ». Le but étant bien évidemment de ne pas laisser le temps à la victime de prendre du recul.
Comprendre le procédé d'une attaque est la première étape pour organiser sa défense. Il faut donc éduquer les salariés et leur donner quelques astuces pour ne pas tomber dans le piège :
• faire attention aux fautes d'orthographe : bien que les emails de phishing soient de mieux en mieux conçus, on y retrouve régulièrement des erreurs de syntaxe ou d'orthographe.
• regarder l'adresse mail ou le lien URL : même lorsqu'un email ou une interface web est une parfaite copie de l'original, l'adresse de l'expéditeur ou l'URL n'est pas la bonne puisqu'elle ne provient pas du même nom de domaine.
Des salariés éduqués et conscients du danger sont le meilleur atout contre les cyber-attaques, en particulier contre le phishing.
Mais, cela n'est pas suffisant, notamment sur les terminaux mobiles où nous avons tous tendance à être plus spontanés et donc, à adopter des comportement à risques.
Il est donc important de mettre en place un filtre anti-phishing aussi bien sur les postes fixes que sur les terminaux mobiles. Ces filtres scannent automatiquement les expéditeurs et les contenus afin de bloquer les emails suspects.
Pour les PME, il est donc important d'éduquer l'ensemble du personnel, mais aussi de mettre en place des solutions de filtrage email et de sécurité complètes. Par ailleurs, garder une proximité avec son équipe informatique, ou ses fournisseurs de services, peut également jouer un rôle primordial pour limiter les dommages si un employé est tombé dans le piège.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-menace-du-phishing-plane-sur,20151123,57740.htm

Le président de la CGPME avoue aussi avoir été victime de piratage informatique

	Le président de la CGPME avoue aussi avoir été victime de piratage informatique

Sous l'impulsion de son nouveau président François Asselin, la CGPME compte mettre l'accent sur le numérique. Elle a organisé mercredi 18 novembre sur Paris une session spéciale TPE-PME et cyber-sécurité.

On ne va pas se voiler la face : il y a du boulot sur la sensibilisation au thème de transition numérique pour les TPE-PME.
Un segment vraiment délaissé par les éditeurs alors qu'il correspond à une vraie représentation du tissu économique en France.
Sur les 3 millions d'entreprises en France, une proportion d'1,6 million d'entre elles dispose d'un effectif situé dans une fourchette 1 – 250 salariés.
Et les entreprises concernées se sentent bien seules car l'offre de produits et services n'est pas adaptée à leur besoin.
Alors qu'elles ont besoin de conseils personnalisés dans le domaine du numérique afin que les dirigeants d'entreprises puissent se concentrer sur leur cœur de métier.
[…]
Le témoignage le plus poignant et le plus concret rencontré sur le terrain, c'est François Asselin qui l'a délivré en clôture. Il reflète bien les problématiques auxquelles les PME sont confrontées.
En prenant la parole, François Asselin relate sa mésaventure qui a failli aboutir à la perte de son entreprise familiale de charpente, menuiserie, ébénisterie et ferronnerie d'art (147 salariés avec des serveurs sur trois sites), installée dans les Deux-Sèvres.
« Le problème de la cyber-sécurité, je l'ai vécu il y a plus d'un an et demi », lance François Asselin.
Tout part de l'ouverture d'un mail avec une pièce jointe, qui semblait reprendre un fichier d'entreprise. Mauvaise pioche : c'est un malware, qui rend tous les fichiers de l'entreprise inaccessibles (un volume de 420 000 documents) et fait tomber tous les serveurs.
Le piège du rançongiciel (ramsonware) est tendu. « Un message classique m'attendait sur le site Internet : il fallait que je verse X milliers d'euros en équivalent bitcoins pour récupérer la clé de déverrouillage de mes fichiers. »

Qui contacter en cas de pépin ?

L'anecdote du commissariat de Thouars (siège social de l'entreprise) est croustillante. François Asselin se souvient encore de la scène alors qu'il vient expliquer la situation avec le problème de son ordinateur avec copie d'écran.
« Je me souviens de l'accueil de la fonctionnaire : Hey chef, venez voir !
– Ah bah ça alors ! s'exclame le chef.
– Oui je viens porter plainte, poursuit François Asselin.
– C'est compliqué : comment on qualifie la plainte », s'interroge le supérieur.

Après ce vaudeville numérique, le niveau de la discussion remonte avec la préfecture des Deux-Sèvres contactée. *« Un interlocuteur était parfaitement au courant déjà à l'époque sur ce genre de mésaventure. »*
La situation aurait pu se transformer en catastrophe : *« Nous n'avions plus aucun accès aux logiciels : devis des clients, paie des salariés, facturation des fournisseurs…Cela aurait pu devenir une vraie catastrophe si nous n'avions pas sauvegardé les informations. Ca a sauvé la boîte, sincèrement. »*
Car la société Asselin SAS avait pris le soin de recourir depuis quelques années à une petite société de services informatiques pour assurer l'infogérance de l'entreprise.
« La réponse à ce souci de cyber-sécurité, c'est la qualité de la sauvegarde. Il a fallu 34 heures pour ré-installer les fichiers en place. On a perdu presqu'une journée de travail mais ce n'est pas dramatique. »

Cyber-sécurité : il faut en parler

Fort de cette expérience marquante, François Asselin a pris ce sujet à bras le corps et compte s'appuyer sur la commission Innovation et Economie numérique de la CGPME pour adresser la bonne parole.
« Cette aventure malheureusement, nous sommes assez nombreux à la connaître. Mais très peu d'entreprises ont porté plainte. Parce que l'outil numérique n'est pas devenu aussi indispensable que cela pour certaines entreprises. Ce n'est pas forcément une catastrophe en cas de perte. »
Mais la situation risque d'être critique en pleine transition numérique des entreprises.
Trop alarmiste ? Le président de la CGPME reprend l'exemple de l'entreprise BRM Mobilier de Bressuire (également situé dans les Deux-sèvres). Celle-ci est menacée de fermeture en raison d'une escroquerie de type « fraude au président » qui a siphonné dans le courant de l'été sa trésorerie d'un montant de 1,6 million d'euros.
Une enquête a été ouverte pour escroquerie en bande organisée.

François Asselin demande aux sociétés membres de la confédération qu'il dirige de « prendre des mesures de bon sens ».
« Sur le volet de la dématérialisation, assurez-vous de la qualité de transmissions des fichiers. Ne vous ruez pas sur le premier opérateur ou service gratuit, formez-vous à l'archivage numérique. On le fait correctement pour la version papier mais on est plus léger dans la version numérique. »
Le message est plus global : « On entend souvent parler des attaques visant des grands groupes mais il y a des PME qui sont victimes. On en mesure mal le nombre. Malheureusement, les PME sont trop silencieuses, nous avons un devoir d'évoquer ce sujet. »
En revenant sur son cas individuel, François Asselin rencontre un écueil en termes d'interlocuteurs adéquats : comment se faire accompagner par des professionnels dans le numérique qui répondent aux vrais besoins des TPE/PME. Le tout avec un budget raisonnable.
« Faire appel à une grande société informatique pour me mettre des firewall en cascade, c'est dépenser beaucoup d'argent en n'étant jamais efficace. La meilleure des efficacités, ce sont des choses de bon sens. Révisez vos procédures dans l'entreprise. C'est le meilleur moyen pour éviter la fraude au président qui fait des ravages. »

Attentats : attention au message bidon “On est tous Paris”

Attention au message bidon “On est tous Paris”

Comme après les attentats de janvier, un « hoax » ou « fake » circule à grande vitesse ces dernières heures par SMS, Facebook ou Twitter. Il s'agit d'un message qui dit vouloir prévenir que le mail « On est tous Paris » est dangereux et contient un virus.

En fait, ce message de « prévention » est lui-même potentiellement un virus ou au moins un message bidon qui n'a rien d'officiel.
L'éventuel mail « On est tous Paris » n'existe pas.
Si vous le recevez, soyez vigilants et ne cliquez surtout pas, ne le relayez pas. Il pourrait infecter votre téléphone ou votre ordinateur.
Le voici :

> Vous risquez de recevoir un mail nommé "on est tous Paris" qui est diffusé
> à grande échelle depuis ce WEEK-END.
> Dans ce message une photo de bébé avec un bracelet de naissance où il est
> écrit "on est tous PARIS" vous invitant à cliquer sur la photo.
> Ce message contient un malware (virus) qui permet de prendre le controle à
> distance de votre ordinateur et de récupérer toutes vos données et mots de passe.
> Source : service de cyber criminalité du ministère de la défense.
> Donc, envoyez ce message à vos contacts. C'est urgent et ca va très vite, ca circule depuis dimanche.
> La confirmation de cette info a été diffusée sur EUROPE 1 ce matin.

Ni le service de cybercriminalité du ministère de la défense, ni Europe 1 n'ont diffusé cette pseudo-information. Et les nombreuses fautes d'orthographe et de typographie prouvent facilement que ce message est un « fake ». Ne le diffusez pas !

Depuis vendredi, les rumeurs, fausses infos circulent sur le web. Nous en avons recensé ici :
http://france3-regions.francetvinfo.fr/nord-pas-de-calais/attentats-de-paris-mefiez-vous-des-rumeurs-sur-les-reseaux-sociaux-853751.html

Soyez prudents. Informez sur des sites de confiance et ne relayez pas des images.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, #arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://france3-regions.francetvinfo.fr/nord-pas-de-calais/attentats-attention-au-message-bidon-est-tous-paris-855033.html

Une plateforme en ligne pour combattre le Phishing | Le Net Expert Informatique

	**Une plateforme en ligne pour combattre le Phishing**

Face à l'expansion du hameçonnage (phishing), la police judiciaire française a décidé de s'allier au privé. Une initiative « exceptionnelle », relate l'AFP, présente lors de la signature, le 4 novembre, d'une convention avec l'association privée Phishing Initiative. Cette plateforme, fondée par Microsoft, PayPal et Lexsi, offre aux internautes la possibilité de lutter contre ces menaces en dénonçant l'adresse d'un site – mais pas de mails.

Pour la PJ, il s'agit d'abord de mettre l'accent sur la prévention. C'est, d'un point de vue réaliste, sa seule façon d'agir contre ce phénomène trop complexe à appréhender. Catherine Chambon, sous-directrice de la lutte contre la cybercriminalité à la direction centrale de la PJ, a expliqué à l'agence de presse que les faits étaient le plus souvent « générés par un seul auteur, de l'étranger » ce qui rend les enquêtes « longues ».

Une menace grave

En 2014, 137 000 signalements ont été effectués sur la plateforme gouvernementale Pharos, dont un tiers concernait le phishing. Depuis le début 2015, Phishing Initiative a récolté pour sa part 60 000 signalements dont 35 000 relevaient du hameçonnage. Derrière ces faux e-mails envoyés par des usurpateurs se cachent parfois des attaques hypersophistiquées comme celle menée en février à l'encontre de cent grandes banques.

Pour la société dont l'identité a été volée (une banque, un assureur, un service en ligne…), les dégâts sont d'une autre nature. Elle, qui investit énormément en communication et en marketing, peut voir ruinée sa réputation en quelques heures à peine, selon l'expert Return Path, en raison d'une campagne de phishing.

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-785286-police-phishing.html