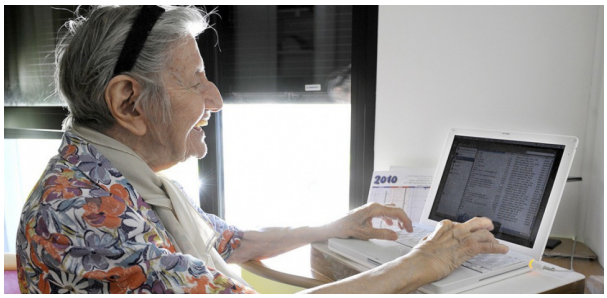
Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater | Le Net Expert Informatique

	Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater

Le piratage, ça n'arrive pas qu'aux autres. Et il n'y a pas besoin d'être ultra-connecté pour en être victime. C'est ce que raconte le « New York Times », avec l'exemple de Madame Walsh, vivant en Californie.

Cette grand-mère de six petits-enfants a accepté de servir de cobaye à deux hackeurs, se pensant à l'abri, puisque n'étant pas quelqu'un de « connecté ». Mme Walsh explique ne disposer d'aucun objet connecté (montre, etc.), sa maison n'est équipée d'aucun appareil technologique récent (thermostat connecté ou autre), et elle n'est pas une grande adepte des gadgets électroniques. Bien sûr, elle dispose d'un compte Facebook, mais n'y publie jamais rien, et s'en sert uniquement pour rester en contact avec des amis. Et pourtant.

E-mail, PaylPal, télévision et garage piratés

Les hackeurs ont bien réussi à pirater Madame Walsh. Le quotidien raconte que les pirates ont successivement testé plusieurs pistes pour tenter de s'attaquer à la grand-mère. Si son compte Facebook se révèle bien protégé, la découverte d'un « J'aime » pour une page de la plateforme de pétitions Change a été le déclic. Dix minutes plus tard, les hackeurs adressent à Mme Walsh un faux e-mail émanant de Change.org proposant de signer une fausse pétition. Bingo, la grand-mère clique, et entre son identifiant et son mot de passe. La voilà victime de « phishing ».

Madame Walsh confesse au « New York Times » utiliser le même mot de passe sur l'ensemble des services internet. Les pirates sautent sur la brèche et s'introduisent dans sa messagerie e-mail pour récupérer ses données de sécurité sociale et d'assurance maladie, et de ses comptes PayPal et Miles.

Pis, les hackeurs s'introduisent également dans le compte e-mail de sa fille, dont le code était « caché » dans un message. Enfin, ils laissent sur l'ordinateur de Mme Walsh un virus qui enregistre tout ce qui est tapé et remplace les publicités des sites visités afin de leur générer des revenus.

Pas repus, les deux hackeurs se sont attaqués à sa maison. En une heure et demie, ils ont pris le contrôle de sa télé (l'installateur du câble n'avait pas protégé la connexion) et trouvé un moyen d'ouvrir à distance la porte de son garage (via un procédé de « brute force » qui a essayé des centaines de combinaisons possibles avant de tomber sur la bonne pour la porte électrique).

Le phishing, risque numéro un

L'exemple du « New York Times » est extrême mais illustre bien que personne n'est à l'abri d'un piratage, même ceux qui se pensent « trop peu connecté pour être en danger ». Et le risque premier demeure le phishing, aussi appelé hameçonnage.

Aujourd'hui, plus de 90% des attaques dans le monde démarrent par un e-mail de phishing », affirme Ismet Geri, directeur général pour la France et l'Europe du Sud de Proofpoint, société spécialisée dans la sécurité des e-mails.

Un e-mail sur 392 serait une tentative de phishing, estime l'entreprise de sécurité informatique Symantec dans son dernier rapport. Au total, 37,3 millions d'internautes sont tombés dans le panneau dans le monde, affirme une enquête de la société de sécurité Kaspersky. La France se classe septième pays au monde dans les victimes avec un internaute sur 30 floué.

LIRE »J'ai cliqué » : chronique d'un phishing ordinaire

L'objectif des pirates est simple : récupérer des coordonnées bancaires, mais aussi des informations personnelles. Selon Symantec, au marché noir, les détails d'une carte de crédit se revendent entre 0,50 et 20 dollars, un passeport scanné 1 à 2 dollars, l'accès à un compte cloud 7 à 8 dollars, l'accès à un compte de jeux vidéo en ligne 10 à 15 dollars, etc.

L'utilisation de ces données est évidente. Les données bancaires permettent d'effectuer des achats en ligne, tandis que les informations personnelles vont permettre de s'identifier sur l'ensemble des services. Surtout que le sésame identifiant/mot de passe devient un Graal, quand on sait que 75% des Français utilisent toujours le même mot de passe.

Je m'estimais plutôt malin, je m'étais trompé ! », a confié le blogueur Thomas Messias au « Parisien » après un piratage de ses comptes. « Evidemment, j'utilisais le même mot de passe pour eBay et pour tous les autres sites… »

Voilà Madame Walsh prévenue. Et pour ce qui est de la maison, de nombreux experts en informatique démontraint régulièrement comment prendre le contrôle d'objets usuels. Cet été, le hackeur Samy Kamkar a démontré comment ouvrir des portes de garage à partir d'un jouet Mattel en moins de 10 secondes :

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://tempsreel.nouvelobs.com/tech/20151015.OBS7721/pas-assez-connectee-pour-etre-menacee-madame-walsh-s-est-pourtant-fait-pirater.html#xtor=EPR-1-ObsActu8h-20151016