FUTURA

Wi-Fi public : les raisons pour lesquelles il faut s'en méfier !

Podcast écrit et lu par Adèle Ndjaki.

[*Générique d'intro, une musique énergique et vitaminée.*]

Les risques liés au Wi-Fi public, c'est le décryptage de la semaine dans Vitamine Tech !

[*Fin du générique.*]

« Wireless Fidelity ». Le Wi-Fi est un système de connexion sans fil à Internet. Un système de connexion créé à la fin des années 90. Aujourd'hui, ce réseau à haut débit fait partie intégrante de la vie en société, on pourrait même dire qu'il est devenu omniprésent, garantissant à tous d'avoir à portée de mains toutes les informations désirées. Cependant, des personnes malintentionnées arrivent à dérober à la lumière du jour certaines informations très sensibles en passant par ces réseaux. Des réseaux pourtant publics, mais qui vous allez les voir, ne sont pas vraiment sécurisés.

[*Une musique électronique calme.*]

À la maison, dans les cafés, les gares, les librairies ou encore dans les locaux professionnels… Le Wi-Fi est aujourd'hui omniprésent. D'ailleurs, c'est la première chose que certains d'entre nous recherchent en arrivant dans un lieu public. Cependant, souvent proposées gratuitement ou en échange de collecte de données de navigation, certaines de ces connexions dites « gratuites » ne garantissent pas vraiment un accès au Net sécurisé. Ce qui est assez embêtant. Pour les hackers, ces réseaux publics sont une aubaine, elles sont à leurs yeux un fabuleux moyen de se procurer facilement les données personnelles de qui s'y connecte. Alors, évidemment, lire un article de presse, regarder le dernier épisode de sa série préférée ou encore scroller ses réseaux sociaux à l'aide d'un Wi-Fi public ne constituent pas en soi un danger. Mais consulter ses comptes bancaires, lire ses messages électroniques ou entrer des informations d'identification le sont bel et bien. Car les pirates informatiques redoublent d'ingéniosité et s'appuient sur ces connexions publiques pour justement accéder aisément à des données aussi sensibles. Ces hackers utilisent plusieurs techniques, comme celle du Honeypot par exemple, qui est l'une des méthodes les plus utilisées par les hackers. Elle consiste à créer un faux réseau Wi-Fi avec le nom d'un établissement public comme un centre commercial ou un restaurant pour subtiliser les identifiants et les données personnelles des personnes connectées. Les pirates informatiques peuvent également intercepter l'ensemble des données transmises entre un individu et le site Web qu'il visite, endommager ou voler des informations en propageant dans un appareil des programmes malveillants ou encore crypter des fichiers importants en

échange d'argent. Car oui, tout cela peut mener à la fin à du chantage, à de l'extorsion ou à de l'usurpation d'identité. Rien que ça… Pour ceux qui cherchent à tout prix à faire des économies sur leur forfait en utilisant un Wi-Fi public, toutes ces informations sont assez inquiétantes.

[*Virgule sonore, une cassette que l'on accélère puis rembobine*.]
[*Une musique de hip-hop expérimental calme*.]

En Australie, un homme a récemment été inculpé après avoir prétendument mis en place de faux réseaux wifi gratuits dans des aéroports et sur les vols intérieurs. D'après les autorités compétentes, le hacker se serait servi d'un ordinateur portable et d'un smartphone pour créer des réseaux Wi-Fi locaux qui imitent les points de connexion légitimes. L'objectif a été d'inciter les utilisateurs à entrer leurs renseignements personnels. Le malfrat a donc eu recours à la technique du Honeypot pour arriver à ses fins, l'une des méthodes qui serait la plus utilisée par les hackers, comme je vous l'ai dit précédemment. Cet événement démontre malheureusement qu'aujourd'hui, quiconque muni d'un appareil anodin comme un téléphone portable et d'une connexion Internet peut facilement devenir un cybercriminel d'envergure pouvant piéger un bon nombre d'individus. Mais comment se peut-il que les Wi-Fi publics soient aussi défaillants ? Ces points de connexion sans fil répondent à des standards de cryptage assez anciens comme le WEP, le WPA et le WPA2, des standards de cryptage devenus de plus en plus vulnérables aux attaques informatiques avec le temps. Et ouvert à tous, n'importe quelle personne peut se brancher sur un hotspot Wi-Fi et épier toutes les personnes connectées dessus. La nature même de cette connexion publique fragilise finalement sa propre sécurité, contrairement au Wi-Fi privé, qui offre une meilleure sécurité via l'utilisation de cartes SIM. Plus puissante et plus stable, la connexion nécessite cependant un coût supplémentaire. Pour mais rien n'est perdu d'avance, afin de minimiser les risques d'être pirater lorsque vous êtes connecté à un réseau public voici quelques astuces données par la CNIL: un, plutôt que de se fier uniquement au nom du réseau qui s'affiche, demandez systématiquement le nom du réseau au commerçant. Deux, lors de l'étape d'identification évitez d'utiliser votre adresse mail principale, remplissez le moins d'informations possibles, et ne cochez pas la case « communiquer mes données à des tiers » à moins que vous ne souhaitiez. Trois, privilégiez toujours la visite de sites HTTPS et utilisez votre propre VPN. Et quatre, désactivez la fonction Wi-Fi de votre appareil lorsqu'il n'est pas utilisé.

[*Virgule sonore, un grésillement électronique*.]

C'est tout pour cet épisode de Vitamine Tech. Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous invite à découvrir notre dernier épisode de Bêtes de science dans lequel Agatha Liévin-Bazin vous raconte l'histoire rocambolesque d'un animal de légende, la salamandre tachetée. Pour le reste, je vous souhaite une excellente journée ou une très bonne soirée et je vous dis à la prochaine dans Vitamine Tech.

[*Un glitch électronique ferme l'épisode*.]