Gare au Wifi gratuit : vos données confidentielles volées en quelques secondes

Il est toujours appréciable de pouvoir se connecter à un réseau Wifi gratuit. Méfiez-vous cependant : que vous utilisiez un smartphone ou un ordinateur, c'est le meilleur moyen de se faire pirater.

Avec Thibaud Badouard

Atlantico : Comment peut-on utiliser les réseaux Wifi gratuits pour voler des données confidentielles ?

Thibaud Badouard : Plusieurs scénarios sont envisageables :**il est d'abord possible pour un attaquant sur le même réseau wifi que la victime d'écouter les flux échangés entre la victime et les serveurs web. Ainsi, si le flux n'est pas chiffré, il pourra récupérer l'ensemble des données en transit. Un autre scénario envisageable est de créer des "points d'accès sauvages" qui ont les mêmes caractéristiques que le réseau d'origine et sur lequel va se connecter la victime sans s'en apercevoir**. Puisqu'il maîtrise ce point d'accès, l'attaquant pourra non seulement obtenir l'ensemble des informations en transit entre la victime et le serveur mais également créer des faux sites sur lesquels seront redirigés les utilisateurs. La mise en place de ces points d'accès sauvages est simple et peut être réalisée avec un téléphone ou des boîtiers conçus à cet effet et disponibles sur Internet.

Est-ce que tous les smartphones sont aussi vulnérables ?

Oui, **il ne s'agit pas d'une vulnérabilité propre aux smartphones mais aux réseaux Wifi** Un utilisateur se connectant sur un réseau Wifi ouvert avec son ordinateur portable est exposé aux mêmes attaques. Ceci étant, certains fabricants spécialisés proposent des terminaux sécurisés, plutôt destinés aux entreprises, qui vont réduire les risques d'interception en forçant par exemple le chiffrement systématique des flux.

Quels types de données sont visés en priorité ?

Les données visées en priorité sont les identifiants et mots de passe de connexion sur les sites internet Une fois ces informations récupérées, l'attaquant pourra récupérer les données qui l'intéressent sans avoir besoin que la victime ne soit sur le réseau wifi sauvage.

Comment s'assurer que sa connexion à un Wifi public est sécurisée ? Comment protéger ses données ?

Il n'y a malheureusement pas de moyen simple pour un utilisateur de s'assurer que le réseau Wifi public sur lequel il est connecté est légitime. **La solution drastique consiste donc à ne pas accéder à des informations confidentielles sur ce type de réseau. Sans aller jusque là et sans acquérir un terminal spécialisé, il existe des solutions logicielles qui sécurisent ces communications notamment à l'aide de VPN, qui chiffrent l'ensemble des données en transit**. Malheureusement, tous les Wifi public ne permettent pas l'utilisation de VPN. **A minima, pour réduire les risques, il est impératif de vérifier avant de se connecter à un site que la**

connexion est chiffrée (https, le fameux cadenas de la barre d'adresse) et que le site sur lequel on se connecte est légitime (si votre navigateur internet vous propose d'ajouter une exception de sécurité, il faut refuser). Par ailleurs, de manière préventive, il est nécessaire de rappeler aux populations concernées les risques associés à ces réseaux et d'illustrer les impacts, qu'ils soient professionnels (espionnage industriel) ou personnels (usurpation d'identité). Dans un contexte où les données accédées sont particulièrement sensibles, il sera nécessaire de fournir un moyen alternatif de connexion ou de sensibiliser aux éléments à ne pas consulter sur ce type de réseaux "à risque".

Comment réagir quand on se fait voler ses données ? Quels recours sont possibles ?

En cas de compromission de ses identifiants et mot de passe de connexion à un site, il est impératif de changer son mot de passe, sur le site en question bien sûr mais également sur l'ensemble des sites sur lequel vous utilisez le même mot de passe ou un mot de passe semblable. Il est également nécessaire de se poser la question de l'impact de la compromission de l'accès (qu'ont-ils pu faire avec : dans le cas d'une messagerie, est-ce que d'autres mots de passe sont accessibles dans les mails, y a-t-il des documents sensibles accessibles, etc.).

Dans un cadre professionnel, et selon les types d'informations concernées (accès au webmail de l'entreprise par exemple) il peut être utile de prévenir le responsable de la sécurité des systèmes d'information de l'entreprise ou l'organisme qui fournit les moyens techniques, afin qu'il puisse prendre les mesures adéquates. Enfin en cas d'usurpation d'identité faisant suite à ce type d'action, un recours légal est à envisager.