Les réseaux sans fil /wifi /WLAN

À la maison, au travail ou dans les lieux publics, les dispositifs mobiles nous permettent aujourd'hui de rester en ligne à tout moment et pratiquement partout, grâce la plupart du temps au wifi.

Pour vous protéger,

- limitez l'utilisation des réseaux sans fil inconnus et, si vous le pouvez, évitez-les tout simplement.
- n'effectuez pas d'opération d'e-banking et, plus généralement, ne transmettez pas de données sensibles lorsque vous utilisez un réseau public.
- connectez-vous toujours, dans la mesure du possible, à des réseaux sans fil chiffrés.
- utilisez une méthode de chiffrement récente (WPA) avec un mot de passe fort pour vous connecter à votre point d'accès.

Principe de fonctionnement

Les réseaux sans fil représentent une solution extrêmement flexible et confortable de se connecter depuis un dispositif mobile à un réseau et à Internet. Leur fonctionnement est basé sur des ondes radioélectriques et ne nécessite donc pas de câbles, ce qui simplifie considérablement les choses. Côté dispositifs mobiles, comme les tablettes p. ex., cette communication sans fil est souvent l'unique possibilité de se connecter au réseau. Ce type de connexion est également souvent activé sur les smartphones.

Toutefois, l'utilisation et l'exploitation de ces réseaux sans fil recèlent aussi un certain nombre de risques dont beaucoup ne sont pas toujours conscients.

Sécuriser l'utilisation d'un réseau wifi (WLAN)

Armez-vous de bon sens lorsque vous utilisez un réseau wifi inconnu.

Connectez-vous toujours si possible à des réseaux wifi chiffrés (WPA2 ou WPA3).

N'effectuez aucune opération d'e-banking et n'envoyez pas de données confidentielles à travers des réseaux sans fil publics, comme les « hotspots »lieux publics (villes, gares, etc.) ou des hôtels.

Utilisez le chiffrement de bout en bout pour les données confidentielles, indépendamment de la technologie de transmission choisie.

Désactivez si possible la fonction de votre dispositif mobile « se connecter automatiquement » pour les réseaux wifi inconnus et non sécurisés.

Sécuriser le fonctionnement de son réseau wifi (WLAN)

Activez un système de chiffrement robuste, basé pour le moins sur le protocole WPA, voire mieux WPA2 ou WPA3, et choisissez absolument une clé réseau forte (ou un mot de passe fort).

Changez l'identifiant ou SSID du réseau si celui-ci contient des informations liées à une personne (ex.: nom de

famille) ou à un routeur (ex.: son type).

Remplacez les mots de passe d'usine du routeur par d'autres mots de passe forts, créés par vous.

Activez le filtrage par adresses MAC.

Réduisez, si possible, la puissance d'émission de votre routeur WLAN et éteignez-le lorsque vous n'avez pas besoin du réseau sans fil local.

De même, prenez les précautions appropriées lorsque vous utilisez votre smartphone comme point d'accès (hotspot), afin d'éviter que d'autres personnes n'utilisent votre connexion mobile.

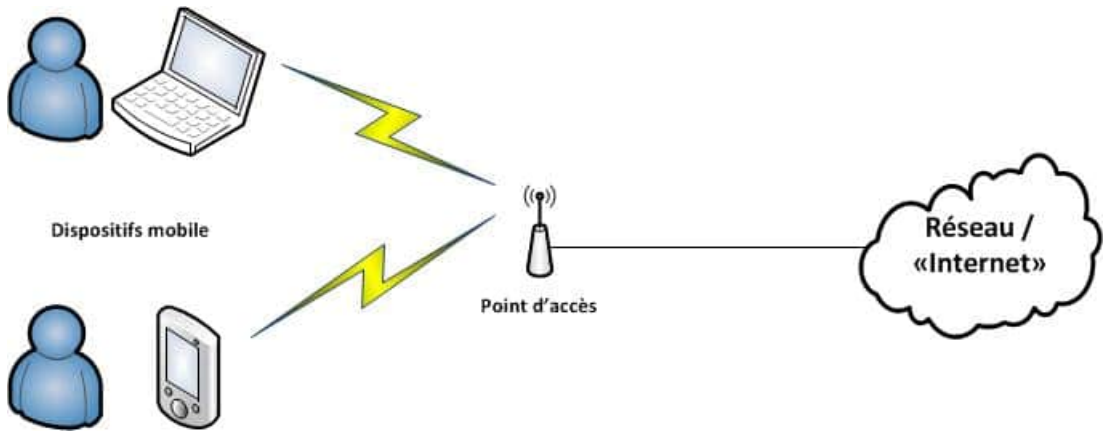
WLAN (en anglais Wireless Local Area Network) signifie littéralement « réseau local sans fil ». En français, on utilise généralement le terme wifi ou wi-fi qui désigne en réalité un protocole de communication sans fil haut-débit. La communication sans fil est extrêmement flexible, confortable et de ce fait aujourd'hui largement répandue.

Or l'utilisation et l'exploitation du wifi comporte également un certain nombre de risques. Toutefois, en adoptant les bonnes pratiques, il est possible d'augmenter considérablement la sécurité.

Pour aller plus loin

Création d'un réseau WLAN

Dans un réseau sans fil, tout tourne autour du point d'accès qui représente la passerelle entre l'interface radio vers les terminaux mobiles d'un côté, et le réseau filaire et Internet de l'autre. Le point d'accès « génère » en quelque sorte le réseau sans fil à partir du moment où son antenne émet un signal wifi dans toutes les directions.



Pour que les terminaux puissent effectivement « voir » le réseau WLAN, le point d'accès émet normalement un identifiant de service ou nom de réseau : le SSID (Service Set Identifier). C'est ce qui permet à l'utilisateur de distinguer les différents réseaux sans fil disponibles dans un même lieu, puis de sélectionner la connexion souhaitée.

Chiffrement

L'inconvénient des connexions sans fil est qu'il est relativement simple d'intercepter les données transmises. Chaque appareil situé dans la portée de communication d'un réseau sans fil capte l'ensemble du trafic de données. C'est pour cette raison qu'il convient de chiffrer la connexion entre les dispositifs mobiles et le point d'accès. Cela n'empêche certes pas la communication d'être interceptée, mais au moins personne ne pourra rien en tirer.

Il existe plusieurs procédures de chiffrement :

- **WEP**
  Le Wired Equivalent Privacy a été le premier protocole de chiffrement à être utilisé de façon standard sur les réseaux WLAN. Facile à cracker, il est aujourd'hui considéré comme vulnérable, raison pour laquelle il convient de ne plus l'utiliser.
- **WPA**
  Le Wifi Protected Access est l'évolution du protocole WEP et se base sur des mécanismes de protection améliorés pour une plus grande sécurité. Cette nouvelle clé a permis d'améliorer l'authentification des utilisateurs du réseau et d'établir un cryptage dynamique pour la transmission des données.
- **WPA2**
  Le WPA2 est basé sur son prédécesseur - le WPA, mais avec un algorithme de chiffrement plus fort, l'AES.
- **WPA3**
  Le WPA3 représente aujourd'hui le standard de chiffrement le plus récent pour les réseaux sans fil. Moins vulnérable que le WPA2, il offre notamment une bien meilleure protection contre les attaques par mot de passe.

Dans la mesure du possible, il convient donc aujourd'hui de n'utiliser dans les réseaux sans fil que le protocole WPA2 ou, mieux encore, le WPA3 lorsque celui-ci est disponible. La clé partagée (ou PSK, PreSharedKey), qui est en quelque sorte le mot de passe pour accéder au réseau, doit être suffisamment robuste. Elle doit contenir au moins 16 caractères et présenter les mêmes caractéristiques qu'un mot de passe fort (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) .

Dans ce contexte, il convient également de préciser que le système ne protège que le trajet entre le terminal et le point d'accès. Le processus de chiffrement terminant au niveau du point d'accès, les données poursuivent ensuite leur chemin sans être protégées. Les contenus confidentiels devraient donc être chiffrés de bout en bout, indépendamment de la technologie de transmission. Concrètement, lors de la navigation sur Internet ou pendant les sessions d'e-banking, la connexion doit être protégée par les protocoles de chiffrement TLS/SSL (https, cadenas dans la barre d'adresse).

Filtrage par adresses MAC

Chaque interface réseau, et donc tous les dispositifs mobiles finaux, possèdent une adresse MAC qui leur permet fondamentalement d'être identifiés. Les points d'accès donnent la possibilité d'activer un filtrage par adresses MAC. De cette manière, seuls les dispositifs mobiles « enregistrés » et identifiés par une adresse MAC connue peuvent accéder au réseau.

Les adresses MAC des dispositifs sont cependant falsifiables. Des outils spéciaux permettent de « capturer » une adresse MAC autorisée pour l'attribuer à une autre machine et de contourner ainsi le filtrage MAC. Il convient malgré tout d'utiliser cette option de protection dans la mesure où le filtrage MAC constitue un obstacle supplémentaire en cas d'attaque.