Wi-Fi public

Les participants se familiariseront avec les avantages et les risques associés au Wi-Fi public. Ils apprendront plus spécifiquement à reconnaître les réseaux Wi-Fi non sécurisés lorsque disponibles, à comprendre les compromis inhérents à l’utilisation de réseaux non sécurisés et à prendre des décisions éclairées quant aux situations dans lesquelles les utiliser.

Documentation

- Fiche Sécurité de connexion

Ressources

- Image modem sans fil

Qu’est-ce que le Wi-Fi ?

Première partie

Questions aux élèves

Quels appareils utilisez-vous pour accéder à Internet ?

Comment ces appareils se connectent-ils à Internet ?

Image Class Interaction

Le Wi-Fi est une méthode couramment utilisée pour connecter des appareils à Internet. Le Wi-Fi utilise des signaux radio pour connecter les appareils sans connexion physique ou filaire.

Imaginez que vous avez trois ordinateurs portables que vous souhaitez connecter à Internet. Pour ce faire, vous aurez besoin de ce qui suit :

1. Un point d’accès : on appelle point d’accès ce qui diffuse un signal Wi-Fi et fournit l’accès à Internet. Vos appareils doivent capter ces signaux pour pouvoir se connecter à Internet. Vous aurez parfois besoin d’une autorisation spéciale (par exemple, un nom d’utilisateur et un mot de passe) pour pouvoir vous connecter et utiliser le signal diffusé par un point d’accès.

2. Un routeur : un routeur est un appareil qui crée un réseau entre tous les appareils (ordinateurs, tablettes, téléphones mobiles) dans un lieu donné (école, bibliothèque, domicile, etc.). En règle générale, le point d’accès est intégré aux routeurs (voir le diagramme ci-dessus).

> Les routeurs ont une portée limitée (généralement courte). Pour cette raison, si votre appareil est trop éloigné du routeur, vous capterez un signal Wi-Fi faible ou ne capterez aucun signal. Par ailleurs, si quelque chose fait obstacle entre vous et le routeur (par exemple, un immeuble ou un mur de briques), le signal sera réduit.
>
> Enfin, si se connecter à un routeur permet d’accéder à un réseau, cela ne garantit pas de pouvoir accéder à Internet. Pour que plusieurs appareils sur un réseau puissent se connecter à Internet, le routeur doit être lui-même connecté à un modem.

3. Un modem : un modem est un appareil qui crée et maintient une connexion avec votre fournisseur d’accès à Internet (FAI) pour que vous puissiez vous connecter à Internet. Il convertit les signaux de l’extérieur en signaux lisibles par votre ordinateur et vos autres appareils numériques.

Dans une configuration type, le point d'accès et le routeur sont un seul et même appareil connecté au modem à l'aide d'un câble spécial appelé câble Ethernet. C'est à cela que l'on fait référence lorsqu'on parle de connexion Internet « filaire ».

Les appareils mobiles peuvent également utiliser une connexion cellulaire pour se connecter à Internet, en particulier si l'on se trouve hors de portée du réseau Wi-Fi de son domicile, d'une école ou d'une bibliothèque. Les connexions cellulaires désignent des signaux radio sans fil dont la couverture est beaucoup plus importante que celle des routeurs. Les connexions cellulaires utilisent des émetteurs-récepteurs spéciaux appelés antennes-relais pour connecter votre appareil mobile à Internet.

Deuxième partie

Questions aux élèves

Quels sont les avantages du Wi-Fi ?

Quels sont les inconvénients du Wi-Fi ?

Quels problèmes de sécurité pourrait poser le Wi-Fi par rapport à une connexion Internet filaire ?

Pourquoi perd-on son signal Wi-Fi sur son téléphone lorsqu'on sort d'un bâtiment ?

Choisir un réseau Wi-Fi

Première partie

Questions aux élèves

Tous les réseaux Wi-Fi sont-ils sécurisés ? Pourquoi ? Pourquoi pas ?

Informations aux élèves

Vous avez parfois la possibilité de choisir le réseau Wi-Fi que vous souhaitez utiliser. Il est important de se rappeler qu'une connexion au mauvais réseau peut comporter des risques. Par exemple, les réseaux Wi-Fi non sécurisés ne demandent pas de mot de passe pour se connecter. Si vous utilisez un réseau non sécurisé, il est possible que les autres personnes sur ce réseau voient vos informations. Elles peuvent alors s'emparer des informations que vous envoyez sur le réseau ou surveiller ce que vous faites.

Les réseaux Wi-Fi sécurisés et fiables demandent quant à eux un mot de passe et utilisent un système de chiffrement. Avec ces réseaux, vous avez la certitude que celui auquel vous vous connectez possède un nom de réseau qui le représente. Par exemple, se connecter à un réseau se faisant passer pour le réseau de votre école peut entraîner une divulgation des informations de compte. Par conséquent, les réseaux sécurisés et fiables sont ceux qui offrent une protection maximale.

Vous devez tenir compte du contexte ou de l'emplacement du réseau Wi-Fi. Par exemple, si vous êtes au cinéma et que vous voyez le nom du réseau de votre école s'afficher sur votre téléphone lorsque vous recherchez une connexion Wi-Fi, vous devriez comprendre que ce réseau cherche à imiter ou à usurper l'adresse du réseau de votre école afin de récupérer les mots de passe d'étudiants peu méfiants.

Lors de la configuration d'un réseau Wi-Fi protégé par mot de passe, le propriétaire doit choisir d'activer le protocole de chiffrement du routeur. Les protocoles de chiffrement communs sont les suivants : Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) et WPA2. Ces protocoles font en sorte que les informations envoyées sans fil sur le réseau soient chiffrées (ou « brouillées »).

Le chiffrement a été conçu de sorte qu'il soit plus difficile pour les pirates informatiques de voir ce que vous envoyez. Tous ces protocoles (WEP, WPA et WPA2) ont toutefois montré qu'ils n'étaient pas totalement sûrs. Il est donc important de s'appuyer également sur des connexions web sécurisées lors de l'envoi d'informations en ligne.

HTTPS est un protocole standard utilisé par les sites web pour chiffrer les données qui transitent sur Internet. Le chiffrement peut empêcher n'importe quel tiers d'avoir facilement accès à vos données de connexion. Il offre une couche de sécurité

supplémentaire et peut être utilisé dans tous les navigateurs en ajoutant « https:// » au début de l'URL (par exemple, https://www.mysite.com). Toutefois, tous les sites web ne prennent pas en charge le protocole HTTPS.

1. Ne saisissez d'informations sensibles (par exemple, mots de passe ou informations relatives aux cartes de crédit) que sur les pages web dont l'URL commence par « https:// ».

2. La plupart des navigateurs affichent un indicateur de sécurité (généralement un cadenas dans la barre d'adresse) pour signaler une connexion HTTPS.

3. Malheureusement, le protocole HTTPS seul ne garantit pas que vous soyez en sécurité étant donné que certains sites web malveillants le prennent également en charge. Le protocole HTTPS sécurise la connexion, mais ne garantit pas les bonnes intentions d'un site web.

Informations aux élèves

Secure Sockets Layer (SSL) et Transport Layer Security (TLS) sont les technologies qui garantissent la fiabilité du protocole HTTPS. Les technologies SSL/TLS utilisent des clés de chiffrement numériques, qui fonctionnent plus ou moins comme de véritables clés. Si vous écrivez un secret sur un bout de papier, toute personne qui trouve le bout de papier pourra lire votre secret. Supposons maintenant que vous remettez une clé en personne à votre ami, puis envoyez votre secret dans une boîte que seule la clé en question peut ouvrir. Si quelqu'un intercepte la boîte, il pourra difficilement lire votre secret sans la clé. Si quelqu'un a substitué votre boîte par une boîte similaire, la clé ne marchera pas avec la nouvelle boîte. Les technologies SSL/TLS fonctionnent de la même façon avec les sites web.

Les indicateurs de sécurité des navigateurs communiquent aussi des informations de certificat de validation étendue (EV). Les certificats EV sont accordés aux sites web qui vérifient leur identité auprès d'autorités de certification. Dans certains navigateurs, l'indicateur de certificat EV se trouve dans le nom du site ou dans l'entité d'enregistrement indiqué à côté de la barre d'adresse. Si vous avez des doutes sur les bonnes intentions d'un contenu de site web en particulier, vous pouvez vérifier si l'URL du certificat correspond à l'URL du navigateur en cliquant sur « Afficher le certificat ». (Vous pouvez montrer aux participants où trouver l'option « Afficher le certificat » à l'écran.) Le chemin de cette option varie d'un navigateur à l'autre. Par exemple, dans Chrome, il faut aller à Afficher **>** Développeur **>** Outils pour les développeurs. Dans Outils pour les développeurs, cliquez sur l'onglet Sécurité, puis sur Afficher le certificat.

Questions aux élèves

À quoi devez-vous penser lorsque vous vous connectez à un nouveau réseau ?

1. Réponses possibles : le lieu (ou le propriétaire du réseau), l'accès (ou les autres personnes connectées au réseau) et l'activité (ou ce que vous faites sur le réseau).

À qui appartient votre réseau Wi-Fi chez vous ? À l'école ? Au café ?

1. Le réseau Wi-Fi du domicile appartient à vos parents/tuteurs, le réseau de l'école appartient aux administrateurs ou au quartier et le réseau du café appartient à son propriétaire.

Connaissez-vous ces personnes personnellement ? Leur faites-vous confiance ?

1. Incitez les participants à discuter de la manière dont ils pourraient faire confiance à ces personnes autrement.

Informations aux élèves

Vous devez connaître et faire confiance à la personne qui héberge le réseau Wi-Fi. Vous pouvez parfois identifier le propriétaire en utilisant le SSID du réseau.

Le Service Set Identifier (SSID) est le nom donné à un réseau Wi-Fi qui s'affiche lorsque vous essayez de vous connecter. Le SSID est souvent utilisé pour transmettre des informations sur le propriétaire du réseau, ainsi que d'autres détails sur le réseau. Vous devez néanmoins rester prudent, car tout le monde ou presque (qui sait comment faire) peut créer un SSID. Par exemple, une personne peut créer un SSID identique à celui que vous utilisez à l'école. Ceci est un exemple d'usurpation d'un réseau connu et fiable afin de récupérer potentiellement les noms d'utilisateur et les mots de passe.

Savoir qui héberge le réseau peut vous aider à déterminer si le réseau est sécurisé. S'il appartient à une personne ou à une organisation digne de confiance, vous vous sentirez plus à l'aise au moment de vous connecter. Cependant, s'il s'agit d'un réseau non connu, vous ne devez pas vous connecter, car vous ne savez pas qui est le propriétaire du routeur auquel vous vous connectez. Étant donné que tout le trafic du réseau passe par le routeur, le propriétaire pourrait surveiller ou enregistrer votre trafic web.

Lorsque vous vous connectez au Wi-Fi, votre appareil est connecté à un réseau local d'appareils, et ce réseau se connecte à Internet au sens large. Votre appareil échange des informations avec ce réseau, il est donc important de faire confiance aux autres appareils auxquels vous êtes connecté(e). Ceci implique tous les appareils sur le réseau. C'est exactement comme les travaux de groupe ; vous devez pouvoir faire confiance aux personnes avec lesquelles vous travaillez.

L’utilisation d’un mot de passe sur le réseau permet de limiter les connexions. Cela signifie que vous aurez une meilleure idée des personnes qui sont connectées (qu’il s’agisse de votre famille, de vos amis ou des autres clients d’un café) que si le réseau était complètement ouvert.

Votre décision de rejoindre ou non un réseau qui peut sembler suspect dépend des compromis que vous êtes prêt(e) à faire en termes de sécurité en ligne. Vous pourriez vous demander si les avantages de rejoindre un réseau disponible valent la peine de risquer une violation de votre compte.

Questions aux élèves

Pouvez-vous lire les actualités en ligne/un blog en utilisant un réseau Wi-Fi chez vous ? À l’école ? Au café ?

1. Expliquez qu’en général, les contenus d’une page web ne sont pas des informations sensibles. Vous pouvez probablement le faire sur n’importe quel réseau.

Pouvez-vous envoyer un numéro de carte de crédit en utilisant un réseau Wi-Fi chez vous ? À l’école ? Au café ? Pourquoi ?

1. Lancez une discussion afin d’expliquer pourquoi cela est plus sûr avec un réseau Wi-Fi domestique plutôt qu’avec le Wi-Fi d’un café. Expliquez également que même si le réseau d’une école est probablement fiable, cela ne vaut peut-être pas la peine de prendre le risque puisque ces informations sont très sensibles.

Pouvez-vous consulter votre messagerie personnelle en utilisant un réseau Wi-Fi chez vous ? À l’école ? Au café ?

1. Expliquez pourquoi il est probablement plus sûr de le faire avec un réseau domestique, selon ce que contient le compte de messagerie. Par exemple, certaines personnes possèdent plusieurs comptes de messagerie qu’elles utilisent à diverses fins (p. ex. e-mails marketing/promotionnels sur un compte, et e-mails destinés aux amis et à la famille sur un autre compte).

Informations aux élèves

Il est recommandé d’envoyer/de consulter les informations sensibles (notamment les mots de passe et les informations bancaires) sur un réseau privé et sécurisé, ainsi que sur des sites web utilisant les technologies SSL/TLS plutôt que sur un réseau public partagé. Ces informations privées sont exposées à un risque lorsque vous les envoyez ou y accédez sur un réseau partagé utilisé par des personnes que vous ne

connaissez pas ou en qui vous n’avez pas confiance.

Le niveau de sensibilité des informations n’est pas toujours évident, car la confidentialité repose sur une décision personnelle que vous êtes seul(e) à pouvoir prendre. Pour savoir si vous devez vous connecter au réseau, vous devez examiner chaque situation individuellement. Avant de décider de vous connecter ou non, demandez-vous si vous faites confiance au propriétaire du réseau et aux autres personnes connectées, et interrogez-vous sur votre activité en ligne et sur les informations que vous partagez.

Réseaux sécurisés et non sécurisés

Première partie

Interaction dans la classe

Remarque : une partie du contenu de cette activité a été abordée dans l'« Activité n° 2 : Choisir un réseau Wi-Fi ». À vous de décider si vous souhaitez ou non revoir cette partie.

Informations aux élèves

Comme indiqué précédemment, les réseaux Wi-Fi non sécurisés ne demandent pas de mot de passe pour se connecter. L'utilisation d'un réseau non sécurisé fait courir un risque aux données que vous transmettez et recevez en passant par ce réseau.

Les réseaux Wi-Fi sécurisés demandent quant à eux un mot de passe et utilisent un système de chiffrement. C'est la personne qui configure le réseau qui décide ou non d'activer le chiffrement. Le chiffrement brouille les informations que vous envoyez et recevez sur un réseau, de sorte qu'il est beaucoup plus difficile pour un pirate informatique connecté au même réseau Wi-Fi de voir ce que vous envoyez ou recevez.

Ce n'est toutefois pas parce qu'un réseau est sécurisé que vos données sont en parfaite sécurité. Les réseaux sécurisés sont certes plus sûrs que les réseaux non protégés, mais cela n'empêchera pas un pirate informatique déterminé d'accéder à vos informations s'il le souhaite.

Il existe trois protocoles de chiffrement courants pour les réseaux Wi-Fi : il s'agit des protocoles WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) et WPA2. Les protocoles WEP et WPA sont obsolètes et les réseaux qui les utilisent ne devraient pas être considérés comme étant sécurisés. Il a par ailleurs été démontré que le protocole WPA2 n'est pas non plus complètement sûr.

Pour vous assurer de protéger au mieux vos informations, vérifiez que les sites web que vous consultez sont également chiffrés à l'aide des certificats SSL/TLS.

Questions aux élèves

Est-ce que quelqu'un peut citer un exemple d'un réseau protégé par mot de passe qu'il ou elle a utilisé ?

1. C'est en général les réseaux Wi-Fi que vous utilisez chez vous, à l'école ou dans certains lieux publics comme les cafés.

Est-ce que quelqu'un peut citer un exemple d'un réseau non sécurisé qu'il ou elle a utilisé ?

Et avez-vous des exemples de réseaux sécurisés ?

Informations aux élèves

Vous pouvez vérifier si un réseau Wi-Fi est chiffré ou non en examinant les paramètres réseau ou les paramètres sans fil sur votre appareil.

Deuxième partie

Interaction dans la classe

Avant de passer à cette activité d'apprentissage, effectuez une recherche Internet pour savoir comment vérifier le type de chiffrement des réseaux Wi-Fi pour différents systèmes d'exploitation. Montrez ensuite comment déterminer quel type de chiffrement un réseau utilise. Sur macOS, par exemple, cliquez sur Préférences Système -> Réseau -> Sélectionnez Wi-Fi -> Sélectionnez le nom de réseau approprié. Sous l'onglet Wi-Fi, vous trouverez une liste des réseaux connus et une colonne indiquant le type de chiffrement utilisé.

Informations aux élèves

Toutes les connexions ne sont pas les mêmes. Lorsqu'un réseau n'est pas sécurisé, n'importe qui peut s'y connecter et on ne sait pas vraiment qui le contrôle. Se connecter à un réseau non sécurisé vous rend vulnérable, dans la mesure où les informations que vous envoyez ou recevez, telles que votre trafic web (pages, mots de passe, etc.), sont potentiellement visibles par toute personne connectée au réseau si vous n'utilisez pas une connexion SSL/TLS.

Interaction dans la classe

En fonction des connaissances techniques des participants, songez à aborder l'utilisation de réseaux privés virtuels (VPN) comme couche de sécurité supplémentaire lorsque l'on se connecte à un réseau Wi-Fi. Pour en savoir plus, reportez-vous aux liens relatifs au VPN dans la section Ressources.

Déterminer la sécurité d’une connexion

Titre de la partie

Interaction dans la classe

Demandez aux participants de se mettre par groupes de 2-3 personnes. Distribuez la fiche Sécurité de connexion : fiche du participant et attribuez un scénario à chaque groupe. Donnez cinq minutes aux participants pour discuter de leurs scénarios. Demandez ensuite aux groupes de partager leurs réponses. Les réponses sont indiquées en vert dans la fiche.

Exercice

Première partie

Devoir

Demandez aux participants de :

1. Tracer la chronologie d'une journée type, en indiquant les réseaux Wi-Fi auxquels ils se connectent.

2. Parmi les réseaux indiqués dans la chronologie, demandez aux participants d'en choisir deux et d'écrire un court paragraphe pour chacun avec la description du réseau, en précisant notamment qui d'autre s'y connecte et dans quelle mesure il est sécurisé.

3. Pour les deux réseaux choisis, demandez par ailleurs aux participants de décrire les avantages et les éventuels risques de l'accès à de tels réseaux.