

NAVIGUER SUR INTERNET EN TOUTE SECURITÉ

Avant et pendant la navigation sur Internet, et l'utilisation de ses services, il est impératif de respecter certaines précautions.

Nous examinerons dans cet exposé le pourquoi et le comment de ces précautions.

1 - Mais pourquoi prendre des précautions ?

- Dès qu'un ordinateur est connecté à Internet il va subir en permanence plusieurs attaques par minute. Ces attaques sont essentiellement des attaques automatiquement lancées à partir de machines déjà contaminées par des virus informatiques. L'attaque directe par un pirate informatique est rare.
- Les finalités de ces attaques:
 - accéder au système
 - obtenir des informations sur l'utilisateur,
 - récupérer des identifiants et mots de passe (pour une connexion bancaire par exemple)
 - perturber le fonctionnement de l'ordinateur (publicités intempestives, données devenues inaccessibles, ...)
 - utiliser le PC comme « rebond » pour effectuer une attaque,
 - **le but ultime consiste essentiellement à essayer de soutirer de l'argent aux utilisateurs soit directement soit par une usurpation d'identité**

Pour en savoir plus : site de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information): <http://www.ssi.gouv.fr/>

A consulter notamment le lien <http://www.ssi.gouv.fr/particulier/principales-menaces/>

→ Exemples d'attaques :

- logiciels malveillants, comme *WannaCrypt*, qui sont des Ransomware (logiciels de rançonnage): réception d'un e-mail contenant une pièce jointe qui, si elle est ouverte, va chiffrer les fichiers du disque dur. La victime est ensuite invitée à verser de l'argent afin de débloquer ces fichiers. Voir <http://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiel-2/>
- les mails provenant d'une personne de votre connaissance et qui se trouve bloquer à l'étranger La personne est en détresse et a un besoin impératif d'argent
- les mails provenant de sociétés comme Orange, EDF, Assurance Maladie, votre banque, les Impôts... et qui vous demandent de cliquer sur un lien pour un remboursement, un problème de sécurité, ...(Phishing ou Hameçonnage)
- les appels téléphoniques provenant des impôts ou d'autres organismes vous demandant des informations personnelles pour vous rembourser un trop plein versé.,
- les fenêtres publicitaires qui s'ouvrent de manière intempestive dans Internet
- les appels téléphoniques venant soi-disant de Microsoft pour un problème de l'utilisateur.

L'appelant demande l'autorisation de prendre la main sur son PC. Si l'utilisateur accepte son ordinateur est bloqué et ne refonctionne qu'en payant une somme d'argent conséquente

→ Quelques chiffres :

- 2 millions de français en 2015 ont répondu favorablement à des mails frauduleux leur demandant leurs coordonnées bancaires (Phishing): 100 fois plus qu'en 2014
- 391 000 PC bloqués en France en 2016 avec demande de rançon pour les débloquenter
- nombre de sites d'investissements illégaux: de 10 en 2010 on est passé à 400 en 2016. Selon le parquet de Paris 4,3 milliard d'euros auraient été perdus sur ces sites illégaux

2 -Quelles précautions prendre ?

2 – 1 - Précautions techniques

- disposer d'un antivirus à jour ; vérifier que la base de données virales est à jour
« Scanner » périodiquement son disque dur (une fois pas semaine)
- disposer d'un antispyware à jour ; vérifier que la base de données est à jour
« Scanner » périodiquement son disque dur (une fois pas semaine)
- vérifier que les mises à jour Windows s'effectuent régulièrement et normalement
- s'assurer que les logiciels qui utilisent Internet sont bien à jour
- s'assurer que le pare-feu est actif et bien configuré
- être vigilant avec les connexions wi-fi publiques
- travailler avec un compte utilisateur qui possède des droits limités
- effectuer régulièrement des sauvegardes de ses données

2 – 2 - Précautions humaines

- se méfier des mails non habituels (de même pour des SMS ou des appels téléphoniques suspects)
- se connecter sur des sites internet sûrs
- mots de passe : éviter ceux qui sont faciles (prénoms, mots du dictionnaire, ...)
- ne pas donner d'informations personnelles et de sécurité (mots de passe, données personnelles,...) demandées par mail, téléphone, SMS ou un collègue.
- lire les alertes de sécurité (Microsoft, Assurance Maladie, Banque,...)

Pour en savoir plus : <http://www.ssi.gouv.fr/particulier/bonnes-pratiques/>

Quelques vidéos de démonstration: <https://www.hack-academy.fr/home>

Si vous êtes victime: <https://www.cybermalveillance.gouv.fr/>

MOOC de l'ANSSI: <https://secnumacademie.gouv.fr/> (MOOC: Massive Online Course ou cours en ligne gratuit et ouverts à tous)

2 – 3 - Conclusion

Quand on navigue sur Internet, ou que l'on utilise ses services comme la messagerie, il faut toujours rester vigilant. Cette attitude permettra à l'utilisateur de se servir de son ordinateur sans que celui-ci subisse des ralentissements, voire des blocages, dus à des virus et de se prémunir d'attaques informatiques de type demande de rançons.

3 - Antivirus

3-1 - Qu'est-ce qu'un virus ?

Un virus est un programme qui va se loger quelque part dans un système d'exploitation ou dans un programme à l'insu de son utilisateur. Son objectif est variable. Cela va de la simple balle de ping-pong qui traverse l'écran à la destruction des données de l'utilisateur. Il peut modifier des informations pour qu'elles deviennent inutilisables, bloquer l'ordinateur en supprimant certains fichiers ou en saturant les ressources de la machine.

Les effets d'un virus dépendent de l'objectif de son auteur, mais les virus ne sont jamais inoffensifs.

Pour information un nouveau virus apparaît tous les 15 secondes dans le monde.

3-2 - Qu'est-ce qu'un antivirus ?

Un antivirus est un programme qui effectue des actions de:

⇒ **détection** : il vérifie la présence de virus dans les fichiers que vous utilisez, et vérifie régulièrement tous les fichiers de façon automatique ou lorsque vous le lui demandez.

⇒ **éradication** : dans la mesure du possible il supprime les virus détectés.

Attention ! Certains virus attaquent directement les logiciels antivirus et les désactivent. Vérifier que les mises à jour des données virales fonctionnent bien et que les « scan » programmés s'effectuent toujours. Si l'antivirus est bloqué il faudra lancer alors un « scan » du disque dur à partir d'un antivirus accessible par Internet (voir « scan » du disque dur chapitre 3.5)

3-3 - Choisir un antivirus

- Il existe des antivirus gratuits et d'autres payants (abonnement annuel). Quelques éditeurs :

- Avast
- Norton AntiVirus (Symantec)
- Kaspersky Anti-Virus Personal
- Trend Micro Anti-Virus
- McAfee
- G-Data
- Panda
-

- Editeurs d'antivirus dont la licence d'utilisation est gratuite.

- Avast
- AVG
- Bitdefender Free
- Microsoft Security Essentials
-

Il existe des sites qui donnent des informations sur les antivirus gratuits.

Exemple: <http://www.commentcamarche.net/faq/35-antivirus-gratuit-lequel-choisir>

Attention ! Ces versions gratuites sont généralement moins complètes, donc moins efficaces que les versions payantes.

Remarque : les fournisseurs d'accès Internet proposent presque tous un antivirus qui vérifie les e-mails que vous recevez, mais aussi ceux que vous envoyez. Cet antivirus ne protège pas votre ordinateur directement, il ne s'occupe que des e-mails et de leurs pièces jointes.

Prendre garde aux faux antivirus

Il faut installer un antivirus d'un éditeur connu. Ne jamais installer un des multiples faux antivirus présents sur Internet. Ce type de logiciel une fois installé sur l'ordinateur envoie des messages pour effrayer l'utilisateur en lui faisant croire que son système a été infecté avec des menaces qui en réalité n'existent pas. Puis il l'invite à acheter des services pour nettoyer ces prétendues menaces. Le faux antivirus continue d'envoyer ces alertes dérangeantes et intrusives jusqu'à ce qu'un paiement soit effectué.

3- 4 - Installer l'antivirus

Suivre la procédure proposée par l'antivirus :

- fermer toutes vos applications.
- désinstaller, s'il en existe un, l'antivirus préinstallé sur l'ordinateur, même s'il s'agit de la même marque
- procéder à l'installation
- redémarrer l'ordinateur à la fin de l'installation

3-5 – « Scanner » le disque dur de votre ordinateur

3-5-1- Mise à jour

La base de données virales est mise à jour en permanence, au fur et à mesure des sorties de nouveaux virus.

Il faut s'assurer aussi que la version installée soit bien la dernière.

3-5-2 – « Scan » du disque dur

Lorsqu'on qu'un antivirus "scanne" un ordinateur il lit les fichiers du disque dur un par un et vérifie qu'ils ne contiennent pas à l'intérieur des morceaux de programmes qui pourraient être des virus.

→ **Cette étape est longue.** Lancer un « scan » une fois par semaine

.3-5-3 Traitement des virus

Lorsque l'Antivirus trouve un fichier qui contient un virus il le retire. Mais, parfois, le virus est trop bien implanté, l'antivirus est alors obligé de mettre le fichier en "quarantaine". Vous ne pourrez plus accéder à votre fichier, mais il ne représente plus une menace.

.3-5-4 Quand le « scan » ne s'exécute pas

Si l'ordinateur est infecté par un virus qui bloque l'Antivirus (blocage des mises à jour, blocage du « scan ») il faut effectuer un « scan » du disque dur à partir d'un antivirus accessible par Internet. Se connecter avec son navigateur à un des sites qui offre ce type de service (attention aux faux sites de recherche de virus) :

- Bitdefender
- Trend Micro
- F-Secure
- ...

Note : Ces sites vous demanderont de télécharger et installer des logiciels, acceptez-les. Si votre pare-feu vous demande de les autoriser à accéder à Internet, vous pouvez dire oui.

3-6 – Téléphone mobile : Les premiers virus

Les premiers virus pour les téléphones mobiles viennent d'apparaître, même si leur vitesse de propagation est relativement lente.

Les constructeurs de téléphones travaillent avec les sociétés d'antivirus pour intégrer des antivirus dans les prochains modèles de téléphone.

En attendant, il est conseillé de se munir d'un logiciel antivirus, comme pour votre ordinateur.

Quelques éditeurs : - Avast Free Mobile Security
- Trend Micro Mobile Security
- F-Secure Mobile Anti-Virus

Les téléphones récents sont les plus vulnérables, puisqu'ils sont équipés des technologies Bluetooth et MMS. Bluetooth permet aux téléphones de communiquer avec d'autres équipements électroniques, mais permet aussi aux virus de se propager de téléphone en téléphone. De la même manière, les MMS peuvent servir à transmettre des virus.

4 - Antispyware

4-1 - Qu'est-ce qu'un « spyware » ?

Il s'agit de petits logiciels espions qui s'installent à votre insu en utilisant une faille de sécurité de votre navigateur ou s'installent en même temps que certains autres logiciels. La traduction française la plus couramment rencontrée est "espiogiciel".

La frontière avec les virus est très mince, mais cette fois l'intrusion est à l'initiative de sociétés commerciales douteuses. Contrairement aux virus les "spywares" ne se propagent pas.

Les spywares peuvent effectuer des tâches très diverses :

- envoyer des informations depuis votre PC sur vos habitudes d'utilisation d'Internet,
- changer la page d'accueil de votre navigateur,
- changer les pages web que vous visitez,
- afficher des publicités (on parle alors de Adware),
- etc.

4-2 - Qu'est-ce qu'un « antispyware » ?

Il fonctionne presque à l'identique d'un antivirus, l'antispyware va "scanner" toutes vos données, mais aussi regarder quels programmes sont en cours de fonctionnement, regarder si vous n'avez pas des cookies qui renseignent des sociétés sur les sites que vous visitez, etc.

4-3 - Choisir un « antispyware »

Quelques éditeurs proposent des anti-spywares sous licence gratuite :

- "Windows Defender" de Microsoft (installer par défaut sur Windows 8)
- SpyBot Search & Destroy
- MalwareBytes
- ZHPCleaner
- AdwCleaner (il élimine les logiciels publicitaires qui s'incrument dans le navigateur)

Attention! Comme il existe des faux antivirus il existe des faux « antispyware »

4- 4 - Installer un « antispyware »

L'installation d'antispyware est identique à celle d'un antivirus : se reporter au chapitre 3.4

4-5 – « Scanner » le disque dur de votre ordinateur

Le « scan » de l'ordinateur avec l'antispyware est identique à celui d'un Antivirus : se reporter au chapitre 3.5

5 – Mises à jour logiciels

5-1 - A quoi servent les mises à jour ?

Les mises à jour des logiciels et de Windows permettent de maintenir le système à jour. Elles consistent à télécharger et installer des nouveaux modules qui apportent des améliorations, corrigent des erreurs dans les programmes, renforcent la sécurité.

Un système d'exploitation comme Windows est extrêmement complexe et des failles de sécurité sont régulièrement découvertes.

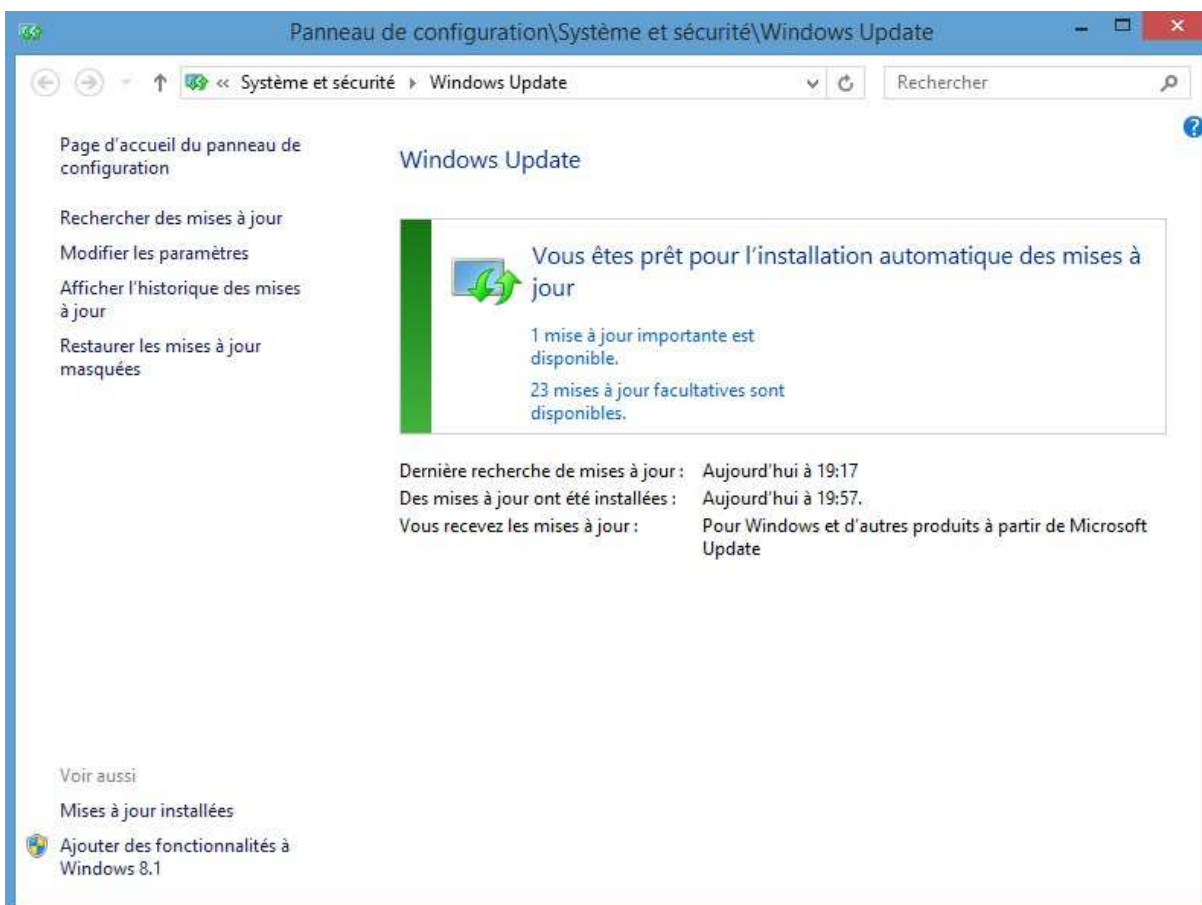
Si ces erreurs n'étaient pas corrigées elles risqueraient de permettre à des virus ou des pirates informatiques de pénétrer dans l'ordinateur et d'y exécuter des actions malveillantes.

Exemple: voir le bulletin de sécurité critique de Microsoft MS17-010 du 14 mars 2017. Cette faille de sécurité a été exploitée lors d'une attaque qui a touché plusieurs pays à mi-mai 2017 (comme l'entreprise Renault en France).

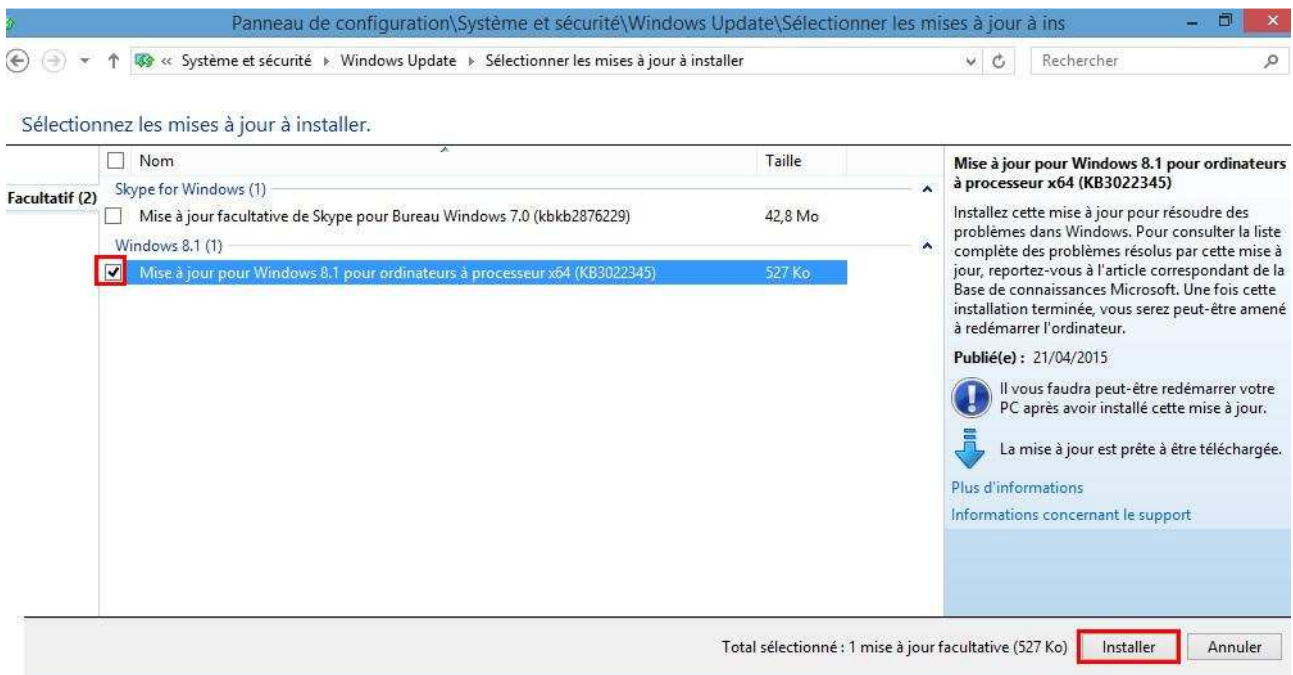
5-2 - Mises à jour automatiques de Windows

Pour accéder aux mises à jour :  + **Panneau de configuration** et cliquer ensuite sur **Windows Update** (sous Windows 8 :  + **W** puis saisir le mot *Update*)

⇒ Un message apparaît qui indique le nombre de mises à jour détectées. Pour installer l'un des correctifs il faut cliquer sur le lien bleu affiché dans le cadre.

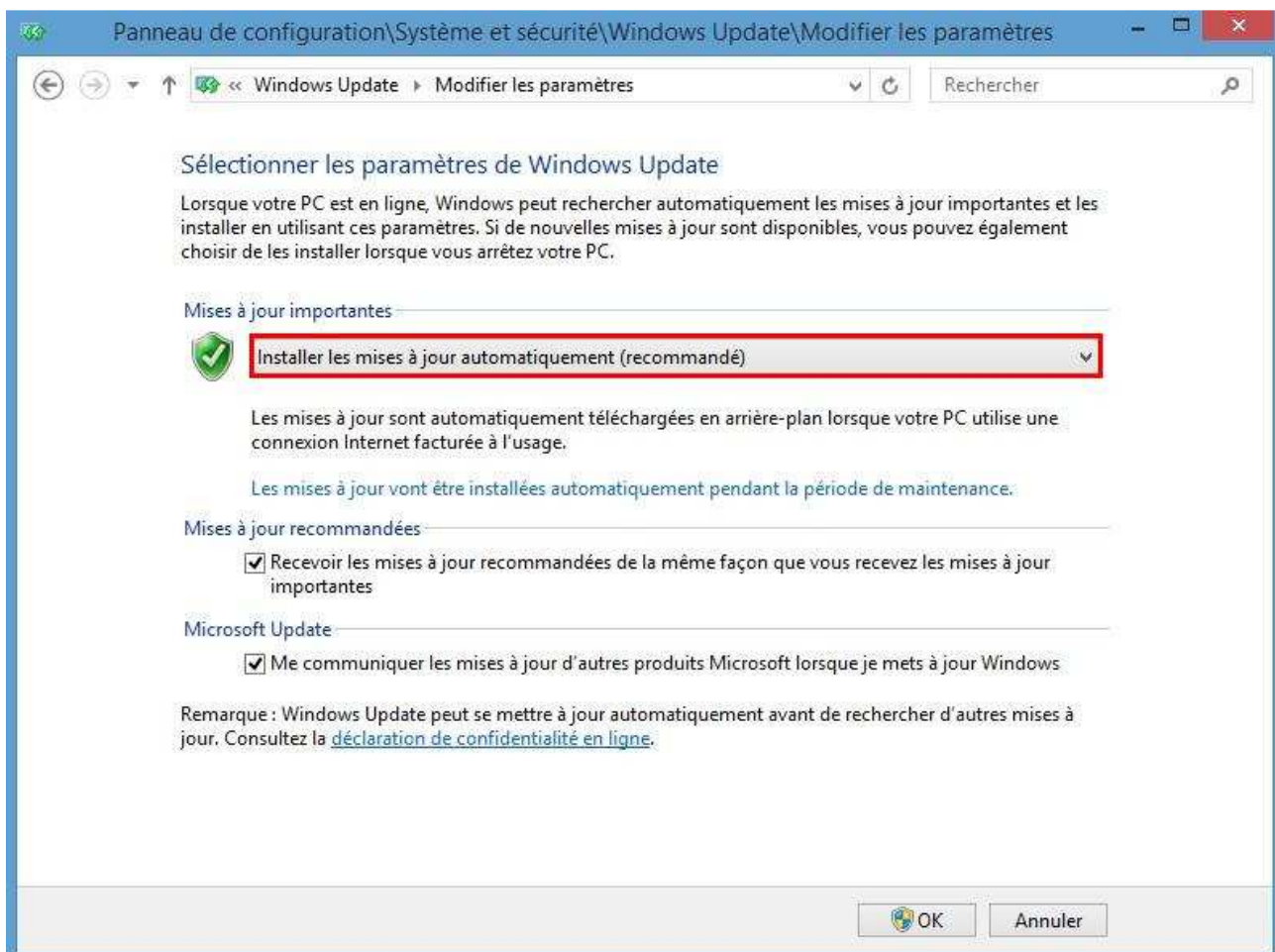


⇒ Cocher les correctifs que vous souhaitez installer puis cliquez sur le bouton **Installer**.



⇒ Finaliser l'installation par un redémarrage de l'ordinateur

Pour paramétrer les mises à jour de Windows Update : sélectionner *Modifier les paramètres*. L'action *Installer les mises à jour automatiquement* doit être sélectionnée. Si ce n'est pas le cas sélectionner cette action et valider par la touche **OK**.



Les mises à jour de sécurité de Windows sont dénommées "mises à jour critiques" par Microsoft.

Ces mises à jour s'effectuent très facilement, mais leur transfert et installation peuvent prendre du temps.

5-3 - Mises à jour des autres logiciels

Il faut veiller à mettre à jour les logiciels liés à la sécurité (antivirus, antimalwares) et ceux qui utilisent Internet : le navigateur, les plugins (java, Adobe Acrobat, Flash,...).

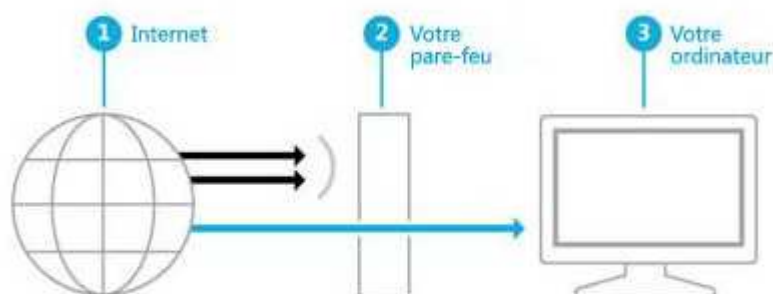
6 – Le Pare-feu Windows

6-1- Configuration essentielle

Un Pare-feu, « Firewall » en anglais, sert à protéger un ordinateur des attaques qui proviennent d'Internet.

Le Pare-feu va agir en bloquant des « portes » d'entrées ou de sorties du PC.



En effet tous les échanges entre l'ordinateur et Internet sont constitués d'innombrables petits paquets de données. Ces paquets passent obligatoirement par le pare-feu qui les filtre. En fonction de leur provenance ou de leur destination le Pare-feu décide de les laisser passer ou non. Pour prendre cette décision, il dispose d'un certain nombre de règles.



Un pare-feu crée un obstacle entre Internet et votre ordinateur

La seule présence d'un Pare-feu ne garantit pas une protection maximale. Il faut que celui-ci soit correctement paramétré et configuré.

Des services en ligne permettent de tester l'efficacité générale d'un Pare-feu en simulant des attaques et en examinant les failles potentielles (voir le chapitre 6-2-2 *Tests*).




Pour accéder au Pare-feu :  + **Panneau de configuration** et cliquer ensuite sur **Pare-feu Windows** (sous Windows 8 :  + **W** puis saisir le mot *pare-feu*)

Le Pare-feu dispose de trois profils :

- *Domaine* : ordinateur intégré dans un réseau d'entreprise (sans objet ici)
- *Privé* : ordinateur connecté à une box d'un opérateur internet (risque informatique modéré)
- *Public* : ordinateur connecté à Internet par connexion 3G ou Wi-Fi dans un espace public (risque informatique élevé)



Page d'accueil du panneau de configuration

Autoriser une application ou une fonctionnalité via le Pare-feu Windows


-  Modifier les paramètres de notification
-  Activer ou désactiver le Pare-feu Windows
-  Paramètres par défaut
-  Paramètres avancés
- Dépanner mon réseau



Protégez votre ordinateur avec le Pare-feu Windows

Le Pare-feu Windows a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.


 Réseaux privés
Connecté 

Réseaux à domicile ou sur un lieu de travail, où vous faites confiance aux personnes et aux périphériques présents sur le réseau




État du Pare-feu Windows :	Activé
Connexions entrantes :	Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées
Réseaux privés actifs :	 Réseau
État de notification :	M'avertir lorsque le Pare-feu Windows bloque une nouvelle application

 Réseaux publics ou invités
Connecté 

Réseaux dans des lieux publics, tels qu'un aéroport ou un cybercafé

État du Pare-feu Windows :	Activé
Connexions entrantes :	Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées
Réseaux publics actifs :	 Réseau non identifié
État de notification :	M'avertir lorsque le Pare-feu Windows bloque une nouvelle application



Le lien *Activer ou désactiver le Pare-feu Windows* permet de modifier le fonctionnement du pare-feu de façon globale.

 > Panneau de configuration > Système et sécurité > Pare-feu Windows > Personnaliser les paramètres  



Personnaliser les paramètres pour chaque type de réseau

Vous pouvez modifier les paramètres de pare-feu pour chaque type de réseau que vous utilisez.

Paramètres des réseaux privés

-  Activer le Pare-feu Windows
 - Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées
 - M'avertir lorsque le Pare-feu Windows bloque une nouvelle application
-  Désactiver le Pare-feu Windows (non recommandé)

Paramètres des réseaux publics

-  Activer le Pare-feu Windows
 - Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées
 - M'avertir lorsque le Pare-feu Windows bloque une nouvelle application
-  Désactiver le Pare-feu Windows (non recommandé)

⇒ Il faut laisser le pare-feu au **niveau configuré par défaut**, c'est-à-dire l'option *Activer le Pare-feu Windows*. Ce mode permet de protéger l'ordinateur tout en autorisant les flux du réseau à destination de programmes préalablement autorisés à entrer dans la machine.

Le mode Désactiver le Pare-feu Windows est fortement déconseillé : dans ce cas l'ordinateur n'est plus protégé.

⇒ La case *Bloquer toutes les connexions entrantes* est adaptée lorsque votre ordinateur est connecté dans un environnement hostile comme une connexion en réseau sans fil (Wi-Fi) dans un lieu public. Ce mode active un bouclier qui protège totalement votre ordinateur du trafic réseau provenant de l'extérieur. Par contre votre ordinateur peut toujours accéder à des ressources réseau (Web, courrier électronique,...).

⇒ Activez la case à cocher *M'avertir lorsque le Pare-feu Windows bloque un programme* si vous voulez être prévenu lorsqu'un programme souhaite modifier le fonctionnement du pare-feu.

6-2- Configuration avancée

6-2-1- Paramètres avancés

On peut créer des règles spécifiques pour le Pare-feu. Elles sont accessibles par le lien « *Paramètres avancés* ». Ces fonctions sont réservées aux utilisateurs très expérimentés. Le lien « *Paramètres par défaut* » permet de revenir à la configuration standard du pare-feu.

6-2-2- Tests

Ces tests ne sont utiles que dans le cadre de la vérification de la sécurité de votre configuration.

Les tests reproduisent les différents types d'attaques que votre ordinateur peut subir régulièrement : scan de port TCP (*Transmission Control Protocol*), attaques chevaux de Troie. Opérées à distance ou directement depuis votre ordinateur, ces simulations permettent de contrôler l'efficacité de votre protection.

Technique 1 : La vérification par scan de ports

Votre ordinateur utilise le protocole de communication TCP/IP (IP : *Internet Protocol*) pour communiquer sur Internet. Ce protocole fonctionne à l'aide de différents ports qui fonctionnent un peu comme des portes pouvant être ouvertes ou fermées.

Chaque port correspond à une utilisation particulière d'Internet : le port 80 est associé au web, les ports 20 et 21 pour le FTP (*File Transport Protocol*) , les ports 25 et 110 sont associés à la messagerie, le port 23 pour telnet (doit être bloqué : informations circulent en clair),...

C'est via ces "portes" que les principales attaques se produisent. Un port ouvert sur l'extérieur est visible pour les pirates et leur permet d'effectuer une tentative d'intrusion par ce biais. Un port fermé est protégé, mais visible par les pirates. Bien que l'ordinateur soit sécurisé, le fait d'être visible peut représenter un risque. Le pirate voyant une machine peut alors cibler une attaque, en espérant trouver une autre vulnérabilité. En revanche, un port masqué est invisible pour tous les autres ordinateurs sur Internet et reste inexploitable pour une intrusion.

Le test va donc "scanner" votre ordinateur à la recherche de ports ouverts ou fermés et vous signaler les entrées accessibles ou visibles par tous. Idéalement, tous les ports doivent être masqués et cela peut prendre du temps dans la mesure où il en existe plusieurs milliers !

Technique 2 : La vérification simulant un programme de type Cheval de Troie ou troyan

Ici, un petit programme inoffensif va reproduire le fonctionnement d'un cheval de Troie et tenter de communiquer des informations à votre insu auprès d'un serveur situé sur Internet. Un pare-feu efficace devrait identifier la menace et interdire la communication de se réaliser. Dans le cas contraire, votre ordinateur court un risque.

Important ! La réussite des tests ne signifie pas que votre ordinateur soit entièrement à l'abri de l'ensemble des menaces d'intrusions. Il s'agit simplement d'un indicateur vous permettant de constater un bon fonctionnement général. Les mises à jour régulières des logiciels (Windows en particulier) et une vigilance permanente sont les meilleures attitudes à adopter.

Testez l'efficacité de votre pare-feu Première partie du test : scan de port

Rendez-vous sur la page suivante : <http://www.zebulon.fr/outils/scanports/> puis cliquez sur « Testez la sécurité de votre PC »

Testez la sécurité de votre ordinateur

Test de firewall : scanneur de ports TCP

Afin de tester la sécurité de votre poste, nous vous proposons d'effectuer ce test. Celui-ci va scanner les ports TCP les plus couramment utilisés. Les résultats seront ensuite interprétés afin de vous aider à déterminer si la sécurité de votre machine est optimale.

Testez la sécurité de votre PC

Une fois le scan terminé, il vous sera indiqué l'état des ports TCP testés : il peuvent être soit ouverts, fermés ou masqués. Le maximum de sécurité étant attend lorsque l'ensemble des ports sont masqués. Pour chacun de ces ports, il vous sera également indiqué les trojans susceptible de l'utiliser.

Afin d'interpréter les résultats du test d'un simple coup d'œil, une icône vous indiquera l'état de sécurité général constaté :



Test effectué avec succès :

Aucun ports détectés



Alerte niveau 1 :

Un ou plusieurs ports détectés comme fermés



Alerte niveau 2 :

Un ou plusieurs ports détectés comme ouverts



Alerte niveau 3 :

Un ou plusieurs ports détectés comme fermés et un ou plusieurs ports détectés comme ouverts

⊕ Le rôle de notre script étant de tester la sécurité de votre machine, il est normal que votre firewall puisse vous avertir d'un scan de vos ports provenant de l'IP 37.59.21.72 de notre serveur. Ce test ne scanne qu'une petite partie des 65536 ports que comporte votre ordinateur. Les ports scannés correspondent à ceux étant les plus susceptibles d'être utilisés par un trojan ou cheval de troie ; en aucun cas la réussite de ce test vous garantie que votre PC est complètement protégé.

⊕ Il est conseillé de désactiver Norton avant de réaliser ce test.

Soyez patient, la procédure peut durer plus d'une minute. A l'issue du test, les résultats identiques à l'illustration ci-dessous seront affichés.

Testez la sécurité de votre ordinateur

Attention ! Il existe un ou plusieurs ports détectés comme fermés !



Un ou plusieurs ports fermés ont été détecté. Bien qu'il soit protégé, un port fermé reste visible, un pirate potentiel peut donc tenter d'attaquer votre machine. Pour plus de sécurité, il est conseillé de masquer ces ports ou de modifier la configuration de votre firewall.

L'Internet par Satellite

Partout en France jusqu'à 22 Méga. Internet, Télé et Téléphone inclus.



Ports TCP ouverts














Aucun port détecté

Ports TCP fermés

113	auth	Utilisé par certains serveurs de messagerie ou de newsgroups (MiRC - Virc...). Des problèmes de performances peuvent survenir si ce port est masqué.	
-----	------	--	--

Ports TCP masqués

21	ftp	Utilisé pour le transfert de fichier entre ordinateurs	
22	ssh	Le shell SSH permet de se connecter à un serveur de façon sécurisée	
23	telnet	Utilisé pour obtenir un shell distant	
25	smtp	Utilisé pour le transfert de courrier électronique entre deux hôtes. Si vous n'utilisez pas de serveur de messagerie, il est conseillé de fermer ce port.	
79	finger	Permet de connaître diverses informations relatives à votre profil	
80	http	Utilisé pour les services Web. Si vous n'utilisez pas de serveur web, il est conseillé de fermer ce port	
110	pop3	Utilisé par les serveurs de messagerie Internet. Si vous n'utilisez pas de serveur de messagerie, il est conseillé de fermer ce port.	
119	nntp	Utilisé par les serveurs de news pour la distribution d'articles Usenet	
135	epmap	Utilisé pour les applications client/serveur basées sur des systèmes d'exploitation Microsoft	
139	netbios-ssn	Utilisé pour le partage de fichiers dans un réseau local	
143	imap	Utilisé par les serveurs de messagerie Internet pour l'envoi de messages électroniques. Si vous n'utilisez pas de serveur IMAP, il est conseillé de fermer ce port.	

389	ldap	LDAP (Lightweight Directory Access Protocol) : utilisé pour accéder automatiquement à des services d'annuaires en ligne	
443	https	Utilisé pour sécuriser les communications HTTP. Si vous n'utilisez pas de serveur web, il est conseillé de fermer ce port. Ce port est également utilisé par AOL Instant Messenger	
445	microsoft-ds	Utilisé pour le partage des protocoles SMB. Son exploitation peut permettre d'obtenir vos mots de passe	
1002	N/A	Port non standard	
1024	N/A	Port réservé	
1025	N/A	Port non standard	
1026	N/A	Port non standard	
1027	N/A	Port non standard	
1028	N/A	Port non standard	
1029	N/A	Port non standard	
1030	N/A	Port non standard	
1720	h323hostcall	Port non standard. Peut être utilisé par NetMeeting	
5000	N/A	Utilisé pour communiquer avec tous les périphériques UpnP reliés à votre réseau	

Cet exemple illustre les trois cas de figure possibles. Trois listes apparaissent, représentant dans l'ordre les ports ouverts, les ports fermés, et les ports masqués. Chaque ligne représente un port particulier (nom et numéro) suivi de la description de l'utilisation du port. Dans la liste des "Ports TCP ouverts" s'il existe un port ouvert cela signifie que ce dernier peut être utilisé pour une attaque. Dans la liste des "Ports TCP fermés" s'il existe un port fermé cela signifie que ce dernier est inaccessible, mais visible. Un pirate peut dans ce cas tenter une attaque sur la machine qu'il voit, en cherchant une autre vulnérabilité. Dans la liste des "Ports TCP masqués", cela signifie que le port est fermé et invisible, et donc complètement sécurisé. Si tous les ports sont masqués, le PC est invisible.

Seconde partie du test : attaque d'un cheval de Troie

Il s'agit ici de télécharger une petite application et de l'exécuter directement sur votre ordinateur pour reproduire l'attaque d'un cheval de Troie.

Téléchargez l'application suivante leaktest.exe (25 ko) depuis le site <https://www.grc.com/it/leaktest.htm> et enregistrez-la sur votre disque dur.

Lancez l'application leaktest.exe et la fenêtre suivante s'ouvre. Cliquez sur le bouton « *Test for Leaks* ».



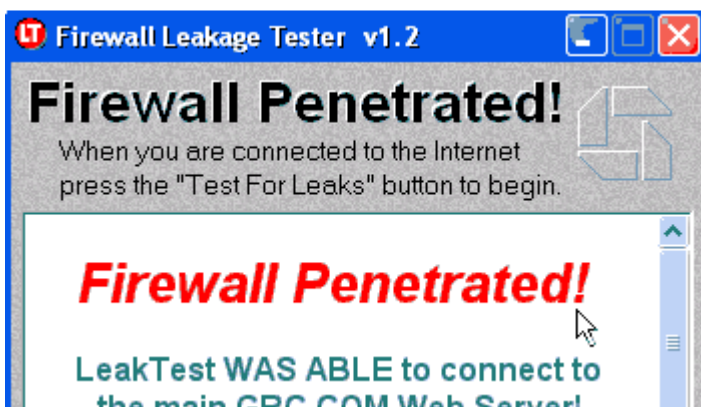
Le programme va tenter d'entrer en communication avec un serveur distant et de lui communiquer des informations à votre insu. Aucune information personnelle ne sera transmise pendant le déroulement de l'opération.

Durant le test, votre pare-feu devrait normalement vous indiquer qu'un programme tente de forcer une communication. N'autorisez donc aucune action pendant le test.

Si le test est réussi, et qu'aucune communication n'a pu être établie, le message suivant est affiché.



Dans le cas contraire, et si le programme a pu passer au travers du pare-feu, c'est l'écran suivant qui devrait s'afficher.



Cet écran signifie que le Pare-feu n'a pas joué son rôle de contrôle des communications sortantes.

En conclusion

La réussite de ces tests ne signifie pas la sécurité totale de votre ordinateur. Cela étant, en fonction des résultats, vous pourrez constater que votre Pare-feu fonctionne correctement vis-à-vis des attaques les plus répandues.

En revanche, toute faille signalée est à considérer ici comme un risque éventuel pour la sécurité de votre ordinateur.

Remarque : il existe un Pare-feu au niveau de la box.

7 - Sécurité et connexion WI-FI

La connexion à Internet par Wi-Fi (**Wireless Fidelity**) s'effectue par ondes radio.

Cette connexion présente plusieurs risques :

- ⇒ un pirate informatique, à proximité, pourrait « écouter » le réseau et tenter d'intercepter les données diffusées (le « wardriving »).
- ⇒ un tiers pourrait utiliser la connexion Wi-Fi de votre box (en cas d'utilisation illégale vous risqueriez d'être pénalement responsable).

→ Il faut donc s'assurer que vous utilisez une connexion Wi-Fi sécurisée

Pour en savoir plus : site de l'ANSSI lien <http://www.ssi.gouv.fr/particulier/bonnes-pratiques/liaisons-sans-fil-et-mobilite/>

7 – 1 – Configuration de votre box

Les box actuelles sont maintenant bien sécurisées. Les informations indiquées ci-dessous concernent essentiellement une vérification de leurs paramètres.

Pour se connecter à l'interface de sa box taper **http://192.168.1.1** dans son navigateur. Se connecter ensuite avec l'identifiant **admin** et le mot de passe indiqué dans le manuel d'utilisation de la box (si le mot de passe est aussi admin il faudra le modifier).

7 -1 - 1- Désactivation / Activation de la connexion Wi-Fi

Si vous n'utilisez pas la connexion Wi-Fi, c'est à dire si la connexion à Internet s'effectue à l'aide d'un câble Ethernet et que vous ne vous servez pas d'appareils avec liaison sans fil, vous pouvez désactiver le Wi-Fi au niveau de la box. Soit par un bouton situé sur la box (voir le manuel d'utilisation), soit au niveau du paramétrage de la box en étant connecté en **admin**. Pour réactiver le Wi-Fi procéder de la même façon.

Exemple sur une Livebox d'Orange :

admin: [déconnexion](#)

français

mon réseau **mon WiFi** mon téléphone assistance configuration avancée

paramètres WiFi [mon WiFi](#) > paramètres WiFi

WiFi Avancé

WiFi

Vous pouvez configurer l'accès au WiFi

état de la connexion WiFi	désactivé activer	
	définir les plages d'activation du WiFi	
réseau	WiFi 2,4 GHz	WiFi 5 GHz
nom du réseau WiFi (SSID)	Livebox	Livebox
clé de sécurité	C2867FE71867C167186F854C59	C2867FE71867C167186F854C59
type de WiFi activé		

aide

Activer/désactiver le WiFi
Si votre réseau n'est muni d'aucun appareil sans fil, il est conseillé de désactiver le WiFi

Nom du réseau WiFi (SSID)
Vous pouvez modifier le nom du réseau WiFi de votre Livebox pour le personnaliser

Définir les plages d'activation de mon WiFi
Par défaut, votre WiFi est activé en permanence (7j/7 et 24h/24h), vous pouvez définir des jours et plages horaires d'activation de votre WiFi en cliquant sur "définir les plages d'activation du WiFi"

7- 1- 2 - Changer le mot de passe de sa box

Les box sont livrés avec un mot de passe en principe personnalisé (sur les box Orange les 8 premiers caractères de la clé de chiffrement). Cependant sur les anciennes box, ou si vous devez réinitialiser les paramètres de la box, le mot de passe est **admin**. Il conviendra dans ce cas de le changer.

Exemple changement de mot de passe sur une Livebox d'Orange :

français

mon réseau mon WiFi mon téléphone assistance **configuration avancée**

configuration [configuration avancée](#) > administration

réseau

configuration pare-feu

accès à distance

utilisateur

connexion à Internet

administration

administration

modifier le mot de passe d'administration de la Livebox

compte d'administration : admin

mot de passe courant :	<input type="text"/>
nouveau mot de passe :	<input type="text"/>
confirmation du nouveau mot de passe :	<input type="text"/>

7 – 1 – 3 - Nom du réseau Wi-Fi

L'identifiant réseau (aussi appelé SSID).est le nom de la connexion réseau de votre box. Dans l'exemple du chapitre 7-1-1 il s'agit de **Livebox**. Le nom par défaut donne des informations aux éventuels pirates sur votre type de box et sa configuration.

Vous pouvez remplacer ce nom par celui que vous voulez. Il faut éviter de mettre un nom évident (nom personnel, adresse,...). Bien noter ce nom.

7 - 1 - 4 - Clé de sécurité pour se connecter

Le principe est de chiffrer la communication entre votre ordinateur et la box (le routeur Wi-Fi).

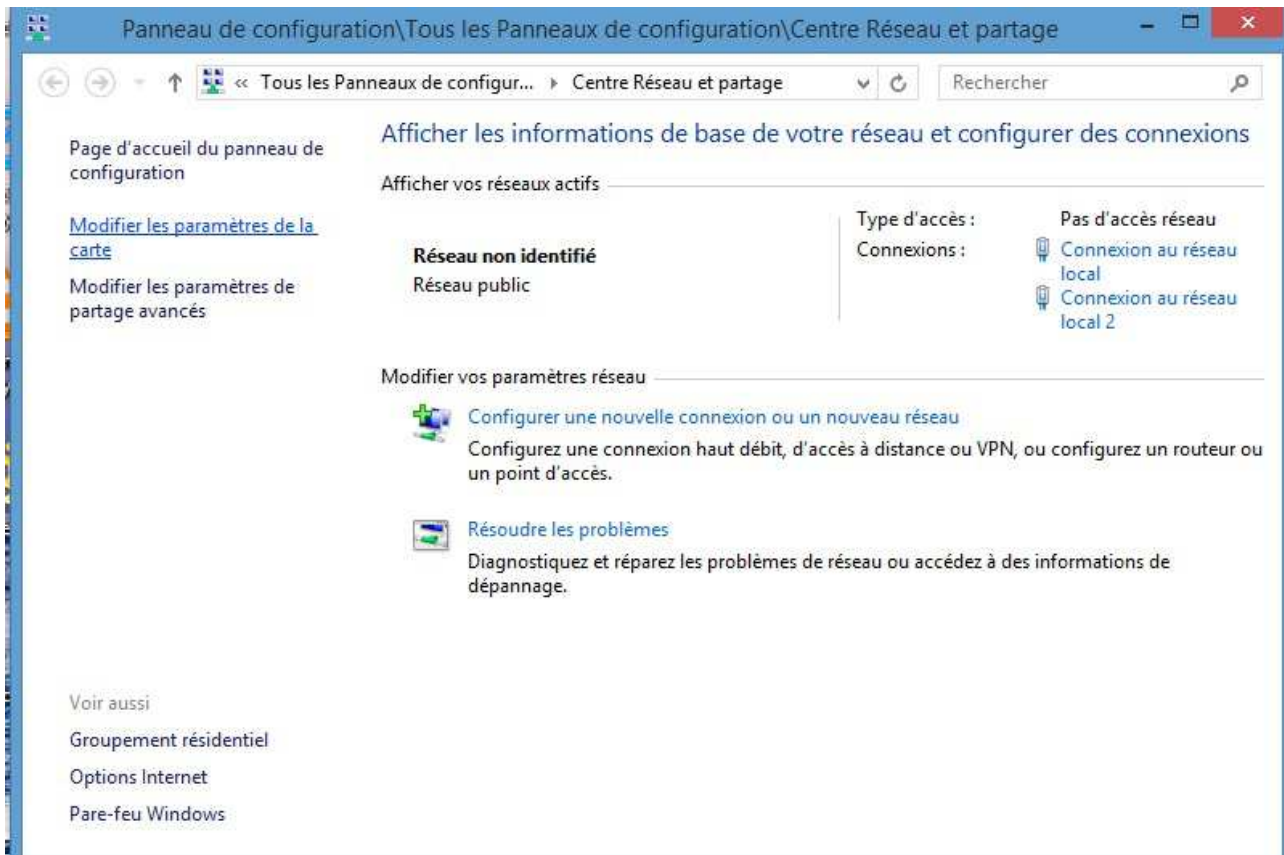
Il existe plusieurs normes pour chiffrer la communication Wi-Fi: le WEP, le WPA, le WPA2. Ils sont intégrés à votre box et par défaut c'est le WPA ou le WPA2 qui est utilisé.

Attention! Ne pas utiliser le WEP car il n'est pas fiable (la clé de chiffrement peut être "cassée" en moins d'une minute).

Il est possible de modifier la clé de sécurité (voir l'accès au chapitre 7-1-1)

7 – 2 – Configuration Wi-Fi dans Windows

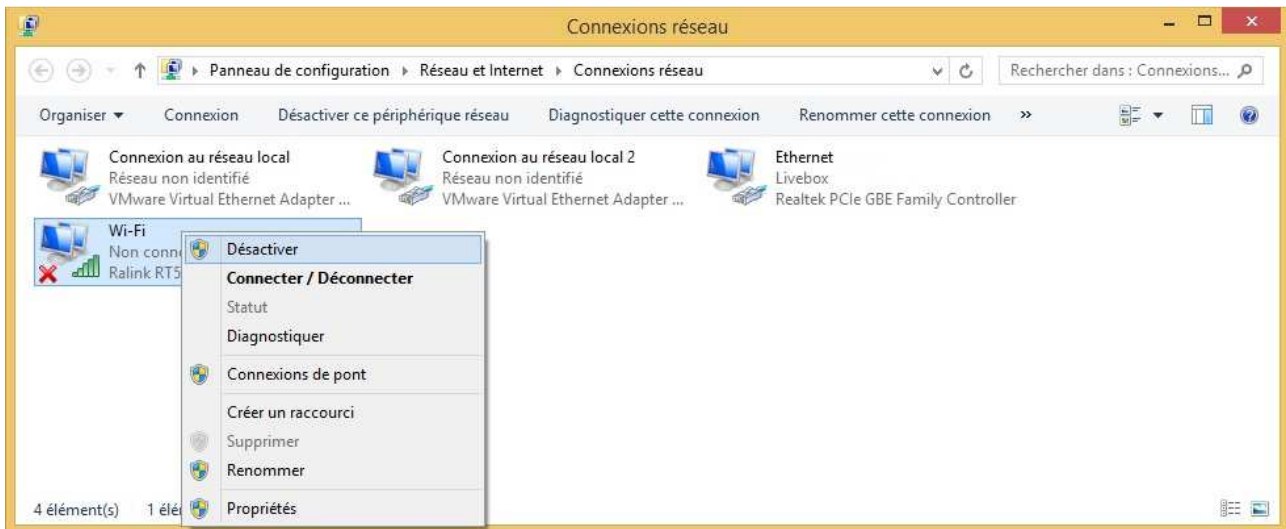
Pour accéder au Centre réseau et Partage :  + **Panneau de configuration** et cliquer ensuite sur **Centre réseau et Partage** (sous Windows 8 :  + **W** puis saisir *Centre réseau et Partage*)





7 - 2 - 1 - Désactivation et activation de la connexion Wi-Fi

Si la connexion à Internet est réalisée à l'aide d'un câble Ethernet et que vous n'utilisez aucun appareil avec liaison sans fil vous pouvez désactiver le Wi-Fi au niveau de *Modifier les paramètres de la carte réseau* dans le **Centre réseau et Partage**

- cliquer sur *Modifier les paramètres de la carte* (ou *Gérer les connexions réseau* sous Vista)
- clic droit sur le *Wi-Fi* et sélectionner *Désactiver* (idem pour l'*Activer*)

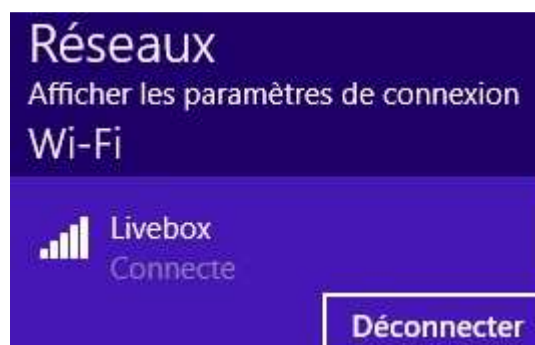


7 - 2 - 2 - Se connecter à un réseau Wi-Fi sécurisé

Pour vous connecter à un réseau Wi-Fi:  + **Panneau de configuration** et cliquer sur **Centre réseau et Partage** puis **Connexion à un réseau** (depuis Windows 8:  + **W** puis saisir le mot *réseau*, cliquer sur **Connexion à un réseau**)

- cliquer sur le bouton *Connecter* (ou *Connexion*)
- indiquer *la clé sécurité réseau*

Pour se déconnecter il faudra cliquer sur *Déconnecter*

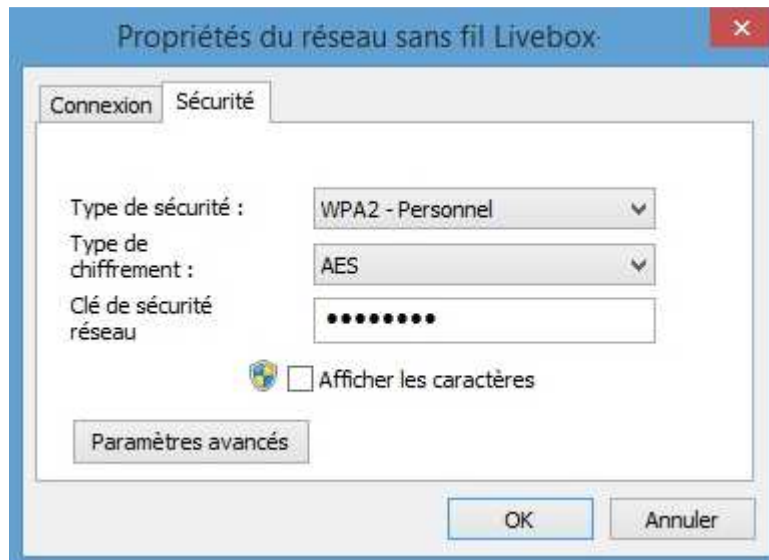


Attention si le WEP est utilisé la communication peut-être facilement interceptée par un pirate informatique (voir le chapitre 7-1-4).

7 - 2 - 3 – Afficher la clé de sécurité réseau

Pour afficher la clé aller dans *Modifier les paramètres de la carte réseau* (ou *Gérer les connexions réseau*) dans le **Centre réseau et Partage**

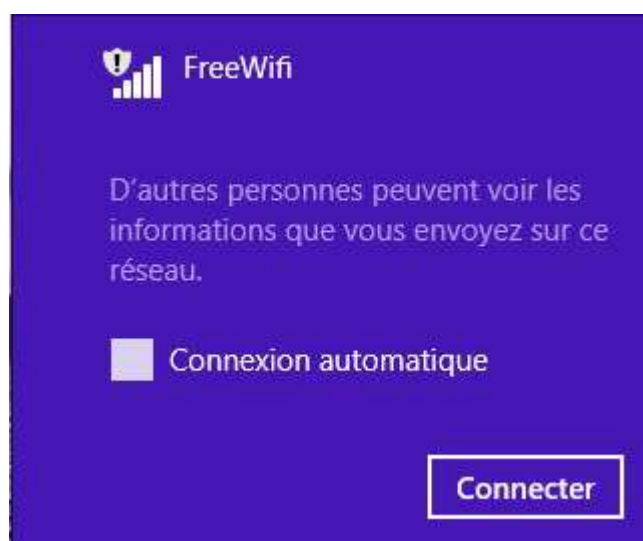
- cliquer sur *statut*
- clic sur le bouton *Propriétés sans fil*
- onglet *Sécurité*
- en cliquant sur *Afficher les caractères* la clé s'affiche en clair



7 - 2 - 4 – Eviter de se connecter à un réseau Wi-Fi ouvert

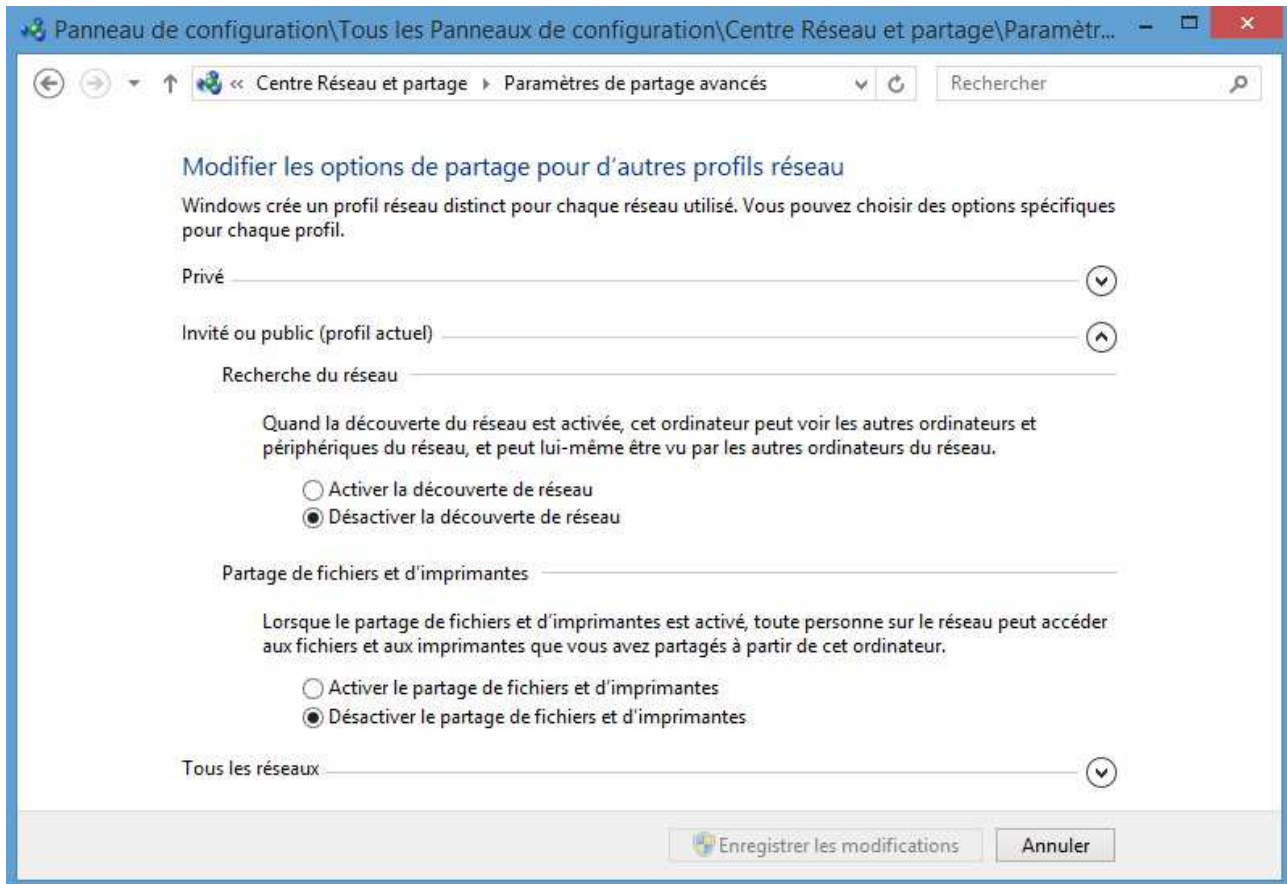
Il faut être particulièrement vigilant si vous vous connectez à un réseau wi-fi public (aéroport, hôtel, restaurant,...), c'est-à-dire non chiffré (sans clé). En effet les informations circulent en clair et un pirate serait susceptible de les capturer (technique dite du sniffing) : identifiants, mots de passe, données personnelles,...

Si vous êtes connectés sur ce type de réseau n'effectuer pas d'opérations sensibles, comme la consultation de comptes bancaires, mais uniquement des actions standards. Exemple: recherche d'informations sur Internet.



Il convient aussi de s'assurer que le réseau wi-fi public auquel vous voulez vous connecter correspond bien à celui affiché: un pirate informatique pourrait très bien avoir créé un point d'accès wi-fi avec un nom proche de celui recherché.

Dans un réseau wi-fi public il faut vérifier que le *Partage de fichiers et d'imprimantes* soit bien désactivé. L'accès s'effectue dans le **Centre réseau et Partage** par le lien *Modifier les paramètres de partage avancés* (ou *Partage et découverte* dans Vista)



7 – 3 – Alerte de sécurité sur la connexion Wi-Fi

Une vulnérabilité dans le protocole WPA/WPA2 vient d'être découverte. Elle a fait l'objet d'une alerte sur le site de l'ANSSI depuis le 16/10/2017 : voir <https://www.cert.ssi.gouv.fr/alerte/CERTFR-2017-ALE-014/>

Dans cette alerte il est indiqué qu'un attaquant pourrait intercepter la clé de chiffrement (la clé de sécurité réseau) lors d'une connexion Wi-Fi si le pirate était peu éloigné de l'appareil connecté. L'attaquant pourrait alors accéder à des informations sensibles: numéros de cartes bancaires, mots de passe, e-mails, photos,... Il pourrait aussi introduire dans le système un virus de type rançongiciel.

Tous les types d'appareils connectés en Wi-Fi sont concernés, notamment les ordinateurs et smartphones sous Windows, Linux, Apple, Android.

L'ANSSI recommande de bien mettre à jour les systèmes qui se connectent à un réseau Wi-Fi.

7 – 4 – Ondes électromagnétiques et possibles effets sur la santé

Téléphones portables, Wi-Fi, antennes relais, fours à micro-ondes et autres équipements bluetooth : les ondes électromagnétiques sont partout. A ce jour, leurs effets sur la santé ne sont pas précisément connus mais l'OMS reconnaît désormais que les radiofréquences sont de possibles cancérigènes. Sans chercher à ne pas les utiliser il semble judicieux de prendre certaines précautions.

Le téléphone portable est une source importante d'ondes électromagnétiques. Pour réduire votre exposition, il est donc important d'optimiser son utilisation. Pour cela, téléphonez uniquement dans les zones de bonne réception et évitez de l'utiliser en voiture, dans le train, etc... En effet le champ électromagnétique est particulièrement puissant lorsque le téléphone capte mal son réseau. La réglementation française impose que le DAS (Débit d'Absorption Spécifique) des téléphones mobiles ne dépasse pas 2 W/kg. La valeur du DAS d'un téléphone portable est précisée dans la notice constructeur.

Concernant le Wi-Fi l'intensité qu'il émet peut être jusqu'à 6 fois moins importante que les téléphones portables. Par précaution si vous n'utilisez pas le Wi-Fi, dans le cas d'une connexion à Internet réalisée à l'aide d'un câble Ethernet, vous pouvez désactiver le Wi-Fi.



8 - Sauvegarder de vos données

Par sécurité nous vous rappelons qu'il faut effectuer régulièrement des sauvegardes de ses données (sur un disque dur externe par exemple, dans le cloud). En effet en cas de problèmes graves (panne matériel, problème informatique, virus) cette sauvegarde seule permettra de récupérer ses données si une réinstallation système s'avérait nécessaire.

9 - Comptes utilisateurs

Il faut éviter de travailler avec un compte *Administrateur* mais plutôt utiliser un compte *Standard* (droits limités)

Pour créer un compte avec des droits limités (type *standard*) il faut :

- se connecter avec un compte de type *Administrateur*
- accéder à l'écran des *Comptes d'Utilisateurs* :  + **Panneau de configuration** et cliquer ensuite sur **Comptes d'Utilisateurs** (sous Windows 8 :  + **W** puis saisir *Comptes d'Utilisateurs*)



- cliquer sur le lien « *Gérer un autre compte* »
- Ajouter un utilisateur dans les paramètres de l'ordinateur
- cliquer sur *Ajouter un compte d'utilisateur*
- Choisir *Compte local* si le système le propose
- Saisir un nom et un mot de passe

Par défaut ce compte sera considéré comme « *utilisateur standard* ». C'est avec celui-ci qu'il conviendra d'utiliser l'ordinateur.

10 - Mails

10 – 1 – Quelques précautions pour lire vos mails

La messagerie est un vecteur très important pour les attaques informatiques. Quelques règles s'imposent pour lire vos courriels :

- ⇒ N'ouvrez jamais les e-mails dont vous ignorez l'origine, même si l'objet est attirant et qu'il est noté comme important (produits gratuits, gain d'argent, remboursement, recrutement, demande d'aide,...).
- ⇒ Ne communiquez jamais d'informations personnelles (mots de passe, coordonnées, date de naissance, adresse, codes personnels, etc.)
- ⇒ Appliquez quelques contrôles simples :
 - *L'e-mail est-il en français ? Est-il en anglais ?*
 - *Si le message est en français, contient-il des caractères bizarres ?*
 - *Le contenu vous semble-t-il tout à fait intelligible, cohérent ?*
 - *Connaissez-vous l'émetteur ?*
 - *Etes-vous réellement dans la liste des destinataires ?*
 - *Etes-vous réellement concerné ?*
 - *S'il existe une pièce jointe est-elle d'un type à risque ?*
 - *Existe-t-il un lien vers un site internet ?*

Suivant le type de réponses, prenez vos précautions, le message peut contenir un virus ou bien être du « phishing » (voir le chapitre 10-2). **Au moindre doute il faut supprimer le message.**

10 – 2 – Le Phishing ou Hameçonnage

Le Phishing ou Hameçonnage est une technique de tromperie sur Internet qui consiste à faire croire à l'utilisateur qu'il est connecté à un site, qu'il utilise habituellement, dans le but de lui soutirer des informations personnelles (date de naissance, identifiant de comptes bancaires, mots de passe, numéro de cartes bancaires,...). Les adresses Internet (URL : *Uniform Resource Locator*) de phishing ressemblent à des adresses de sites authentiques.

Pour convaincre l'utilisateur de se rendre sur ce type de site les pirates utilisent des e-mails ressemblant à ceux qui pourraient être envoyés par l'organisme du site visé avec présence d'un lien qui va rediriger l'utilisateur sur le faux site.

Méfiez-vous systématiquement des e-mails demandant des informations personnelles, souvent avec un caractère d'urgence, émanant de certaines Administrations (Impôts, Assurance Maladie,...), de votre banque, d'EDF,.... . Ce type de demandes peut se faire aussi par appels téléphoniques ou SMS.

Les raisons invoquées pour extorquer des informations relèvent généralement de la sécurité de vos données personnelles. Quelques exemples :

- « *Un problème technique nous oblige à ...* »
- « *Une mise à jour de sécurité va améliorer ...* »
- « *Un intrus a tenté de s'introduire sur vos comptes en ligne...* »

D'autres raisons concernent des remboursements à effectuer, avec demande du numéro de la carte bancaire par exemple.

Afin de rendre plus crédible le message, certains vont même jusqu'à donner des conseils antiphishing ! Ils précisent qu'il ne faut jamais divulguer d'informations confidentielles par e-mail et vous invitent à vous rendre sur leur site sécurisé pour vérifier vos données (par exemple le numéro de carte bancaire, le numéro de compte, le code d'accès, la date de naissance, etc..).

⇒ **Pour s'assurer de l'authenticité des messages**

- Ne cliquez sur aucun des liens si vous avez un doute.
- Tapez vous-même l'adresse Internet dans le navigateur ou contactez la société par téléphone.
- Ne renseignez pas les informations personnelles demandées par ces messages.
- Ne renseignez ce type d'information que sur un site Web sécurisé (il doit commencer par **https://**, mais quelques rares sites frauduleux commencent aussi par **https**).
- Considérez qu'un message (e-mail, message téléphonique, SMS, ...) donné dans une langue qui n'est pas celle habituellement utilisée par l'émetteur, est un faux.
- N'appellez pas un serveur vocal que l'on vous aura demandé de rappeler par e-mail ou par un message téléphonique si vous ne connaissez pas ce numéro (souvent le numéro est surtaxé).
- Ne tapez pas vos codes d'accès sur un téléphone, si les opérations que vous voulez effectuer sur ce serveur vocal ne sont pas de votre propre initiative.

Si vous avez un doute sur l'authenticité d'un message contacter directement l'organisme sensé vous l'avoir envoyé (par téléphone par exemple).

⇒ Vous pouvez utiliser des fonctions antiphishing de votre navigateur :

- Netcraft (gratuit) est un puissant outil de lutte contre le phishing (<http://www.toolbar.netcraft.com>)

11 - Se connecter sur des sites internet sûrs

Quand vous naviguez sur Internet il faut éviter tous les sites à risque : sites de téléchargement de films, de musique, de jeux gratuits,....

Si le pare-feu bloque l'action d'un site suivre les recommandations du pare-feu (laisser bloquer l'accès à votre système).

Il ne faut accéder qu'à des sites sûrs.

12 - Mots de passe

12 – 1 – Le processus d'authentification

Le processus d'authentification s'établit en deux étapes :

- Identification : présenter un identifiant au système (par exemple un nom d'utilisateur)
- Vérification : présenter ou générer une information d'authentification qui prouve le lien entre le système et l'identifiant (le mot de passe)

12 – 2 – Le mot de passe

En général l'identifiant n'est pas secret et la sécurité ne repose plus que sur le mot de passe.

Les mots de passe sont habituellement stockés sur l'ordinateur après avoir été transformés par un processus de « hachage » à sens unique. Avec Windows le mot de passe « haché » est stocké dans la base SAM dans le dossier c:\windows\system32\config (SAM: Security Account Manager ou gestionnaire des comptes de sécurité).

La vérification du mot de passe s'effectue en « hachant » le mot de passe donné par l'utilisateur et en le comparant avec la version originale conservée sur la machine.

12 – 3 – Attaques des mots de passe

⇒ Ne jamais communiquer son mot de passe à quiconque

⇒ Ne pas écrire son mot de passe à proximité du l'ordinateur

⇒ Ne pas utiliser des mots de passe simples: mots du dictionnaire, noms, prénoms, adresse, date de naissance, numéro sécurité sociale, même série de lettres ou de chiffres (11111), suite de nombres évidente (123456789), peu de caractères.....

→ Il existe des programmes pour "craquer" les mots de passe : exemple le logiciel *Cracker*
- il utilise tous les mots du dictionnaire (il essaie 1 million de mots en 1 seconde)
- il utilise différentes techniques (substitution de chiffres aux lettres, substitution de caractères de contrôle aux lettres, inversion des lettres dans un mot, combinaison sur le nom de l'utilisateur)

→ Il existe des virus qui enregistrent les touches que vous utilisez (keyloggers)

12 – 4 – Choisir un « bon » mot de passe

Il faut choisir un mot de passe difficile à découvrir et le garder secret.

Quelques principes : pas de mots de passe simples (voir chapitre 12-3), 8 caractères minimum, au moins une majuscule, une minuscule, un chiffre.

Pour changer de mot de passe pour un utilisateur de type « standard » : Ctrl + Alt+ Supr puis « Modifier un mot de passe ».

Il existe des sites qui génèrent des mots de passe « solides ».

Exemple : sur le site de Norton

<https://identitysafe.norton.com/fr/password-generator>