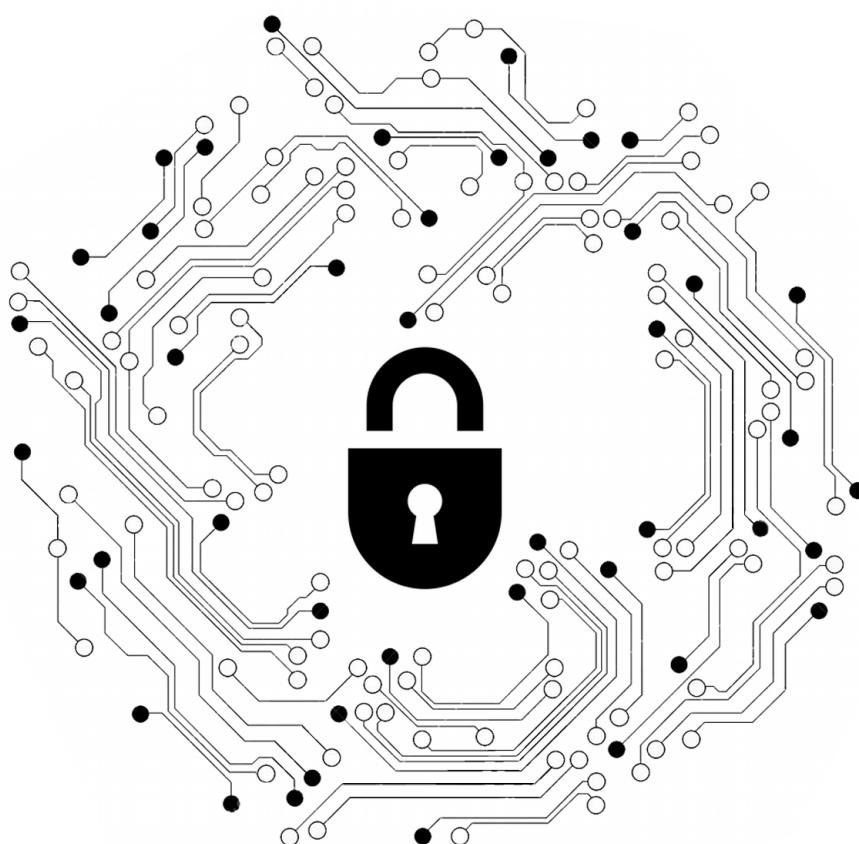


Surveillance Self-Defense

Boîte à Outils



Cette boîte à outils, inspirée du site *Security in a box*, a été créée dans le cadre des ateliers *Surveillance Self Defense* organisés par le *Gsara asbl* en vue de sensibiliser à la protection des données en ligne.

<SOMMAIRE>

PROTEGER SON ORDINATEUR	2
> LUTTER CONTRE LES VIRUS ET LES LOGICIELS ESPIONS	2
// ANTIVIRUS	2
AVAST!	
// ANTI-MOUCHARD	4
SPYBOT SEARCH & DESTROY	
TEATIMER	
// PARE-FEU	6
COMODO FIREWALL	
> CREER UN MOT DE PASSE SOLIDE	8
> UTILISER DES LOGICIELS LIBRES	10
FRAMASOFT	
PROTEGER SES ECHANGES	11
> FAIRE PREUVE DE VIGILANCE	11
PRIVACY BADGER	
CCLEANER	
> SECURISER SES EMAILS	13
MOZILLA THUNDERBIRD	
> SECURISER SA MESSAGERIE INSTANTANEE	15
PIDGIN	
OFF-THE-RECORD (OTR)	
> SECURISER SON VOIP	18
JITSI	

</SOMMAIRE>

ETAPE 1

PROTEGER SON ORDINATEUR

Quels réflexes adopter pour une utilisation responsable de son ordinateur dans le monde numérique ?

> LUTTER CONTRE LES VIRUS ET LES LOGICIELS ESPIONS

Des virus et logiciels espions peuvent collecter nos données et endommager notre ordinateur. Antivirus, anti-mouchard et pare-feu sont trois types de programmes qui empêchent l'infection de notre machine.

// ANTIVIRUS



avast! est un programme antivirus complet compatible avec Windows qui sert à détecter et éliminer les virus et logiciels malveillants de notre ordinateur. Le programme est gratuit dans le cadre d'une utilisation non commerciale mais la copie doit être enregistrée après l'installation, sinon elle expire au bout de 30 jours. L'enregistrement permet de recevoir automatiquement les mises à jour du programme et des définitions de virus. Des mises à jour régulières sont essentielles afin de protéger efficacement notre ordinateur des nouveaux virus.

Note : S'assurer de ne pas avoir deux programmes antivirus installés et actifs simultanément. Si l'on utilise un programme que l'on souhaite changer pour *avast!*, il faut d'abord désinstaller l'autre programme antivirus avant d'installer *avast!*.

Comment télécharger *avast!* :

- Cliquer sur le lien suivant pour ouvrir la page de téléchargement : <https://www.avast.com/fr-fr/index>.
- Cliquer sur le bouton « Télécharger » au bas de la colonne *Antivirus Gratuit*, puis cliquer sur le lien « Télécharger gratuitement » qui s'affiche sur la prochaine page.
- Cliquer sur « Enregistrer le fichier » pour sauvegarder le fichier *setup_av_free_fre.exe* sur son ordinateur.


Comment installer *avast!* :

- Double-cliquer sur « *setup_av_free_fre.exe* » pour lancer l'installation du programme.
- Cliquer sur « Exécuter » pour activer la barre de progression du décompactage, qui peut prendre jusqu'à une minute, selon la vitesse de l'ordinateur. Cliquer ensuite sur « Suivant ».
- Lors du processus d'installation d'*avast!*, la fenêtre d'installation s'affiche avec l'option

Participer à la communauté avast! automatiquement sélectionnée. Pour des raisons de sécurité et de confidentialité, il est préférable de désactiver cette option. Cliquer ensuite sur « Suivant ».

- La fenêtre *avast! recommande* s'affiche avec l'option *Oui, installer le navigateur Google Chrome* automatiquement sélectionnée. Il est préférable de désactiver cette option aussi. Cliquer ensuite sur « Suivant ».
- Un message s'affiche après quelques minutes pour indiquer que le processus d'installation est terminé. Cliquer sur « Fin » pour finaliser le processus d'installation du logiciel. Quelques secondes plus tard, une icône *avast!* apparaît dans la *Barre d'état système*.

Comment enregistrer *avast!* :

- Cliquer sur  pour afficher la fenêtre principale d'*avast!*.
- Cliquer sur « Enregistrez-vous maintenant » (par les menus *Maintenance* et *Enregistrement*).
- Cliquer sur « S'enregistrer ». Le formulaire d'enregistrement d'*avast!* antivirus gratuit s'affiche. Les seuls champs obligatoires sont le *Nom* et l'*E-mail*. Ils sont identifiés par des astérisques. Les autres champs sont facultatifs.
- Saisir son nom et son adresse de courriel dans les champs appropriés, puis cliquer sur « Enregistrer pour obtenir la licence gratuite ».
- Cliquer sur « OK » pour afficher le panneau *Votre enregistrement* dans la fenêtre principale du programme. S'il est écrit *État actuel : enregistré*, *avast !* a été correctement installé.
- Après avoir installé et enregistré *avast!*, on peut supprimer l'exécutable d'installation de son ordinateur.

Autres programmes compatibles avec GNU Linux, Mac OS et/ou Microsoft Windows

Bien qu'*avast!* soit recommandé, il existe d'autres programmes compatibles avec Microsoft Windows qui valent également la peine de s'y intéresser :

- [Avira AntiVir Personal Edition](#)
- [AVG Anti-Virus](#)

Quant aux systèmes d'exploitation *GNU Linux* et *Mac OS*, même s'ils sont pratiquement épargnés des parasites, il existe plusieurs bonnes raisons pour y installer des programmes contre les virus et malwares. Ainsi, même si notre propre système est protégé, nous pouvons répandre des virus à notre insu. Par ailleurs, ces systèmes d'exploitation ne seront peut-être pas épargnés indéfiniment.

À l'heure actuelle, il n'existe aucun programme antivirus gratuit que nous pourrions recommander pour *Linux* et *Mac OS*. Cependant, il existe plusieurs produits commerciaux qui présentent de nombreux avantages et une excellente protection. Voici la liste des programmes les plus populaires :

- [avast!](#)
- [Kaspersky](#)
- [Mcafee](#)
- [Sophos](#)
- [Symantec](#)

// ANTI-MOUCHARD

Spybot Search & Destroy est un programme libre et gratuit dont l'usage est très répandu pour détecter et éliminer des systèmes informatiques, divers types de logiciels publicitaires (*adware*), malveillants (*malware*) ou espions (*spyware*). Le programme nous permet également de vacciner notre système contre ces logiciels avant même qu'ils n'infectent notre ordinateur.



Le terme « logiciel publicitaire » (ou publiciel ; *adware* en anglais) désigne tout logiciel qui affiche des publicités sur notre ordinateur. Certains types de publiciels fonctionnent sensiblement comme des logiciels espions et peuvent envahir notre vie privée ou menacer la sécurité de notre système.

Le terme « logiciel malveillant » (*malware* en anglais) désigne tout programme – par exemple des Chevaux de Troie (*Trojans*) ou des vers informatiques (*worms*) – conçu pour nuire à notre ordinateur ou en détourner les opérations sans notre consentement, ou sans même que nous en soyons conscients.

Le terme « logiciel espion » (ou mouchard ; *spyware* en anglais), désigne tout programme conçu pour récolter des données, observer et enregistrer nos renseignements privés et surveiller nos habitudes de navigation sur Internet. Tout comme les logiciels malveillants, les mouchards s'exécutent souvent sur notre ordinateur à notre insu.

L'installation d'un programme comme *Spybot* permet de protéger notre système et notre vie privée. *Spybot* installe aussi une application supplémentaire appelée **TeaTimer**. Cette application protège notre ordinateur contre d'éventuelles infections par des logiciels malveillants.

Note : *Windows Vista* comporte son propre programme anti-espion, appelé *Windows Defender*. Il est tout aussi efficace. Si vous en êtes satisfaits et que vous n'avez pas eu de soucis avec divers logiciels mentionnés ci-dessus, alors laissez-le. *Windows Vista* semble laisser *Spybot* fonctionner sans conflit.

Comment télécharger *Spybot* :

- Cliquer sur le lien *Spybot* ci-dessous pour ouvrir la page de téléchargement : <http://www.safer-networking.org/fr/mirrors/>
- Choisir une source de téléchargement parmi celles listées sur cette page en cliquant sur le bouton « Téléchargement ici ».
- Télécharger le programme d'installation et l'enregistrer-le sur son ordinateur.

Comment installer *Spybot* :

- Double-cliquer sur le programme pour lancer l'installation. Si la boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, cliquer sur « Exécuter ».
- Choisir une langue et cliquer sur « OK » pour afficher la fenêtre *Installation - Spybot Search & Destroy – Bienvenue dans l'assistant d'installation de Spybot - Search & Destroy*.
- Cliquer sur « Suivant » pour afficher la fenêtre *Accord de licence*. Lire l'*Accord de licence* avant de poursuivre le processus d'installation.
- Cocher l'option *Je comprends et j'accepte les termes du contrat de licence* pour activer le

bouton *Suivant*, puis cliquer sur « Suivant » pour afficher la fenêtre *Dossier de destination*.

- Cliquer sur « Suivant » pour afficher la fenêtre *Composants à installer*.
- Cocher toutes les composantes sauf *Icônes pour malvoyants* et *Explorer file scan plugin* et cliquer ensuite sur « Suivant » pour afficher la fenêtre *Sélection du dossier de menu Démarrer*.
- Cliquer sur « Suivant » pour accepter l'emplacement par défaut et afficher la fenêtre *Tâches supplémentaires*.
- Cliquer sur « Suivant » pour afficher la fenêtre *Prêt à installer*, puis cliquer sur « Installer » pour afficher la fenêtre *Installation en cours*.
- Cliquer sur « Terminer » pour finaliser le processus d'installation et lancer *Spybot - Search & Destroy*.
- Si l'exécutable de *Spybot* est enregistré sur l'ordinateur, on peut le supprimer après l'installation.

Comment utiliser Spybot :

- Lorsque l'installation est terminée, *Spybot* affiche automatiquement la fenêtre *Infos légales*. Pour lancer *Spybot* la prochaine fois, sélectionner Démarrer > Programmes > Spybot - Search & Destroy > Spybot - Search & Destroy.
- Cliquer sur « OK » pour afficher la console *Spybot - Search & Destroy* et la fenêtre *Créer une sauvegarde du Registre*. Il est fortement conseillé de créer une copie de sauvegarde du registre.
- Cliquer sur « Créer une sauvegarde du registre » pour créer et sauvegarder une copie de sauvegarde du registre de votre système.
- Cliquer sur « Suivant » pour afficher la fenêtre *Spybot – Rechercher des mises à jour*.
- Cliquer sur « Vacciner le système » pour afficher la fenêtre *Vaccination du système* et lancer la vaccination du système.
- Si une page de navigateur est restée ouverte, la fenêtre *Open browsers detected* s'affiche avant que le processus de vaccination se mette en marche. Fermer le navigateur, puis cliquer sur « Ok » pour vacciner le système.
- Cliquer sur « Suivant », puis cliquer sur « Commencer à utiliser un programme » pour revenir à la console de *Spybot - Search & Destroy* en mode *Vaccination*.

// PARE-FEU

Un pare-feu agit comme un portier ou un gardien de notre ordinateur. Il applique une série de règles quant à l'information qui est autorisée à y accéder et celle qui doit pouvoir en sortir. Il est le premier programme à recevoir et à analyser l'information provenant d'Internet et le dernier programme à balayer l'information sortante.

Le pare-feu permet d'empêcher les pirates ou autres intrus d'accéder aux renseignements personnels stockés sur notre ordinateur. Il empêche aussi les programmes malveillants d'envoyer de l'information vers Internet sans autorisation. Il faut savoir que tous les systèmes d'exploitation en ont un et, pour maximiser son efficacité, il est toujours recommandé de le mettre à jour.



Cependant, pour ceux qui voudraient un autre pare-feu que celui du système d'exploitation, nous recommandons **Comodo Firewall**, logiciel pare-feu bien connu et réputé. Il est d'exploitation libre, ce qui signifie qu'il n'est pas nécessaire d'obtenir une licence d'utilisation pour s'en servir.

L'utilisation d'un programme pare-feu personnalisé exige, dans les premiers temps, un investissement important de temps et d'effort. Il faut s'assurer que tous les paramètres sont correctement réglés et adaptés à l'usage que l'on fait de son ordinateur. Une fois la période initiale d'apprentissage complétée, le pare-feu n'exige que des interventions mineures de notre part.

Note : Ne jamais accéder à Internet si aucun pare-feu n'est installé sur l'ordinateur ! Même si le modem Internet ou le routeur possède son propre pare-feu, il est fortement recommandé d'en installer également un sur l'ordinateur.

Comment télécharger Comodo :

- Cliquer sur le lien ci-dessous pour ouvrir la page de téléchargement de *Comodo Firewall* : www.personalfirewall.comodo.com/free-download.html
- Cliquer sur le bouton vert « Download » en bas à droite de l'écran sous l'image du logiciel.
- Cliquer sur « Enregistrer le fichier » pour sauvegarder le fichier *cfw_installer_5732_83* sur votre ordinateur, puis double-cliquer sur « cfw_installer_5732_83 » pour lancer l'installation du programme.

Comment installer Comodo :

L'installation de *Comodo* est relativement simple et rapide. Elle comporte deux étapes : il faut dans un premier temps désactiver manuellement le pare-feu de Windows et ensuite installer le logiciel *Comodo*. Idéalement, il ne faut utiliser qu'un seul logiciel pare-feu sur notre ordinateur. Si l'on utilise un autre pare-feu sur sa machine, il faut le désinstaller avant d'installer *Comodo* afin d'éviter les conflits possibles entre logiciels d'un même type.

1. Pour désactiver le programme Pare-feu Windows :

- Sélectionner *Démarrer > Panneau de configuration > Pare-feu Windows* pour afficher la fenêtre *Pare-feu Windows*.

- Cocher l'option *Désactivé (non recommandé)* pour désactiver le Pare-feu Windows.
- Cliquer sur « Ok » pour finaliser la désactivation du *Pare-feu Windows*.

2. Pour installer le programme *Comodo* :

- Double-cliquer sur le programme pour entamer le processus d'installation. Si une boîte de dialogue *Fichier ouvert - Avertissement de sécurité* s'affiche, cliquer sur « Exécuter » et choisir la langue.
- Cliquer sur « Ok » pour afficher le *Contrat de licence de l'utilisateur*. Lire attentivement le *Contrat de licence de l'utilisateur* avant de poursuivre le processus d'installation du logiciel, puis cliquer sur « J'accepte » pour afficher la fenêtre *Enregistrement gratuit*.
- Ne pas saisir d'adresse email dans le champ *Entrez votre adresse email (facultatif)*, cliquer simplement sur « Suivant » pour afficher la fenêtre d'extraction des fichiers. Lorsque le processus d'extraction est complété, la fenêtre *Dossier de destination* s'affiche.
- Cliquer sur « Suivant » pour accepter l'emplacement par défaut et afficher la fenêtre *Sélection du niveau de sécurité du pare-feu*, puis cocher l'option *Pare-feu seulement*.
- Cliquer sur « Suivant » pour afficher la fenêtre *Configuration de Comodo Secure DNS*, avec l'option *Je veux utiliser les serveurs Comodo SecureDNS* sélectionnée.
- Cliquer sur « Suivant » pour afficher la fenêtre *Prêt à installer Comodo Firewall*, puis cliquer sur « Installer » pour lancer l'installation et afficher la fenêtre *Installation de Comodo Firewall en cours*. À l'issue du processus d'installation, la fenêtre *L'installation du Comodo Firewall est terminée* s'affiche.
- Cliquer sur « Terminer » pour afficher la fenêtre de confirmation *Fait*, puis cliquer à nouveau sur « Terminer » pour afficher la fenêtre de confirmation.
- Cliquer sur « Oui » pour redémarrer l'ordinateur et finaliser la procédure d'installation de Comodo.
- Dans le champ *Donnez un nom à ce réseau*, saisir un nouveau nom ou accepter le nom par défaut. Laisser les options de la rubrique *Étape 2 - Déterminez si vous voulez faire confiance aux autres PC en réseau* désélectionnées, puis cliquer sur « Ok » pour finaliser l'installation.

> CREER UN MOT DE PASSE SOLIDE

La plupart des services sécurisés qui nous permettent d'utiliser les technologies numériques pour accomplir des tâches importantes exigent que nous gardions en mémoire un ou plusieurs mots de passe. Ces codes secrets, phrases ou séquences de caractères inintelligibles constituent souvent une première barrière (et parfois la seule et unique barrière) entre nos données et les tiers qui souhaiteraient lire, copier, modifier ou détruire ces renseignements sans notre permission. Il existe plusieurs stratagèmes par lesquels une personne malveillante peut intercepter nos mots de passe. Nous pouvons nous défendre efficacement contre la plupart de ces manœuvres en appliquant quelques mesures de précaution fondamentales, notamment par le choix du mot de passe.



- **Il doit être long :**

Plus un mot de passe est long, moins il est probable qu'un programme informatique soit en mesure de le deviner rapidement. Il faut essayer, autant que possible, de créer des mots de passe de dix caractères ou plus - si toutefois le programme utilisé le permet.

- **Il doit être complexe :**

En plus de la longueur, la complexité d'un mot de passe contribue à faire en sorte qu'un logiciel de « craquage (ou cassage) de mots de passe » soit incapable de trouver la bonne combinaison de caractères. Une combinaison de majuscules, de minuscules, de chiffres et de symboles (comme des signes de ponctuation) devrait être utilisée dans tous les mots de passe.

- **Il ne doit comporter aucun élément personnel :**

Le mot de passe ne doit pas faire référence à une caractéristique personnelle, c'est-à-dire inclure un nom, numéro d'assurance sociale, numéro de téléphone, date d'anniversaire, etc. Ce sont des informations qu'une personne mal intentionnée peut facilement apprendre en effectuant une recherche rapide.

- **Il ne faut pas le partager :**

Il ne faut révéler son mot de passe à personne, à moins que cela ne soit absolument nécessaire. Si nous sommes tout de même amenés à partager notre mot de passe avec un ami, un collègue ou un membre de notre famille, il faut le modifier afin de transmettre un mot de passe temporaire à cette personne, et ensuite, lorsqu'elle a fini de s'en servir, rétablir le mot de passe secret. Il existe des alternatives au partage du mot de passe comme créer un compte particulier pour chacune des personnes qui souhaite ou doit accéder au service dont il est question.

- **Il doit être unique :**

Un bon mot de passe doit être difficile voire impossible à deviner et doit être choisi de telle sorte que nous soyons en mesure de limiter les dégâts si quelqu'un parvient à l'intercepter. Il faut donc éviter d'utiliser le même mot de passe pour plusieurs comptes. Autrement, si une personne mal intentionnée parvient à deviner ou intercepter notre mot de passe, elle aura accès à un grand nombre de nos données. Cela est d'autant plus important que certains services comportent des lacunes permettant facilement de casser les mots de passe.

- **Il doit être pratique :**

En fonction du nombre de comptes que nous avons, la quantité de mots de passe à retenir peut sembler insurmontable et le recours à une base de données de mots de passe sécurisée, telle que le programme **KeePass** (<http://www.keepass.fr/>) apparaît comme la solution. Il est toutefois déconseillé de garder tous nos mots de passe dans un même programme/fichier car une fois celui-ci infiltré, toutes nos données sont mises en péril. Notre mot de passe doit donc être pratique afin de pouvoir être mémorisé aisément.

Comme conseillé précédemment, il est important d'utiliser plusieurs types de caractères pour composer un mot de passe. Nous pouvons aussi employer des procédés mnémoniques comme des acronymes pour retenir nos différents mots de passe. Cela nous permet de transformer de longues phrases en séquences de caractères complexes et, à première vue, aléatoires. Voici deux exemples pour nous aider à trouver notre propre méthode de combinaison de mots et de phrases, à la fois complexes et faciles à mémoriser :

We hold these truths to be self-evident: that all men are created equal = WhtT2bs-e:taMac=

Are you happy today? = rU:-)2d@y?

- **Il doit être changé régulièrement :**

Un bon mot de passe doit être rafraîchi régulièrement, de préférence tous les trois mois. Certaines personnes s'attachent à un mot de passe particulier et n'en changent jamais. C'est une mauvaise idée. Plus nous gardons le même mot de passe longtemps, plus il est facile à deviner. De plus, si une personne arrive à utiliser notre mot de passe pour accéder à nos données et se connecter à nos services à notre insu, elle pourra le faire impunément jusqu'à ce que nous en changions.

> UTILISER DES LOGICIELS LIBRES

Quand les utilisateurs ne contrôlent pas le programme, c'est le programme qui les contrôle.

Avant toute chose, soyons pointilleux sur les termes : « logiciel libre » fait référence à la liberté, pas au prix. Ainsi, l'expression « logiciel libre » (*free software* en anglais) désigne des logiciels qui respectent les libertés des utilisateurs, à savoir la liberté d'exécuter, copier, distribuer, étudier, modifier et améliorer ces logiciels. Précisons également que « logiciel libre » et « open source » ne sont pas des synonymes. Si la grosse divergence entre les deux est surtout idéologique, il y a tout de même quelques petites différences dans la pratique. Presque tous les logiciels open source sont des logiciels libres, mais il y a des exceptions. Certaines licences open source sont par exemple trop restrictives et se disqualifient en tant que licences libres. Comme la seule préoccupation de cette licence concerne le code source, ces exécutable ne sont pas des logiciels libres bien que leur code source soit libre.

Les avantages des logiciels libres sont nombreux : fonctionnalité, rentabilité, indépendance, pérennité, etc. Concernant la protection de nos données, ces logiciels apportent la sécurité, la transparence et la liberté.

- **Sécurité :**

Le code pouvant être relu par tous, les failles de sécurité sont détectées et corrigées plus rapidement que pour les logiciels propriétaires. Les faiblesses et les erreurs qui peuvent être exploitées dans le but de détourner le logiciel de sa fonction initiale font également l'objet de recherches par de nombreuses personnes dont des experts en sécurité informatique.

- **Transparence :**

La disponibilité des sources garantit notre liberté car il n'est pas possible d'inclure au sein d'un logiciel libre des fonctionnalités cachées visant à restreindre nos libertés individuelles ou à collecter nos données. Utiliser un logiciel libre nous assure qu'aucun usage déloyal n'est fait de nos données, de notre identité et de nos droits. De plus, les logiciels libres respectent les standards. Ils n'utilisent pas de formats de fichiers opaques ou de protocoles de communication propriétaires.

- **Liberté :**

Il s'agit sans doute de l'avantage principal des logiciels libres : ils ne nous contraignent pas. Nous pouvons les utiliser sans conditions, les modifier ou les redistribuer comme bon nous semble, tant que nous respectons les licences.

Quelques exemples de logiciels libres

Certains développeurs/diffuseurs de logiciels libres proposent des services libres en ligne comme **Framasoft** (<http://www.framasoft.net/>). En plus de répertorier dans son annuaire plus de mille six cents logiciels libres, Framasoft offre d'excellentes alternatives à de nombreux services « propriétaires de liberté » comme Google Sheets et autres Google Docs.

Éditer > [Framapad](#)

Structurer > [Framindmap](#)

Coder > [Framagit](#)

Organiser > [Framadate](#)

Dessiner > [Framavectoriel](#)

Partager > [Framabin](#)

Calculer > [Framacalc](#)

Réseauter > [Framasphère](#)

Etc.

ETAPE 11

PROTEGER SES ECHANGES

Quels logiciels permettent d'éviter que nos conversations, emails, appels et autres échanges sur le net soient lus et entendus par des tiers ? Comment les utiliser ?

> FAIRE PREUVE DE VIGILANCE

Il est essentiel, lorsque nous surfons sur Internet, de veiller à laisser le moins de traces possibles. Ainsi, si nos données ne sont pas toujours partagées sur le Net, elles y sont au moins stockées et même les sites auxquels nous faisons confiance peuvent se faire pirater ou être amenés à changer leurs politiques de confidentialité. Nos données y sont donc toujours potentiellement exploitables.

- **Désinstaller les programmes non utilisés**

Certains programmes peuvent se connecter automatiquement à Internet afin de réaliser des mises à jour ou de transmettre des informations. Ils constituent une porte d'entrée facile dans votre machine.

- **S'informer des paramètres de confidentialité des sites**

Il importe de lire, de comprendre et de modifier en conséquence les paramètres de confidentialité établis par défaut des sites sur lesquels on crée un compte.

- **Utiliser le protocole https://**

Le protocole https:// offre trois niveaux de protection : le chiffrement (consiste à coder les données échangées pour les protéger des interceptions illicites) ; l'intégrité des données (les informations ne peuvent être ni modifiées, ni corrompues durant leur transfert, que ce soit délibérément ou autrement, sans être détectées) ; l'authentification (prouve que les internautes communiquent avec le bon site Web). L'utilisation de https:// plutôt que http:// est dès lors fortement recommandée quand on navigue sur le web.

- **Sécuriser les contenus sur les réseaux sociaux**

La plupart des réseaux sociaux permettent d'intégrer leur contenu avec d'autres réseaux. Par exemple, il est possible de publier automatiquement sur son compte Facebook ce que l'on écrit sur son Twitter. Or, sur certains réseaux, on reste anonyme alors que sur d'autres, on est totalement exposé.

Il ne faut pas se fier aux sites de réseautage social comme principaux supports de contenu ou sources de renseignement. En effet, il est facile pour une agence gouvernementale de bloquer l'accès national à un réseau social si elle juge que certains contenus y sont répréhensibles. De plus, les administrateurs des réseaux sociaux peuvent décider de retirer certains contenus qu'ils jugent condamnables afin d'éviter de subir la censure dans un pays donné.

Lorsque l'on visite des sites sur lesquels sont présents des boutons de réseaux sociaux, ces derniers sont informés de notre visite. Il est donc recommandé de bloquer ce traçage à l'aide d'une extension logicielle libre et gratuite : **Privacy Badger** (<https://www EFF.org/privacybadger>).

- **Supprimer les historiques et mots de passe**

C'est important de supprimer les historiques et mots de passe de navigation, surtout lorsque l'on accède à Internet depuis un lieu public.

- **Vider les caches des navigateurs**

Les caches sont des portes d'entrée faciles vers la machine si l'on rencontre des sites qui ont été piratés. Les vider régulièrement est un premier pas pour éviter de laisser proliférer virus et *malware*.

Il existe un logiciel qui permet de vider les caches : **CCleaner** (<http://ccleaner.fr/>). Il est toutefois vivement conseillé de faire ces manipulations à la main. D'une part, parce qu'il est important de savoir utiliser et comprendre la machine. D'autre part, car de nombreux ratés existent avec de tels programmes.

- sur Chrome :

Les trois petites barres horizontales (en haut à droite) > Paramètres > Historique > Effacer les données de navigation > Sélectionner la période, le contenu voulu puis valider.

- sur Firefox :

Outils > Supprimer l'historique récent > Tout cocher > Valider

- sur Internet Explorer :

Outils > Options Internet > Onglet « Général » > Supprimer > Cocher la case en bas, Tout supprimer > Valider

- sur Opera :

Outils > Préférences > Onglet « Avancé » > Rubrique « Historique » > Cliquer sur « Vider maintenant » correspondant à « Cache disque »

- sur Safari :

Safari > Réinitialiser Safari > Cocher « Vider le cache » (*Empty the cache*) > Cliquer sur Réinitialiser (*Reset*)

- **Effacer les cookies et bloquer les cookies tiers**

Les cookies ne sont habituellement pas nécessaires pour profiter des ressources disponibles sur Internet. Si on souhaite limiter ses traces, il est recommandé de les refuser par défaut.

- **Changer le composant logiciel Flash**

Le composant logiciel Flash est configuré par défaut pour autoriser l'enregistrement d'informations permettant de tracer notre passage. Il est recommandé de [changer ces paramètres en se connectant au gestionnaire de paramètres](#). Il faut configurer les paramètres de confidentialité pour chacun des 8 onglets.

- **Désactiver certaines applications Google**

Un compte Google enregistre toutes nos activités. Pour désactiver l'enregistrement de nos activités sur le Web et dans les applications Google, il faut se rendre sur la page [Historique du compte](#) et y désactiver le bouton correspondant. Toutefois, même si ce paramètre est suspendu, Google est susceptible d'utiliser les recherches que l'on effectue dans les sessions actives. Une alternative possible est l'utilisation du [mode navigation privée](#) pour effectuer des recherches ou parcourir le Web de manière anonyme.

> SECURISER SES EMAILS



Mozilla Thunderbird est un client de messagerie électronique libre, gratuit, multiplateforme et de source ouverte, qui permet de recevoir, envoyer, trier et archiver des messages de courrier électronique. Un client de messagerie est une application informatique qui permet de télécharger et gérer nos emails sans utiliser de navigateur Internet. *Thunderbird*, à lui seul, permet de traiter plusieurs comptes. Il possède, en outre, la capacité d'utiliser le chiffage par clé publique (asymétrique) pour faire en sorte que nos emails restent confidentiels.

Comment télécharger *Thunderbird* :

- Cliquer sur le lien *Thunderbird* suivant pour ouvrir la page de téléchargement : <https://www.mozilla.org/fr/thunderbird/>
- Cliquer sur le lien « Téléchargement gratuit » pour sauvegarder le fichier d'installation sur votre ordinateur.

Comment installer *Thunderbird* :

- Double-cliquer sur le programme ; il est possible que la boîte de dialogue de confirmation *Fichier ouvert - Avertissement de sécurité* s'affiche à ce moment. Si c'est le cas, cliquer sur « Exécuter ».
- Lorsque l'extraction des fichiers de *Thunderbird* est complétée, la fenêtre *Bienvenue dans l'assistant d'installation de Mozilla Thunderbird* apparaît.
- Cliquer sur « Suivant » pour activer la fenêtre *Mozilla Thunderbird - Type d'installation*.
- Cliquer sur « Suivant » pour accepter les réglages par défaut et afficher la fenêtre *Résumé*.
- Cliquer sur « Installer » pour lancer le processus d'installation. Lorsque l'installation est terminée, cliquer sur « Terminer ». *Thunderbird* se lance automatiquement si l'option *Lancer Mozilla Thunderbird* est cochée. Sinon, on peut la retrouver via *Programmes > Mozilla Thunderbird > Mozilla Thunderbird*.

Comment désactiver l'option *Recherche et indexation globales* dans *Thunderbird* :

La fonction *Recherche et indexation globales* de *Thunderbird* doit être désactivée pour optimiser la performance du programme. Selon la quantité et la taille des messages, cette fonction peut ralentir le système en réécrivant continuellement et inutilement les mêmes données sur le disque dur.

- Sélectionner *Outils > Options* dans la console *Thunderbird* pour afficher la fenêtre *Options*.
- Cliquer sur « Avancé » pour afficher le contenu de cet onglet.
- Cliquer sur « Désactiver la recherche et l'indexation globales », dans la section *Configuration avancée*, pour désactiver cette option.

Comment enregistrer un compte de courrier électronique sur *Thunderbird* :

La fenêtre *Assistant d'importation - Importer les paramètres et les dossiers de messages* n'apparaît qu'à la première installation de *Thunderbird*.

- Cocher l'option *Ne rien importer*.
- Cliquer sur « Suivant » pour afficher la fenêtre *Création d'un compte courrier*.
- Saisir les nom, adresse de courrier électronique et mot de passe dans les champs appropriés ; puis décocher l'option *Retenir le mot de passe*.
- Cliquer sur « Suivant » pour afficher la fenêtre *Création d'un compte courrier* avec l'option *IMAP*.
- Cliquer sur « Créer le compte » pour afficher la console *Thunderbird* avec votre compte de courrier compris dans la barre *Tous les dossiers*, en haut à gauche. L'interface principale de *Thunderbird* s'affiche alors.

Notes : Pour ajouter un compte de courriel, sélectionner *Fichier > Nouveau > Comptes courrier*. La fenêtre *Création d'un compte courrier* s'affiche, on peut alors reprendre les étapes énoncées ci-dessus. Après avoir enregistré nos différents comptes de courrier électronique dans *Thunderbird*, les ouvertures de l'interface principale requièrent un mot de passe pour chaque compte. Bien que la fonction d'enregistrement du mot de passe ne soit généralement pas recommandée, *Thunderbird* comporte une fonction *Mot de passe maître*. Cette fonction permet de n'utiliser qu'un seul mot de passe pour protéger tous les autres associés aux différents comptes, que l'on ne saisit qu'une seule fois lors du processus d'enregistrement.

➤ SECURISER SA MESSAGERIE INSTANTANEE

Pidgin est un client de messagerie instantanée (MI) gratuit et de source ouverte qui permet d'organiser et de gérer différents comptes de messagerie instantanée avec une seule et unique interface. Pour utiliser *Pidgin*, il faut disposer d'au moins un compte de MI. Par exemple, un compte de courriel Gmail permet d'utiliser le service de MI Google Talk avec Pidgin.



Pidgin est compatible avec les services de messagerie instantanée suivants: AIM, Bonjour, Gadu-Gadu, Google Talk, Groupwise, ICQ, IRC, MIRC, MSN, MXit, MySpaceIM, QQ, SILC, SIMPLE, Sametime, Yahoo!, Zephyr ainsi que tous les clients de MI utilisant le protocole de messagerie XMPP.

Pidgin ne permet pas la communication entre différents services de MI. Par exemple, si l'on utilise *Pidgin* pour accéder à notre compte Google Talk, il nous est impossible de chatter avec un ami qui utilise un compte ICQ. Par contre, *Pidgin* peut être réglé pour gérer plusieurs comptes compatibles avec l'un ou l'autre des protocoles supportés. Autrement dit, nous pouvons simultanément utiliser un compte Gmail, un compte ICQ, et chatter avec des correspondants qui utilisent l'un ou l'autre de ces services (qui sont supportés par *Pidgin*).

Il est conseillé d'utiliser *Pidgin* pour tous les besoins en matière de messagerie instantanée, puisque ce programme offre plus de sécurité que la plupart des options qui existent et ne vient pas par défaut avec des logiciels publicitaires ou espions superflus qui pourraient compromettre la sécurité de notre machine et notre vie privée.

La messagerie **Off-the-Record (OTR)** est un module complémentaire conçu spécialement pour *Pidgin* qui permet de chatter en privé. Elle offre les fonctionnalités suivantes:

- authentification du correspondant ;
- possibilité de démenti : après une conversation, il est impossible de retracer les destinataires et destinataires des messages ;
- chiffrement des communications instantanées ;
- *Perfect Forward Secrecy* : si une tierce partie trouve l'accès à nos clés privées, nos conversations préalables ne sont pas compromises.

Il faut installer le programme *Pidgin* avant d'installer le plugin OTR.

Comment télécharger *Pidgin* et OTR :

- Cliquer sur le lien suivant pour ouvrir la page de téléchargement *Pidgin* :
<http://www.pidgin.im/download/windows/>.
- Cliquer sur le lien suivant pour ouvrir la page de téléchargement OTR :
<https://otr.cypherpunks.ca/>.
- Sauvegarder les fichiers d'installation et double-cliquer dessus pour les ouvrir.

Comment installer Pidgin :

- Après avoir double-cliqué sur le programme pour l'ouvrir, si une fenêtre *Fichier ouvert - Avertissement de sécurité* s'ouvre, cliquer sur « Exécuter » et choisir la langue.
- Cliquer sur « Suivant » pour afficher la fenêtre *Licence utilisateur*. Après avoir lu la *Licence d'utilisation*, cliquer sur « Suivant » pour afficher la fenêtre *Installation de Pidgin 2.10.3 - Choisissez les composants*.
- Cliquer sur « Suivant » jusqu'à ce que le processus d'installation soit clôturé.

Comment installer le moteur *Off-The-Records* (OTR) :

- Après avoir double-cliqué sur le programme pour l'ouvrir, si une fenêtre *Fichier ouvert - Avertissement de sécurité* s'ouvre, cliquer sur « Exécuter » pour afficher la fenêtre suivante.
- Cliquer sur « Next » pour afficher la fenêtre *License Agreement*; après avoir lu la *Licence d'utilisation*, cliquer sur « I agree » pour afficher la fenêtre *Pidgin-otr 3.2.0-1 Setup - Choose Install Location*.
- Cliquer sur « Install » pour lancer la procédure d'installation et enfin sur « Finish » quand c'est terminé.

Comment enregistrer un compte de MI dans *Pidgin* :

- Lancer *Pidgin* et cliquer sur « Ajouter » pour afficher une fenêtre *Ajouter un compte vierge*.
- Cliquer sur le menu défilant *Protocole* pour visualiser les protocoles de service de MI supportés par *Pidgin*. Sélectionner le protocole de MI approprié.

Certains fournisseurs de services de messageries instantanées affichent leurs zones de texte particulières qu'il faut remplir. D'autres remplissent les zones de texte automatiquement (par exemple, avec Google Talk, la zone de texte *Domaine* est déjà remplie). Cependant, tous les services exigent un nom d'utilisateur et un mot de passe.

- Saisir la première partie de l'adresse mail dans *Utilisateur* (nico.letesteur) et la deuxième dans *Domaine* (@gmail.com) ainsi que le mot de passe. Bien retenir le mot de passe et, pour des raisons de sécurité, ne pas cocher *Mémoriser le mot de passe*.
- Saisir un surnom par lequel on souhaite être identifié dans la zone *Alias local*. (Facultatif)
- Cliquer sur « Ajouter » pour finaliser la procédure d'ajout de compte et afficher la fenêtre *Comptes et la Liste de contacts*.
- Après avoir complété ces étapes, ajouter les contacts *Pidgin* en saisissant leurs coordonnées respectives.

Comment configurer le plugin *Pidgin*-OTR :

- Lancer *Pidgin* et ouvrir le menu *Outils*, puis sélectionner l'item *Plugins*.
- Faire défiler jusqu'à l'option *Messagerie confidentielle Off-the-Record*, puis cocher la case adjacente pour l'activer.
- Cliquer sur « Configurer le plugin » pour configurer la *fenêtre Messagerie confidentielle Off-the-Record*.

Comment produire une clé privée et afficher son empreinte :

Les séances de chat sécurisées avec *Pidgin* ne sont possibles qu'en créant une clé privée pour le compte utilisé. La fenêtre de configuration d'OTR comporte deux onglets: *Configuration* et *Empreintes connues*. L'onglet *Configuration* sert à créer une clé pour chacun des comptes et à régler certaines options d'OTR. L'onglet *Empreintes connues* contient les clés de vos contacts. Il faut disposer d'une clé pour chaque contact avec qui on souhaite chatter de façon privée et confidentielle.

- Pour optimiser la confidentialité des communications, cocher les options *Permettre messagerie privée*, *Commencer messagerie privée automatiquement* et *Ne pas archiver les conversations OTR* dans l'onglet *Configuration* illustré ci-dessus.
- Cliquer sur « Produire » pour créer une clé. Une fenêtre apparaît peu après pour confirmer la création de la clé privée. Cliquer sur « Valider » pour clôturer la procédure.

Une clé privée pour notre compte vient d'être créée. Cette clé est utilisée pour chiffrer nos séances de chat et faire en sorte que personne ne puisse nous espionner. L'empreinte est une longue séquence de lettres et de chiffres utilisés pour identifier la clé d'un compte.

Comment authentifier une séance de clavardage privée :

- Double-cliquer sur le compte d'un des contacts en ligne pour entamer une nouvelle séance de MI. Si le module OTR des deux correspondants sont installés et correctement configurés, un nouvel icône OTR apparaît au bas de la fenêtre de chat.
- Cliquer sur « Non-privé » pour afficher le menu associé, puis sélectionner l'item *Commencer conversation privée*.

Pidgin communique automatiquement avec le programme de messagerie instantanée de notre contact et affiche un message chaque fois que l'on entame une séance de chat privée et sécurisée. En conséquence, le bouton OTR « Non-privé » devient « Non-vérifié ». Ce changement indique que l'on est maintenant prêt à mener une conversation chiffrée avec notre contact sans qu'il ait pour autant été authentifié.

Comment authentifier l'identité de notre contact *Pidgin* :

Pour authentifier notre contact dans *Pidgin*, nous pouvons utiliser trois méthodes différentes :

- saisir un code ou une phrase secrète déterminée à l'avance avec notre contact ;
- poser une question dont seulement nous et notre contact connaissons la réponse ;
- vérifier manuellement nos empreintes respectives via un autre mode de communication.

> SECURISER SON VOIP

« Voice Over Internet Protocol » (VOIP) est une technologie qui permet de téléphoner via le réseau IP. **Jitsi** est un logiciel libre de communication instantanée, d'appel audio et vidéo, et de partage d'écran. *Jitsi* permet d'accéder directement aux correspondants sans passer par un intermédiaire. Il chiffre les communications afin que personne ne puisse y avoir accès.



Comment télécharger Jitsi :

- Cliquer sur le lien suivant pour ouvrir la page de téléchargement *Jitsi* : <https://jitsi.org/Main/Download#stableline>.
- Cliquer sur « Stable builds ». On découvre alors les différentes versions de *Jitsi* disponibles pour chaque système d'exploitation. Cliquer sur celui qui correspond au système d'exploitation.
- Enregistrer le fichier, le retrouver et double-cliquer dessus pour l'ouvrir.

Comment utiliser Jitsi :

- Lorsqu'on lance *Jitsi* pour la première fois, une fenêtre qui nous propose de nous identifier apparaît. Fermer la fenêtre. À la place, créer un nouveau compte en cliquant directement depuis la fenêtre principale de *Jitsi* sur « Fichier > Ajouter un nouveau compte ».
- Sélectionner ensuite un protocole de communication.
- Sur la fenêtre suivante, cocher *Créer un nouveau compte *protocole**.
- Choisir un nom d'utilisateur et un mot de passe. Le nom choisi doit être disponible sur ce serveur (sans quoi il faudra recommencer cette étape). Il permet à nos correspondants de nous y trouver. En cas d'oubli, le mot de passe ne peut pas être récupéré.
- Valider en cliquant sur « Ajouter ».

Comment ajouter un correspondant sur Jitsi :

- Cliquer sur « Fichier > Ajouter un contact » depuis la fenêtre principale de *Jitsi*. Si plusieurs comptes sont enregistrés sur *Jitsi*, choisir celui auquel on veut ajouter un nouveau contact.
- Dans *ID*, entrer le nom enregistré par notre correspondant au moment de créer son compte.
- Dans *Nom affiché*, choisir le nom ou le surnom que l'on souhaite associer à ce contact lorsque l'on utilise *Jitsi* (il peut être identique à son ID). Une demande de confirmation est alors envoyée à cette personne pour que l'on puisse l'enregistrer.

Comment crypter les communications sur Jitsi :

- Cliquer sur la barre « Outils » de la fenêtre de messagerie et cliquer ensuite sur le cadenas. S'il est fermé, c'est que les échanges sont chiffrés.
- Néanmoins, pour être certain que personne ne s'est immiscé dans le processus de chiffrement en authentifiant votre correspondant, aller dans *Chat sécurisé > Authentifier le contact*, puis suivre les instructions qui sont indiquées.

```
<!DOCTYPE HTML>
<HTML>
<HEAD>
  <TITLE>SURVEILLANCE SELF-DEFENSE</TITLE>
</HEAD>
<BODY>
  CYCLE D'ACTIVITES, DONT LES FORMULES SONT MODULABLES ET
  COMBINABLES A SOUHAIT.

  <SENSIBILISATION>
    > UN FILM (6' - REALISATION GSARA)

  <REFLEXION>
    > DES CONFERENCES-DEBATS

  <MISE EN SITUATION>
    > JEU DE POSITIONNEMENT
    > JEU DE LA FICELLE

  <ACTION>
    > LA BOITE A OUTILS
    > LA CRYPTOPARTY

  // VOUS SOUHAITEZ EN ORGANISER ?
  // VOUS SOUHAITEZ Y PARTICIPER ?

  <CONTACT>
    MELODIE.BODSON@GSARA.BE
    02/218.58.85
  </CONTACT>

</BODY>
</HTML>
```