

# AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION



## Guide de protection de la vie privée

Version	Date de la version	Modification apportée
V1.0	Juillet 2019	Draft1

L'objectif de ce document est d'essayer de rendre tous les citoyens conscients des risques informatiques, capables de sécuriser leurs ordinateurs, au travail comme à la maison, prendre les mesures nécessaires pour protéger leurs identités, leurs données privées et profiter de l'Internet, en toute sécurité.

### **Public visé**

Grand public

### **Limitation**

Ce document n'est pas destiné aux entreprises, ces dernières doivent procéder à la mise en place de tout un système de gestion de la sécurité de l'information SMSI.

Seules les bonnes pratiques qui ont été jugées importantes ont été retenues pour des raisons de complexité.

Ce document suppose qu'un poste de travail est une machine à base de processeur Intel sous une version Microsoft Windows supportée vue que c'est la configuration dominante, pour les autres configurations les recommandations peuvent être déduites par analogie.

### **Rôle de l'ANSI**

En cas d'un comportement suspect, L'ANSI met à la disposition des citoyens un support en ligne disponible 12/24 7/7 à l'adresse <https://support.anssi.gov.gn> pour répondre aux incidents informatiques et assister à la mise en place des recommandations de sécurité.

Certes, Internet est un espace de recherche, de divertissement où chacun peut communiquer et s'épanouir en toute liberté. Mais, des risques majeurs demeurent. C'est pourquoi, plusieurs règles de prudence devraient être respectées, dont on cite principalement :

- ✓ Bien choisir son Pseudo ou « pseudonyme »
- ✓ Choisir un Mot de passe robuste :
  - a. Utiliser de longues chaînes de caractères (plus de 8 caractères) composées
  - b. De caractères Alphanumériques et de caractères spéciaux.
  - c. Ne pas utiliser des détails relevant de la vie privée par exemple le numéro de téléphone, la date de naissance ou le nom des parents, etc.
  - d. Changer régulièrement le mot de passe.
  - e. Utiliser un mot de passe spécifique pour la messagerie électronique, et éviter d'utiliser celui du compte Facebook, Twitter ou autre application.
- ✓ Eviter de divulguer son mot de passe à autrui, et stocker ses mots de passe dans un utilitaire de stockage de mots de passe comme KeePass : logiciel gratuit (<http://keepass.info/>)
- ✓ Ne pas répondre aux Quizz incitant à donner des informations personnelles.
- ✓ Utilisez des Add-on comme « web of trust » ou « Firefox No script »
- ✓ Garder votre antivirus, votre système et votre navigateur, à jour pour se prémunir contre les liens douteux, les scripts malicieux, et les infections par les keylogger ou cheval de Troie.
- ✓ Effectuer une déconnexion de votre compte, après l'usage d'un ordinateur non personnel, et supprimer les mots de passe enregistrés.

## **Messagerie électronique :**

- ✓ Ouvrir uniquement les pièces jointes aux messages électroniques attendues ou parvenues de sources fiables.
- ✓ Analyser les pièces jointes avec un antivirus mis à jour.
- ✓ Vérifier l'authenticité d'une demande suspecte (fournir des informations confidentielles) avant de répondre par courrier électronique.
- ✓ Ne pas répondre aux messages indésirables ou douteux.
- ✓ Ne pas ouvrir les messages électroniques indésirables et les supprimer sans les ouvrir.

## **Réseaux sociaux :**

- ✓ Bien choisir sa réponse à la Question secrète : Ne pas fournir d'éléments de vérification courants tels que la date de naissance ou le nom de jeune fille de la mère
- ✓

## **Gérer sa liste d'amis :**

- ✓ Ajoutez dans votre liste, seulement les contacts que vous connaissez et ayant des noms clairs avec une photo réelle.
- ✓ L'ami de ton ami ne sera pas forcément ton ami. Il peut s'agir d'un parfait inconnu mal intentionné

## **Soigner sa réputation :**

- ✓ Être vigilant et veiller régulièrement sur tous les contenus qui sont publiés sur le site à son sujet (images, commentaires...).
- ✓ Une réputation douteuse peut causer parfois la perte d'un emploi, ou même rater une opportunité d'emploi.

## **Faites attention aux tentatives de piratage :**

- ✓ Faites attention aux 'scammers', ce sont des personnes qui tentent de vous piéger ou vous pirater c'est en général de faux profiles, qui vous envoient un lien ou mettent un statut avec un lien à cliquer.

## **Pour Facebook**

- ✓ Si l'un de vos amis est piégé ou victime de vol d'identité ou de piratage vous pouvez l'aider en le signalant aux administrateurs.

## **Paramétrer son compte :**

- ✓ Utiliser des paramètres de confidentialité sur les profils, pour que seuls les amis proches puissent accéder à ces Informations
- ✓ Utiliser la fonction 'Secure browsing' dans les paramètres du compte pour forcer le navigateur à ouvrir votre compte en mode HTTPS pour prévenir les tentatives de Phishing.

## **Pour Facebook**

Il existe une méthode infaillible pour sécuriser votre compte Facebook, qui est la vérification du compte par SMS, après avoir entré votre login et mot de passe, une 2eme étape d'authentification, qui ne peut être passée, que si vous saisissez le mot de passe envoyé par le serveur Facebook sur votre téléphone.

N'hésitez pas à demander assistance au personnel de l'ANSSI :

E-mail : [support@anssi.gov.gn](mailto:support@anssi.gov.gn)

<https://www.anssi.gov.gn>