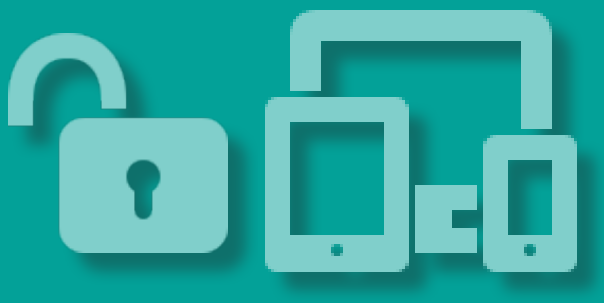
AUCAME
Caen Normandie

Sécurité informatique



Guide des bonnes pratiques

à destination des salariés

Juillet 2019

Sommaire

Mise en page : AUCAME (Agence d'urbanisme de Caen Normandie Métropole) - 2019
Directeur de publication : Patrice DUNY

Pourquoi sécuriser son informatique ?

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages. Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les entreprises. Par exemple, les données les plus sensibles peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un smartphone, d'une tablette, d'un ordinateur portable.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité et de pertes économiques et financières. Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre dans l'entreprise. À cet effet, la sensibilisation des collaborateurs de l'Aucame aux règles d'hygiène informatique est fondamentale et surtout très efficace pour limiter une grande partie des risques.

Réalisé sur la base du document de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et par le groupe de travail interne sur la sécurité informatique, ce guide a pour objectif de vous informer sur les risques et les moyens de vous en prémunir en acquérant des réflexes simples pour sécuriser votre usage de l'informatique.

Le groupe ainsi formé de Bastien BESNARD, Elisabeth BERTRAND, Anne-Sophie BOISGALLAIS, Paul ANDRÉ ET Karine SALIGNON s'est réuni les 5 avril et 20 juin 2019. Il a ainsi permis de rédiger ce guide de bonnes pratiques ayant valeur de recommandations à destination des salariés de l'Agence, ainsi qu'une charte informatique, annexée au règlement intérieur de l'Aucame.

1 – Mots de passe et accès à l'ordinateur

Le mot de passe est un **outil d'authentification** utilisé notamment pour accéder à un équipement numérique et à ses données. Pour bien protéger vos informations, choisissez des mots de passe **difficiles à retrouver à l'aide d'outils automatisés** ou **à deviner** par une tierce personne.

Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) en évitant votre nom, date de naissance et autre suite facile à déduire.

Deux méthodes simples peuvent vous aider à définir vos mots de passe :

- **La méthode phonétique :** « J'ai acheté 5 CDs pour cent euros cet après-midi » : ght5CDs%E7am ;
- **La méthode des premières lettres :** « Allons enfants de la patrie, le jour de gloire est arrivé » : aE2IP,IJ2Géa!

Définissez un mot de passe **unique pour chaque service sensible**. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle...) ne doivent jamais être réutilisés pour d'autres services.

Il est préférable de ne pas recourir aux outils de stockage de mots de passe.

RECOMMANDATIONS :

- Les mots de passe doivent comporter au moins **12 caractères**, des **majuscules**, **minuscules**, **chiffres** et **caractères spéciaux**.
- Ne **pas conserver** les mots de passe dans des fichiers ou sur des post-it.
- Ne **pas préenregistrer** les mots de passe dans les navigateurs, notamment lors de l'utilisation ou la connexion à un ordinateur public ou partagé.
- Créer une alerte **renouvellement** des mots de passe **tous les 6 mois** pour l'accès au **profil**, à la **messagerie** et à **MailInBlack**.

2 - Mettre à jour régulièrement les logiciels

Dans chaque système d'exploitation (Android, 10S, MacOS, Linux, Windows,...), logiciel ou application, des **vulnérabilités** existent. Une fois découvertes, elles sont **corrigées par les éditeurs** qui proposent alors aux utilisateurs des mises à jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

RECOMMANDATIONS :

- Il appartient **à l'utilisateur de mettre régulièrement à jour** Windows et les différents logiciels (Adobe, ArcGis…).
- **Configurer les logiciels** pour que les mises à jour de sécurité s'installent **automatiquement** chaque fois que cela est **possible**. Sinon, téléchargez les correctifs de sécurité disponibles exclusivement sur les sites internet officiels des éditeurs.
- Certains postes ne se mettent pas à jour automatiquement. **Le responsable informatique interviendra une fois par mois** pour les mettre à jour.
- **Mise à jour du serveur** avec l'**obligation d'éteindre** l'ensemble des postes lors d'une réunion d'équipe **une fois par mois.**
- **Obligation d'éteindre** l'ordinateur tous les soirs pour permettre **les mises à jour.**

3 – Les comptes utilisateurs

Lorsque vous accédez à votre ordinateur, vous bénéficiez de **droits d'utilisation** plus ou moins élevés sur celui-ci. On distingue les droits dits « **d'utilisateur** » et les droits dits « **d'administrateur** ».

Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels...), prenez votre compte utilisateur créé spécialement pour vous.

Le compte administrateur n'est à utiliser que par le responsable informatique qui pourra intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, ...).

RECOMMANDATIONS :

- **Chaque utilisateur doit être identifié** nommément afin de pouvoir relier une action sur le système à un utilisateur. Il est **interdit de se connecter sur un autre compte** utilisateur que le sien.
- **Éteindre ou verrouiller son poste** lors d'une **absence « longue »** (rendez-vous extérieur, pause déjeuner, le soir…).
- **Verrouillage auto de la session** au bout d'un certain temps (pause…).
- Encadrez par des **procédures** déterminées les **arrivées et les départs de personnel** pour vous assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et surtout qu'ils sont révoqués lors du départ de la personne.

4 - Effectuer des sauvegardes régulières

Pour veiller à la **sécurité de vos données**, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un **dysfonctionnement** de votre système d'exploitation ou à une **attaque**.

Une sauvegarde du **serveur** est effectuée **toutes les nuits** sur un **boîtier de stockage** ainsi que dans le **Cloud**.

RECOMMANDATIONS :

- **Sauvegarde personnelle** régulière.
- **Ne pas stocker** des documents professionnels **sur le bureau.**
- Possibilité de **créer un raccourci du dossier sur le bureau** pour ne pas avoir à l'enregistrer sur le poste.

5 - Être aussi prudent avec son smartphone qu'avec son ordinateur

Bien que proposant des services innovants, **les smartphones sont aujourd'hui très peu sécurisés**. Il est donc indispensable d'appliquer certaines règles élémentaires de sécurité informatique.

RECOMMANDATIONS :

- N'installez **que les applications nécessaires** et **vérifiez à quelles données** elles peuvent avoir **accès** avant de les télécharger (informations géographiques, contacts, appels téléphoniques...).
- Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer.
- **En plus du code PIN** qui protège votre carte téléphonique, **utilisez un schéma ou un mot de passe** pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement.
- Effectuez des **sauvegardes régulières** de vos contenus sur un **support externe** pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial ;
- **Ne préenregistrez pas** vos mots de passe.

6- Protéger ses données lors de ses déplacements

L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite les **déplacements professionnels** ainsi que le **transport et l'échange de données**. Voyager avec ces appareils nomades fait cependant peser des **menaces** sur des **informations sensibles** dont le **vol** ou la **perte** auraient des **conséquences importantes** sur les activités de l'organisation.

RECOMMANDATIONS :

- N'utilisez **que du matériel** (ordinateur, supports amovibles, téléphone) **dédié** à la mission et ne contenant que les données nécessaires.
- **Sauvegardez** ces données, pour les retrouver en cas de perte.
- **Vérifiez** que vos **mots de passe** ne sont **pas préenregistrés**.
- **Gardez** vos appareils, supports et fichiers **avec vous**, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel).
- **Évitez d'utiliser le Wi-Fi public.**
- **Videz la clef USB après utilisation.**
- **Refusez la connexion** d'équipements appartenant à des **tiers** à vos propres équipements (ordiphone, clé USB, baladeur...).

7 - Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent souvent un **rôle central dans la réalisation des attaques informatiques** (courriels frauduleux, pièces jointes piégées, etc.).

RECOMMANDATIONS :

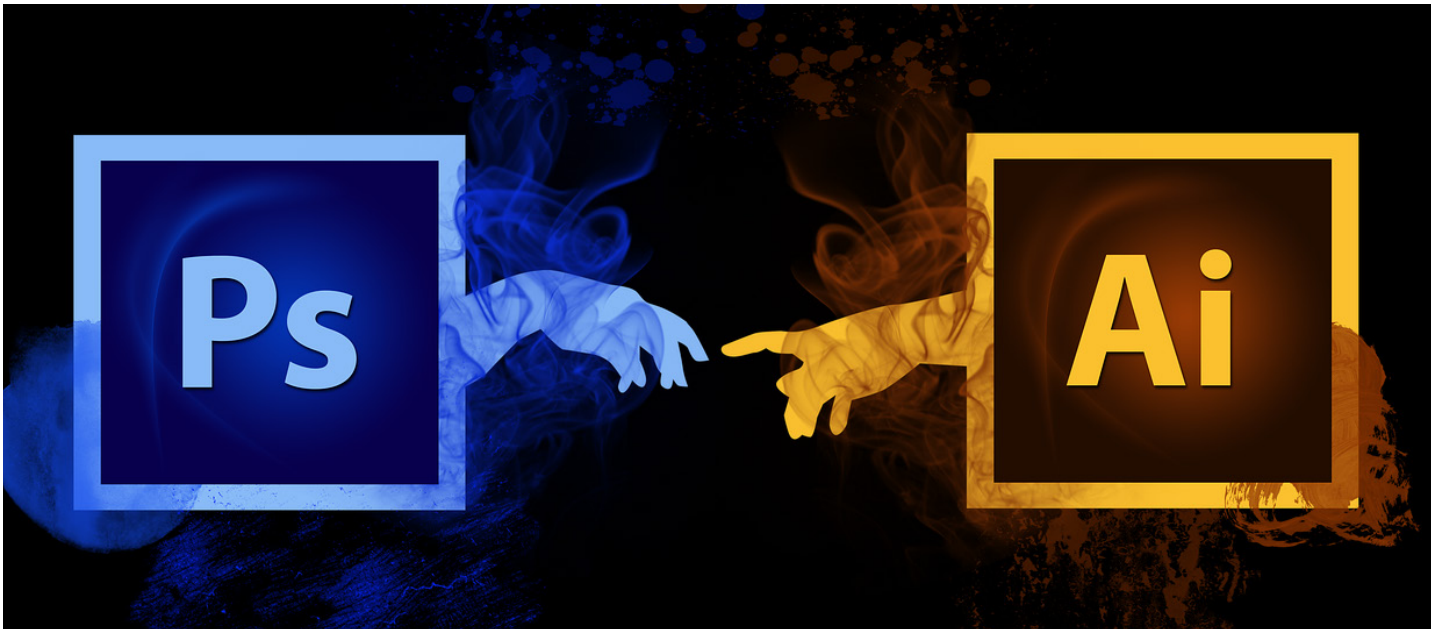
- **Vérifiez la cohérence** entre l'expéditeur présumé et le contenu du message et vérifiez son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail.
- **N'ouvrez pas les pièces jointes** provenant de **destinataires inconnus** ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts.
- Si des **liens** figurent dans un courriel, **passez votre souris dessus avant de cliquer**. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence.
- **Ne répondez jamais par courriel** à une demande **d'informations personnelles ou confidentielles** (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing ».
- **N'ouvrez pas et ne relayez pas** de messages de **types chaînes** de lettre, appels à la solidarité, alertes virales, etc.
- **Désactivez l'ouverture automatique des documents téléchargés.**

8 - Télécharger ses programmes sur les sites officiels des éditeurs

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le **risque d'enregistrer sur votre ordinateur des programmes** ne pouvant être mis à jour et qui, le plus souvent, **contiennent des virus** ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le **contrôle à distance** de votre machine pour **espionner** les actions réalisées sur votre ordinateur, **voler** vos données personnelles, **lancer des attaques,** etc.

RECOMMANDATIONS :

- Téléchargez vos programmes sur les **sites de leurs éditeurs** ou d'autres sites de **confiance**.
- Pensez à **décocher ou désactiver** toutes les cases proposant d'installer des **logiciels complémentaires**.
- **Désactivez l'ouverture automatique** des documents téléchargés et lancez une **analyse antivirus avant de les ouvrir** afin de vérifier qu'ils ne contiennent aucune charge virale connue.

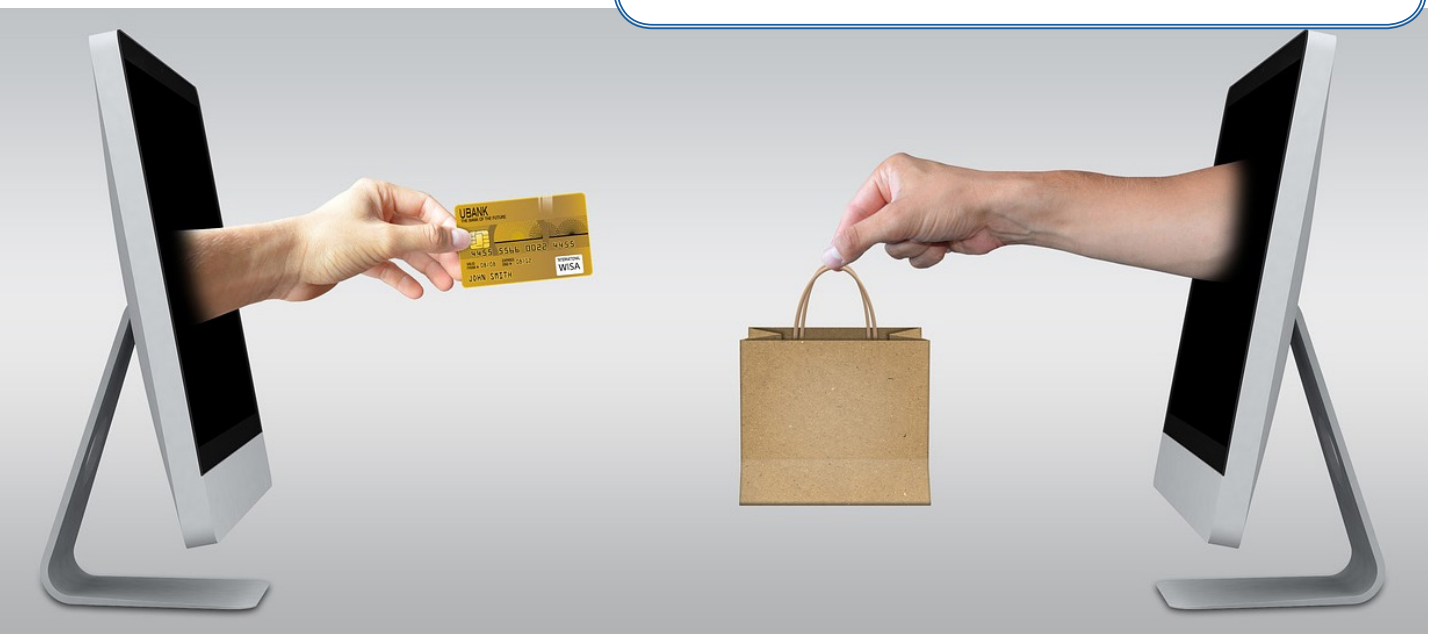


9 - Être vigilant lors d'un paiement sur Internet

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre ordiphone (smartphone), vos **coordonnées bancaires sont susceptibles d'être interceptées** par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet.

RECOMMANDATIONS :

- **Contrôlez la présence d'un cadenas** dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs).
- Assurez-vous que la **mention « https:// »** apparaît au début de l'adresse du site internet.
- **Vérifiez l'exactitude de l'adresse** du site Internet en prenant garde aux fautes d'orthographe par exemple.
- **Privilégiez la méthode** impliquant l'envoi d'un code de **confirmation de la commande par SMS**.
- De manière générale, **ne transmettez jamais le code confidentiel de votre carte bancaire.**
- N'hésitez pas à vous rapprocher de **votre banque** pour **connaître et utiliser les moyens sécurisés qu'elle propose**.
- **Modifier régulièrement les mots de passe des sites d'achats.**



10 - Séparer les usages personnels des usages professionnels

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels.

Le **AVEC (Apportez Votre Equipement personnel de Communication)** ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs **équipements personnels** (ordinateur, ordiphone, tablette, etc.) dans un **contexte professionnel.** Si cette solution est de plus en plus utilisée aujourd'hui, elle pose des **problèmes en matière de sécurité des données** (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

RECOMMANDATIONS :

- **Ne faites pas suivre vos messages** électroniques **professionnels** sur des services de messagerie utilisés à des fins **personnelles**.
- **N'hébergez pas de données professionnelles** sur vos équipements **personnels** (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne.
- De la même façon, **évitez de connecter des supports amovibles personnels** (clés USB, disques durs externes, etc.) **aux ordinateurs de l'entreprise**.

11- Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Les données que vous laissez sur Internet vous échappent instantanément.

Des **personnes malveillantes pratiquent l'ingénierie sociale**, c'est-à-dire **récoltent vos informations personnelles**, le plus souvent **frauduleusement** et **à votre insu**, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.

RECOMMANDATIONS

Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- Soyez vigilant vis-à-vis des **formulaires** que vous êtes amenés à remplir : ne transmettez **que les informations strictement nécessaires**.
- Pensez à **décocher les cases** qui **autoriseraient le site à conserver ou à partager vos données.**
- Ne donnez accès qu'à un **minimum d'informations personnelles et professionnelles** sur les **réseaux sociaux** et soyez vigilant lors de vos **interactions** avec les **autres utilisateurs**.

Guide rédigé d'après les informations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information - *cf. lien ci-dessous*).

Liens utiles aux bonnes pratiques de cybersécurité :

- **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** : https://www.ssi.gouv.fr/
- **Commission Nationale de l'Informatique et des Libertés (CNIL)** : https://www.cnil.fr/
- **Service de l'Information Stratégique et de la Sécurité Économiques (SISSE)** : https://www.entreprises.gouv.fr/information-strategique-sisse
- **Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (Police nationale)** : https://www.internet-signalement.gouv.fr

Dans un souci de cohérente avec les pratiques développées par le groupe de travail « développement durable » de l'Aucame (cf. « *Pour une agence écoresponsable, guide des bonnes pratiques à destination des salariés* »), ce document est imprimé sur papier labellisé FSC et Ecolabel EU.

AUCAME
Caen Normandie

Agence d'Urbanisme de Caen Normandie Métropole
21 rue de la Miséricorde - 14000 CAEN

02 31 86 94 00
contact@aucame.fr

www.aucame.fr