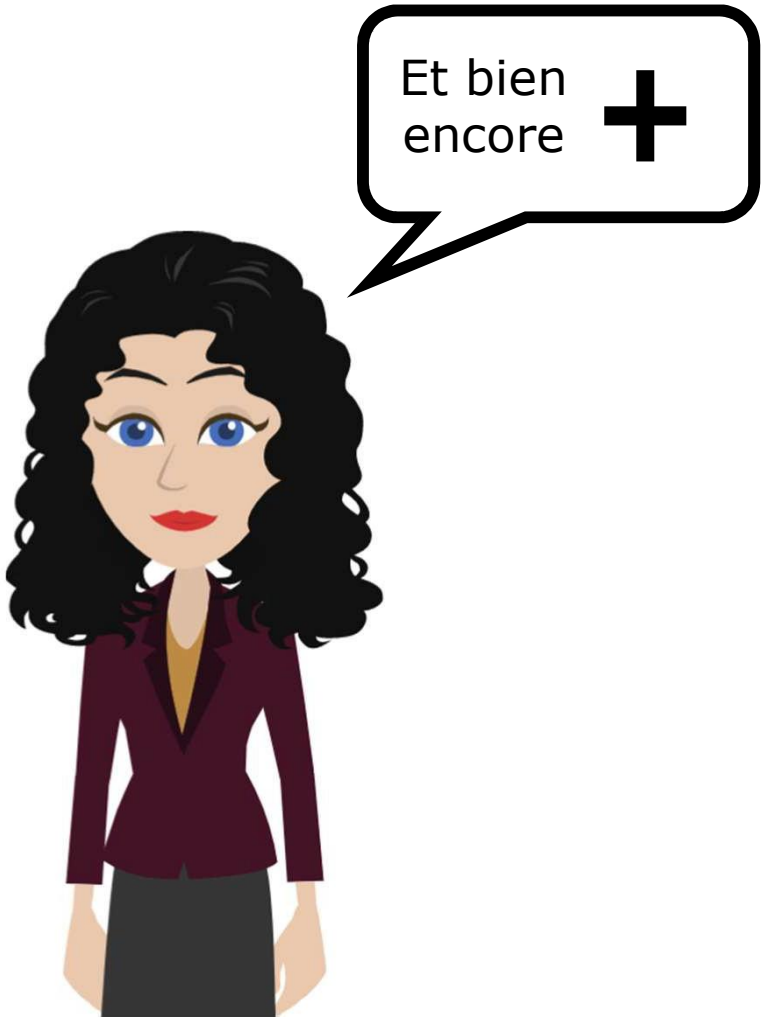
# Guide des bonnes pratiques de l'informatique

**10** bonnes @ttitudes sur le web et les réseaux sociaux

**7** comportements @ adopter avec votre ordinateur




Générations Mouvement
Les Aînés Ruraux

# SOMMAIRE

# 10 bonnes @ttitudes sur le web et les réseaux sociaux

1

**Réfléchissez avant de publier**
Sur internet tout le monde peut voir ce qui est mis en ligne : les photos, les vidéos, les opinions, les informations

2

**Ne dites pas tout**
Donnez le minimum d'informations vous concernant sur les réseaux sociaux : pas d'opinions politiques, pas d'opinions religieuses, pas d'adresse postale et de numéro de téléphone

**Fiabilisez vos mots de passe**
Un mot de passe complexe permet de sécuriser vos comptes. Pour créer un mot de passe vous pouvez, par exemple, choisir une phrase associée au site sur lequel vous voulez employer le mot de passe que vous cherchez à créer. Soit « *Pour protéger mon compte Facebook, j'invente 1 phrase de passe !* » devient « PpmcFB,j'i1pdp ! »


3

**Vérifiez votre e-reputation**
Tapez régulièrement votre nom et votre prénom dans les moteurs de recherche pour vérifier quelles informations vous concernant circulent sur le web. N'oubliez pas de vérifier aussi dans les images …

4


5

**Modérez vos publications**
La diffusion des photos sur le net est incontrôlable. Ne publiez qu'avec l'accord des personnes et ne diffusez pas de photos gênantes de vous-même de votre famille ou encore de vos amis.

**Sécurisez vos comptes**
Paramétrez toujours les profils sur les réseaux sociaux afin de rester maitre des informations partagées.

6

7

**Utilisez un pseudonyme**
Seuls vos proches sauront que c'est vous et non les enseignes commerciales, les moteurs de recherches et tous les inconnus sur les réseaux sociaux. Le pseudo n'empêche pas la bonne attitude n°6 !

**Respectez les autres**
Gardez à l'esprit que vous êtes responsable de ce que vous publiez et écrivez …. même derrière un écran. Faites attention, modérez vos commentaires sur les réseaux sociaux, blogs et forums. Ne faites pas aux autres ce que vous n'aimeriez pas qu'ils vous fassent.

8

9

**Deux adresses email valent mieux qu'une**
Vous pouvez par exemple avoir une adresse email « sérieuse » pour vos échanges avec la famille, les amis, les impôts, la banque….
Et une autre adresse email pour les jeux, les réseaux sociaux, les newsletters …


**Vous êtes seul(e) maitre de vos données personnelles**
Vous seul(e) êtes en mesure : d'accepter ou de refuser de remplir un formulaire, de donner vos coordonnées, d'accepter ou de refuser la conservation de vos données. Vous seul avez souhaité commenter un post ou participer à une conversation sur les réseaux sociaux.

10

# Pour aller + loin

## La pratique des réseaux sociaux pour le compte de Générations Mouvement

Lorsque vous vous exprimez sur les réseaux sociaux sur et/ou pour le compte de Générations Mouvement, gardez à l'esprit que vous représentez le Mouvement.
De fait, veillez à ce qu'il n'y ait pas de confusion possible entre vos opinions et intérêts personnels et ceux de Générations Mouvement.
Internet n'oublie rien et les réseaux sociaux ont des yeux et des oreilles partout !

### Conseil

Identifiez-vous comme bénévole ( ou salarié.e) de Générations Mouvement lorsque vous utilisez les réseaux sociaux pour vos publications associatives (ou professionnelles).

### Rappelez-vous

Gardez à l'esprit que rien n'est « secret » ou « privé » sur Internet et que des publications jugées abusives peuvent refaire surface tôt ou tard.

Pour que vos « amis » digitaux ne deviennent pas vos « ennemis », il faut savoir séparer sa sphère privée de sa sphère associative (ou professionnelle) !

## Informations personnelles, associative et identité numérique sur Internet

De manière générale, dès que vous vous connectez à Internet, certaines de vos données vous échappent totalement : votre adresse Ip, vos données de localisation, le type de support que vous utilisez pour vous connecter, les sites que vous visitez etc. Bien évidemment, il ne s'agit pas de tomber dans la paranoïa, mais simplement de s'informer pour ne pas livrer inutilement vos données personnelles : nom, prénom, adresse email, numéro de téléphone, adresse postale, date de naissance, habitudes de consommations, centres d'intérêts etc.

### Conseil

Utilisez plusieurs adresses électroniques et aussi pseudonymes dédiés à vos différentes activités sur Internet.

Par exemple : une adresse réservée aux activités dites sérieuses (banques, activité associative, etc.) et un pseudonyme et une adresse dite « divers » destinée aux autres services en ligne (shopping, jeux concours, newsletter etc.).

### Comment les organisations commerciales, obtiennent-elles mes données personnelles ?

Les formulaires en tout genre servent à collecter vos données personnelles : avis, inscription à une newsletter, inscription à un réseau social, formulaire pour une carte de fidélité, achat sur Internet …
Mais aussi, le fait d'accepter les cookies sur les sites que vous visitez. Pensez à ne transmettre que les informations nécessaires, soyez attentifs et vérifiez que vous avez décoché les cases qui autoriseraient les sites à conserver ou à partager vos données auprès d'organisations tierces.

## Vie associative et respect du Règlement Général sur la Protection des Données (RGPD)

### Zoom sur le RGPD

Le RGPD, acronyme de Règlement Général sur la Protection des Données, définit un contexte juridique permettant d'encadrer le traitement des données personnelles sur tout le territoire de l'Union européenne.
Ce nouveau **règlement européen** répond notamment aux évolutions technologiques de nos sociétés, à savoir le développement du commerce en ligne et l'explosion des réseaux sociaux et autres applications collectant nécessairement des données personnelles. En ce sens, le RGPD vient s'inscrire dans la continuité de la Loi française Informatique et Libertés de 1978, tout en permettant aux citoyens de mieux contrôler l'utilisation de leurs données personnelles.

Qui dit collecte de données personnelles, dit RGPD. Les associations et Fédérations de Générations Mouvement ne font pas exception.

## Comment se conformer au RGPD dans vos activités associatives ?

### TRIEZ

Effectuez un tri régulier des documents enregistrés sur votre ordinateur et dans votre boite mail, mais aussi dans vos armoires. Ne conservez que les documents utiles à vos fonctions et supprimez les éléments devenus obsolètes.

### PROTEGEZ

Protégez par un mot de passe les fichiers contenant des données personnelles ( nom, prénom, adresse, téléphone etc.) ou des données sensibles (information bancaires etc.)

## INFORMEZ

Assurez-vous que les personnes pour lesquelles vous collectez des données personnelles sont informées du type d'information que vous collectez, de l'utilisation que vous comptez en faire et de comment vous contacter si elles ont des questions.

Vous pouvez, par exemple, informer les adhérents du type de données collectées et leur conservation dans le Règlement intérieur de votre association.

## SECURISEZ

Assurez-vous que les données personnelles des adhérents sont conservées en toute sécurité ( dans SAGA, par exemple).

## COLLECTEZ

Collectez uniquement les données personnelles qui sont nécessaires à vos activités.

## SOUS-TRAITEZ

Assurez-vous du respect du principe de sous-traitance par les prestataires ou partenaires (voyagistes, hôtels, …) auxquels Générations Mouvement pourrait confier la collecte ou l'utilisation de données personnelles.

Pensez au contrat de sous-traitance. Un modèle est disponible sur le site internet de Générations Mouvement, dans la rubrique « Règlement général sur la protection des données ».

## ATTENTION

Générations Mouvement n'est pas autorisée à :

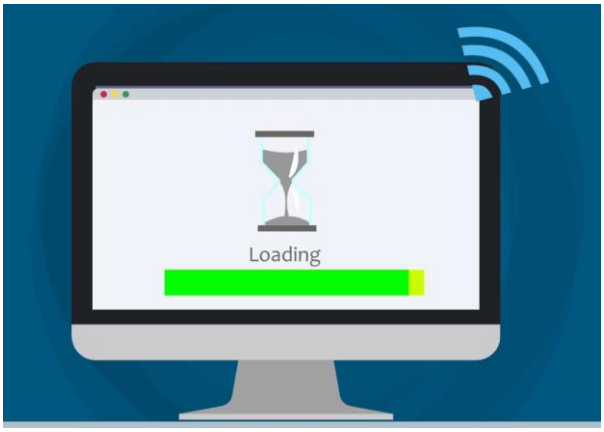
- collecter des informations dites « sensibles » (relatives notamment à l'état de santé, l'origine ethnique, la préférence sexuelle, les opinions politiques, les convictions religieuses) sans l'accord de la personne concernée ou seulement si la loi nous l'impose.
- communiquer des données personnelles à une personne extérieure à l'association sauf en cas d'obligation légale, recours à des prestataires techniques ou si la personne concernée a donné son autorisation.
- conserver ces informations personnelles plus longtemps que la raison juridique pour laquelle elles ont été acquises.

## Qu'est ce que le principe de licéité ?

Générations Mouvement a besoin de collecter et d'utiliser des données personnelles dans le cadre de son activité associative, afin de répondre aux divers besoins des salariés, bénévoles, administrateurs et adhérents.
P.ar exemple, Générations Mouvement utilise des adresses e-mails pour envoyer aux adhérents ou bénévoles ou partenaires les informations dont ils ont besoin. Générations Mouvement collecte des données pour des actions comme des concours, des voyages ou pour la base de données SAGA. Générations Mouvementa besoin d'informations personnelles concernant les salariés afin notamment de gérer leur paie et leur carrière ou pour des raisons juridiques ou pour assurer leur sécurité.

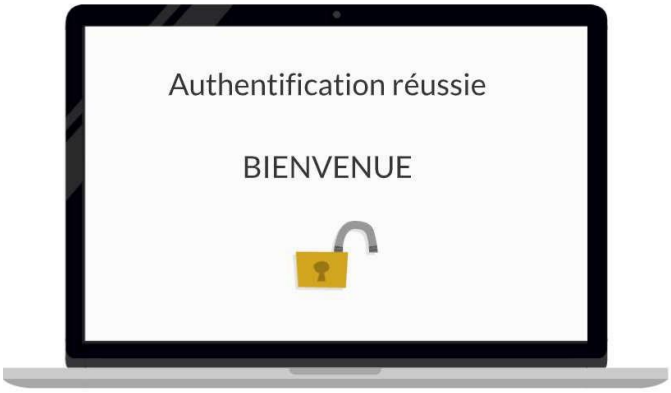
# 7 Comportements à adopter avec votre ordinateur

1




**Exécutez régulièrement les mises à jour de vos logiciels et applications**
Dans chaque système d'exploitation ( Windows, IOS, Androïd…) il y a des failles de sécurité. Heureusement elles sont très vites décelées. Alors n'hésitez pas à faire les mises à jours dès que le système le demande

2

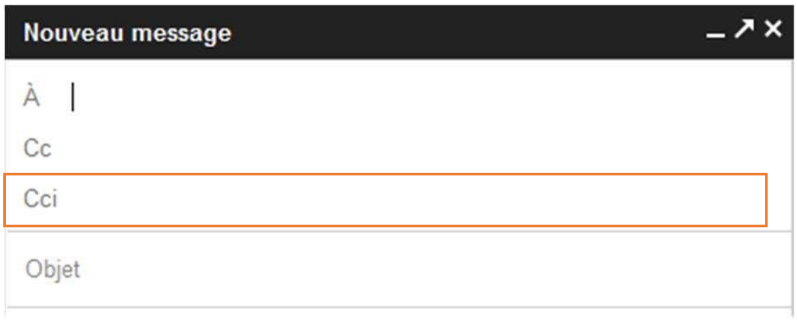



**Effectuez des sauvegardes régulières de vos données**
Si vous enregistrez vos données localement c'est-à-dire sur l'ordinateur et non sur un serveur, il est fortement recommandé de sauvegarder votre système. Cela vous permettra d'en disposer en cas de dysfonctionnement de votre ordinateur.

3

**Fiabilisez vos mots de passe**
Pour bien protéger vos informations et vos données personnelles, choisissez des mots de passe difficiles à retrouver par les outils automatisés ou à deviner par une tierce personne.

4




**Sécurisez votre boite mail**
Si vous devez envoyer un email à un grand nombre de personnes, mettez les adresses de vos destinataires dans le champs Cci d'envoi. Ainsi les adresses ne pourront être récupérées par des tiers.

**Smartphone et tablette ont aussi besoin de protection.**
Tout comme les ordinateurs, vos appareils mobiles vous suivent partout. Apportez leur toute la sécurité nécessaire.

5

6

7

**Séparez les usages personnels, des usages associatifs ou professionnels.**

**Téléchargez en toute sécurité**
Télécharger un nouveau programme est très utile, mais le virus qui se cache derrière…nettement moins. Soyez attentif lors de vos téléchargements.

# Pour aller + loin

## Effectuez des sauvegardes régulières

Imaginez la situation…Vous travaillez depuis plusieurs jours sur ce fichier fastidieux qui vous a demandé beaucoup d'efforts. Vous allumez votre ordinateur et ce dernier ne répond plus. Votre assistant de tous les jours a rendu l'âme et par conséquent votre fichier avec.
Deux cas de figure :

- ☐ Aïe c'est le drame, vous aviez enregistré votre fichier sur le bureau de votre ordinateur et il n'existe aucune autre sauvegarde, il va falloir tout recommencer…

- ☐ Ouf ! vous l'aviez enregistré sur le serveur (ou support externe). Rien n'est perdu !

### Zoom sur la sauvegarde des données

Vous pouvez utiliser des supports externes tel qu'un disque dur externe réservé exclusivement à cet usage.

Si vous constatez des signes de défaillance de votre support externe n'attendez pas pour transférer vos données sur un nouveau support et détruire les données du support défaillant.

Autre alternative, pour sauvegarder vos données : le cloud ou informatique en nuage. Il vous permet de stocker vos données sur des plateformes Internet, accessibles par identifiant et mot de passe. Toutefois, cette solution n'est pas sans risques : confidentialité des données, localisation des données, disponibilité et intégrité des données. Si vous optez pour ces solutions, consultez les conditions d'utilisation de ces services avant d'y souscrire.

## Fiabilisez vos mots de passe

### Zoom sur les mots de passe à éviter

- Les combinaisons trop simples : 123456, 123456789, azerty, motdepasse, 111111…
- Des prénoms
- Des noms d'équipe sportives
- Des artistes ou musiciens
- Des personnalités fictives ou non

Rappelez vous de ne pas conserver les mots de passe dans des fichiers ou sur des post-it ou votre boite mail.

Il est également préférable nepas pré-enregistrer vos mots de passe dans les navigateurs, notamment lors de l'utilisation ou la connexion à un ordinateur public ou partagé.

**Reposez vos méninges !**
Utilisez un gestionnaire de mots de passe ou un trousseau d'accès chiffré pour stocker vos mots de passe en toute sécurité. Vous n'aurez à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes !

### Zoom sur les gestionnaires de mots de passe

Un gestionnaire de mots de passe vous permet de ne retenir qu'un seul mot de passe qui ouvre l'accès à tous les autres. Les mots de passe pourront alors être très longs, très complexes et tous différents car c'est l'ordinateur qui les retient à votre place.
On peut citer entre autres, parmi les logiciels libres régulièrement mis à jour : Keepass, dont la sécurité a été évaluée par l'Agence nationale de sécurité des systèmes d'information (ANSSI), Zenyway ou Passwordsafe.

## La sécurité informatique passe également par votre boite courriel

Bonjour,
J'espère que tu te portes bien?
De mon côté, plusieurs craintes liées à des soucis de santé dont j'aimerais te parler,
Si tu as un peu de temps à m'accorder n'hésite pas à me répondre directement à mon mail vu que je suis hors/ service au tél .
Je reste devant l'ordi
À te lire rapidement.
Michel

Nous avons toutes et tous reçu au moins une fois ce type d'email provenant d'une personne que l'on connait ou non. Vous recevez ce type d'email car le compte de messagerie de votre interlocuteur s'est fait hacker, cela signifie qu'un individu malveillant a pris le contrôle de la messagerie courriel et envoie cet email à tous les contacts de la boite. Ces courriels et leurs pièces jointes jouent souvent un rôle central des attaques informatiques (courriels frauduleux, pièces jointes infectées, etc.).
Pas de panique, lorsque vous recevez ce type de courriel, surtout n'y répondez pas et supprimez-le de votre boîte de réception.

## Conseil

- ✓ Si vous connaissez la personne, n'hésitez pas à vérifier la véracité de l'email par téléphone par exemple.
- ✓ Si vous ne connaissez pas la personne, bloquez l'expéditeur par un clic droit sur votre souris.
- ✓ 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 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 ou votre opérateur Internet/téléphoniquepour 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.
- ✓ Tout ceci est également valable sur les réseaux sociaux.

# Smartphone, tablette, ordinateur portable doivent aussi être protégés

Pratiques, intuitifs, légers, nos terminaux portables nous rendent bien des services. Cependant ils restent encore assez peu sécurisés bien qu'ils exigent le même niveau de sécurité que votre ordinateur. Il est donc indispensable d'appliquer certaines règles élémentaires de sécurité informatique.

## Rappelez-vous

En plus du code PIN qui protège votre carte SIM, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre smartphone et/ ou tablette. Veillez à configurer votre appareil pour qu'il se verrouille automatiquement dès lors que nous ne l'utilisez plus.

## Zoom sur les applications gratuites

En téléchargeant gratuitement une application sur smartphone ou tablette, nous ne nous interrogeons pas de savoir comment les éditeurs vont-ils se rémunérer ? Dommage, car bien souvent si nous ne faisons pas attention, nous acceptons de laisser l'accès à nos informations géographiques, notre répertoire téléphonique, nos photos, nos appels téléphoniques …Avant de télécharger une application vérifiez bien les conditions. En cas de doute, ne la téléchargez pas.

## Conseil

Effectuez des sauvegardes régulières de vos contenus sur un support externe ( ordinateur, disque dur externe …) pour pouvoir les conserver en cas de problème ou changement d'appareil. Là aussi, veillez à ne pas pré-enregistrer vos mots de passe.

## Téléchargez en toute sécurité

Pour vos activités associatives (ou professionnelles), vous êtes parfois amené à télécharger des programmes depuis Internet. Alors, pour télécharger en toute sécurité, voici quelques recommandations :

- Privilégiez le téléchargement des programmes depuis les sites des éditeurs ou d'autres sites de confiance.
- Décochez ou désactivez toutes les cases proposant d'installer des logiciels complémentaires ou explicitant le fait que vos données seront transmises à des partenaires, organisations commerciales tierces etc.
- Les liens publicitaires ou sponsorisés sur les sites internet sont « des aspirateurs à données », ne cliquez pas dessus.
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucun virus.

# Séparer autant que possible les usages personnels des usages associatifs

Les usages et les mesures de sécurité sont différents sur les équipements informatiques (ordinateur, tablette, smartphone) personnels et associatifs. Il est donc recommandé de séparer vos usages associatifs de vos usages personnels.

Pensez à vous équiper d'une messagerie courriel dédiée à vos usages associatifs ou professionnels.

Il est déconseillé d'héberger des données associatives/ professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne.

De la même façon, vos supports amovibles personnels (clés USB, disques durs externes, etc.) doivent rester personnels et ne pas être connectés aux ordinateurs de votre association.

Le but étant de préserver et de protéger les ressources de Générations Mouvement. Ceci, afin qu'elles ne soient perdues, endommagées, mal utilisées, gaspillées, prêtées, transférées ou cédées sans autorisation.

# Guide des bonnes pratiques de l'informatique


19 rue de Paris – 93100 BOBIGNY