Communauté de Communes
Côte Ouest
Centre Manche

MAISON DU PAYS
DE LESSAY
Centre social

Prise en main de la tablette

Connected Seniors

Espace Public Numérique

Table des matières

CONNEXION WIFI 3

CONNEXION A UN ORDINATEUR 4

INTERFACE .....

1. Barre D'état 5
2. Bureau 5
3. Widget 5
4. Barre de recherche Google 5
5. Barre de lancement rapide 5
6. Applications 5

Touches de navigation 6

Les appuis 6

L'écran de verrouillage 6

Le clavier 6

PERSONNALISER SA TABLETTE .....

Fond d'écran 7

Le bureau 7

Accessibilité : 7

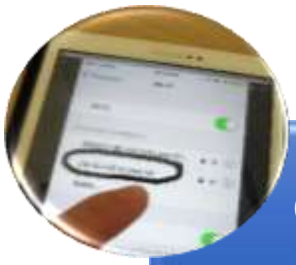
Vue : 8

Audition 8

GOOGLE PLAY 8

10 REGLES DE SECURITE 10

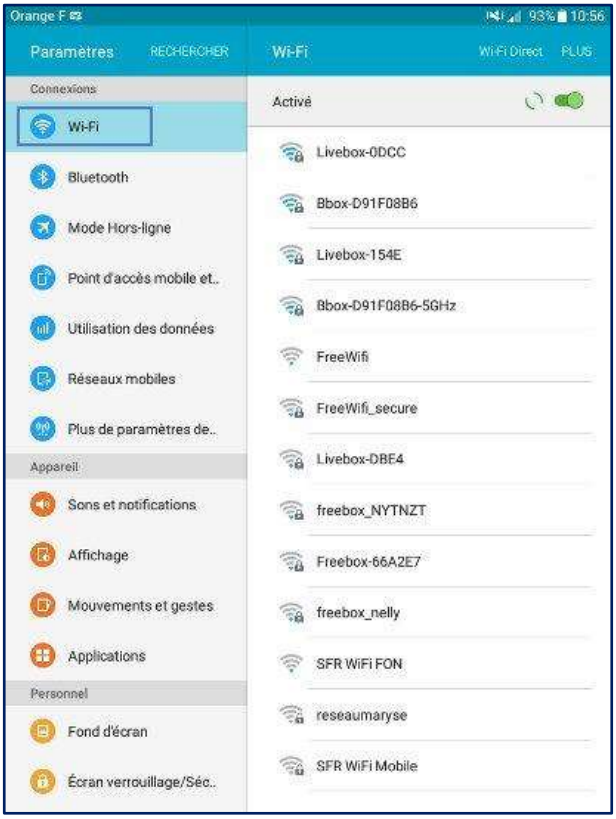
QUELQUES CURIOSITES 12



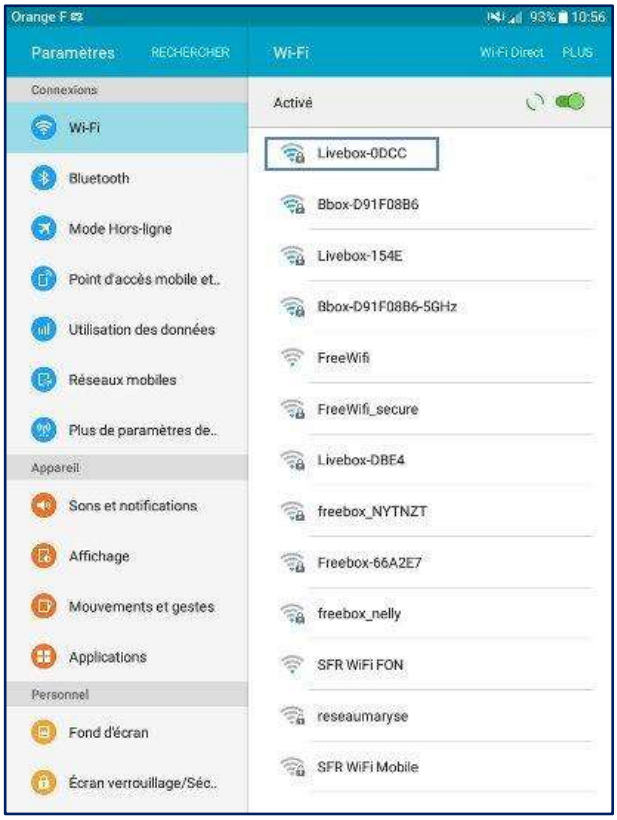
Connexion WIFI

1. Sélectionner Paramètres

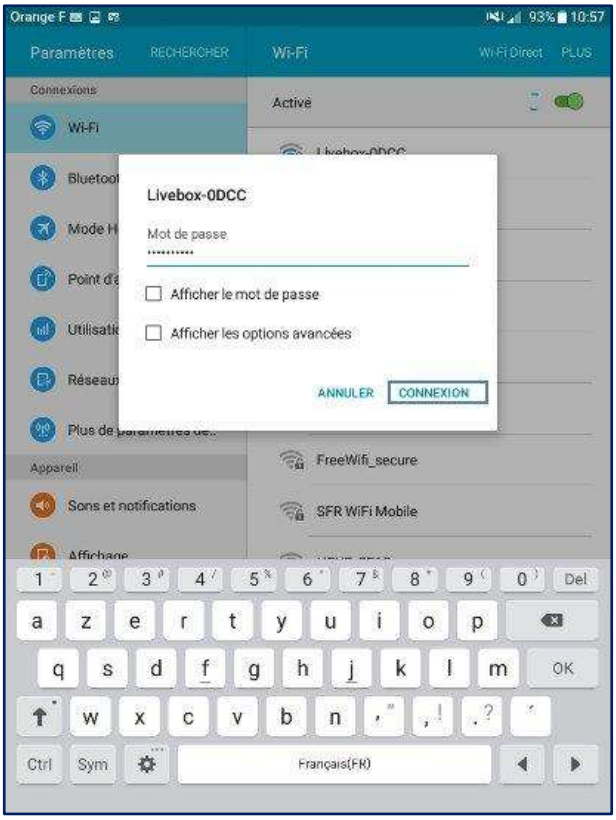
2. Sélectionner wifi

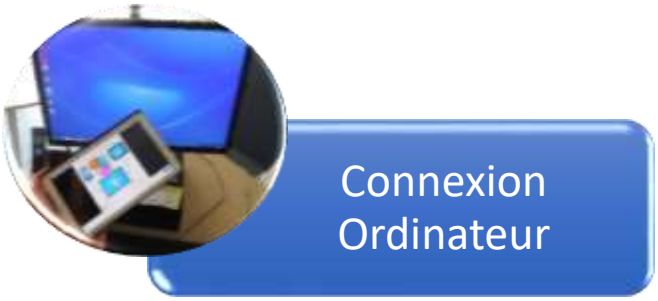


3. Sélectionner votre box



4. Se connecter à la box





Votre tablette est équipée d'une sortie micro USB. Pour la connecter à un ordinateur, utilisez le câble fourni à l'achat et branchez-le sur un port USB de l'ordinateur. Ce dernier installera automatiquement le pilote adéquat pour interagir avec la tablette. Une fois la tablette connectée, vous aurez accès à sa mémoire interne, comme lors du branchement d'une clé USB standard. Vous pourrez dès lors récupérer vos photos et vos documents.

Interface

1. Barre D'état : Indique l'heure, l'état de la batterie, du GPS, du Wifi et du Bluetooth. Informe des notifications et propose des commandes. (Faire glisser vers le bas)
2. Bureau : Peut accueillir les raccourcis des applications, widgets, etc. Le système dispose de plusieurs bureaux à faire défiler de gauche à droite avec le doigt.
3. Widget : Applications automatiquement mises à jour comme la météo, horloge, mail, calendrier etc.
4. Barre de recherche Google : Lance une recherche sur Internet, sans passer par le navigateur.
5. Barre de lancement rapide : Contient les applications les plus courantes. Reste disponible sur tous les bureaux.
6. Applications : Contient toutes les applications installées sur la tablette. (Faire glisser vers le haut)

Touches de navigation

- **Récent** : Affiche les applications utilisées récemment en miniatures.
- **Accueil** : renvoie à l'écran d'accueil.
- **Précédent** : ouvre l'écran précédent.

Les appuis : Il faut distinguer les appuis courts (simple pression), des appuis longs (pression d'environ 2s) et des glissements (appui long avec déplacement sans relever le doigt).

L'écran de verrouillage : Il est le premier écran que l'on voit au réveil de la tablette. Cet écran sert de protection pour éviter d'appuyer par inadvertance sur un raccourci. Par défaut, cet écran affiche l'heure et les notifications.

Le clavier

Lorsqu'on s'apprête à saisir du texte dans une application, un e-mail par exemple, le clavier s'affiche alors à l'écran, simulant ainsi un clavier physique.

1. Le texte (« Je » dans cet exemple) est relatif à la correction automatique. Appuyez sur le mot correctement orthographié pour accélérer la saisie.
2. Permet de supprimer le texte sélectionné ou les caractères qui précèdent ou succèdent le curseur.
3. Permet d'aller à la ligne (retour chariot).
4. Permet de saisir une seule lettre en majuscule. Lorsque cette lettre est saisie, la saisie est de nouveau en minuscule. Pour saisir plusieurs lettres en majuscules, appuyez de manière prolongée sur cette touche.
5. Permet d'utiliser les raccourcis clavier comme copier et coller.
6. Permet de saisir des chiffres et des symboles.
7. Ouvre d'autres options comme la saisie vocale, les émoticônes, la saisie manuscrite, le presse-papiers, le paramétrage du clavier

Personnaliser sa tablette

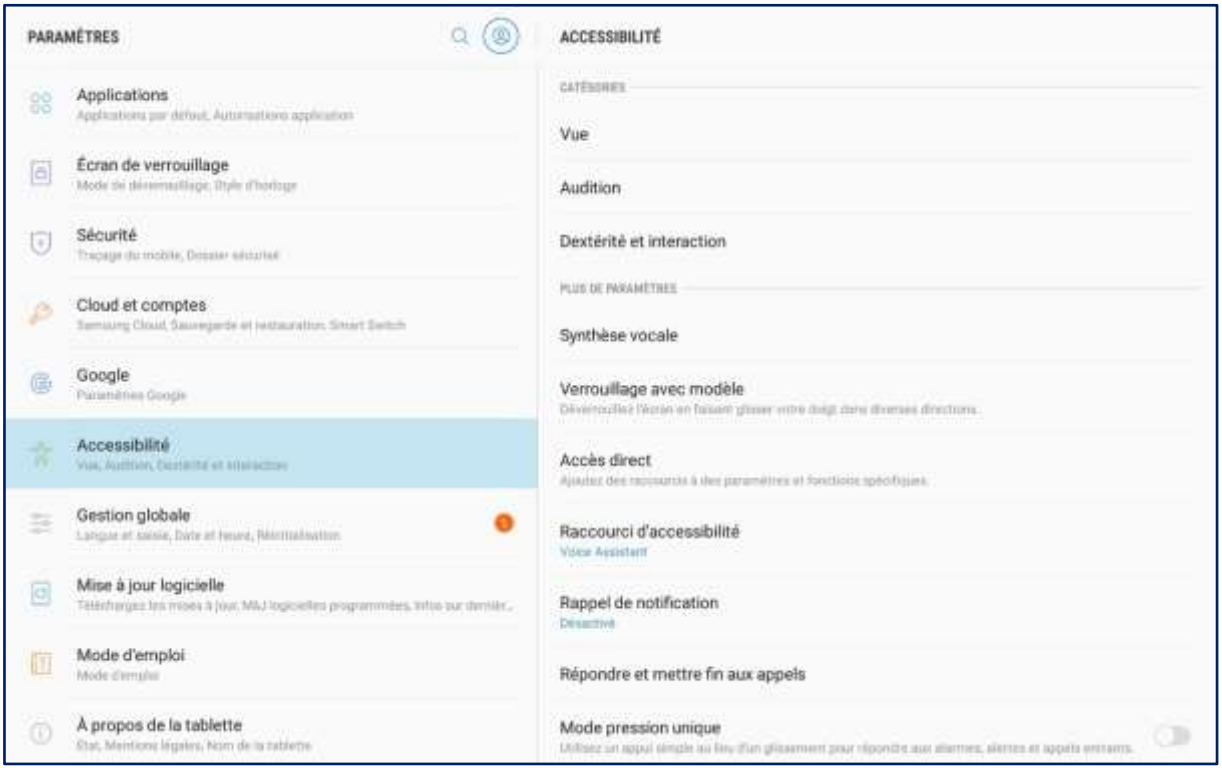
Fond d'écran : Sur le bureau, faire un appui long puis « fonds d'écran » et choisir une image depuis la galerie.

Le bureau : Les bureaux de l'écran d'accueil vous permettent d'organiser et de personnaliser vos raccourcis et widgets.

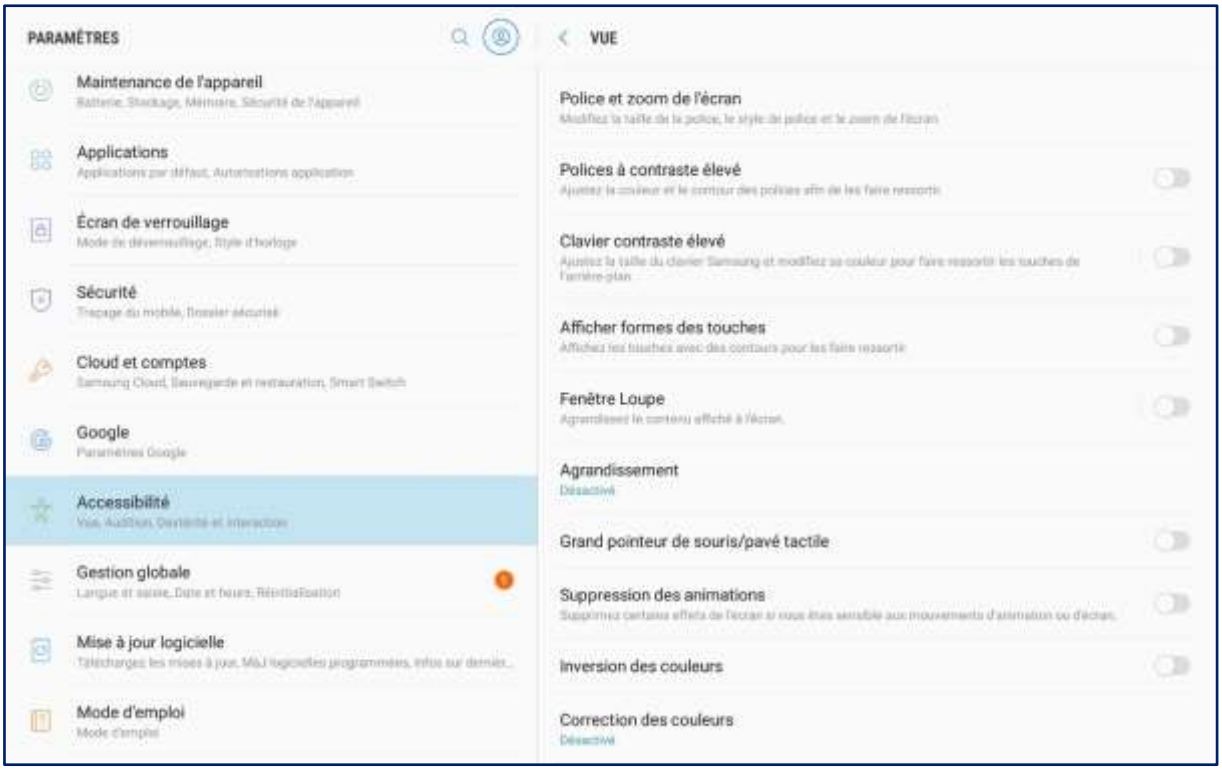
- **Les raccourcis** : Faites un appui long sur le raccourci que vous voulez déplacer ou supprimer et faites-le glisser vers une position libre avant de relâcher.

- **Les widgets** : Sur le bureau, faire un appui long puis « Widgets ». Faites un appui long sur le widget que vous voulez déplacer ou supprimer et faites-le glisser vers une position libre avant de relâcher.

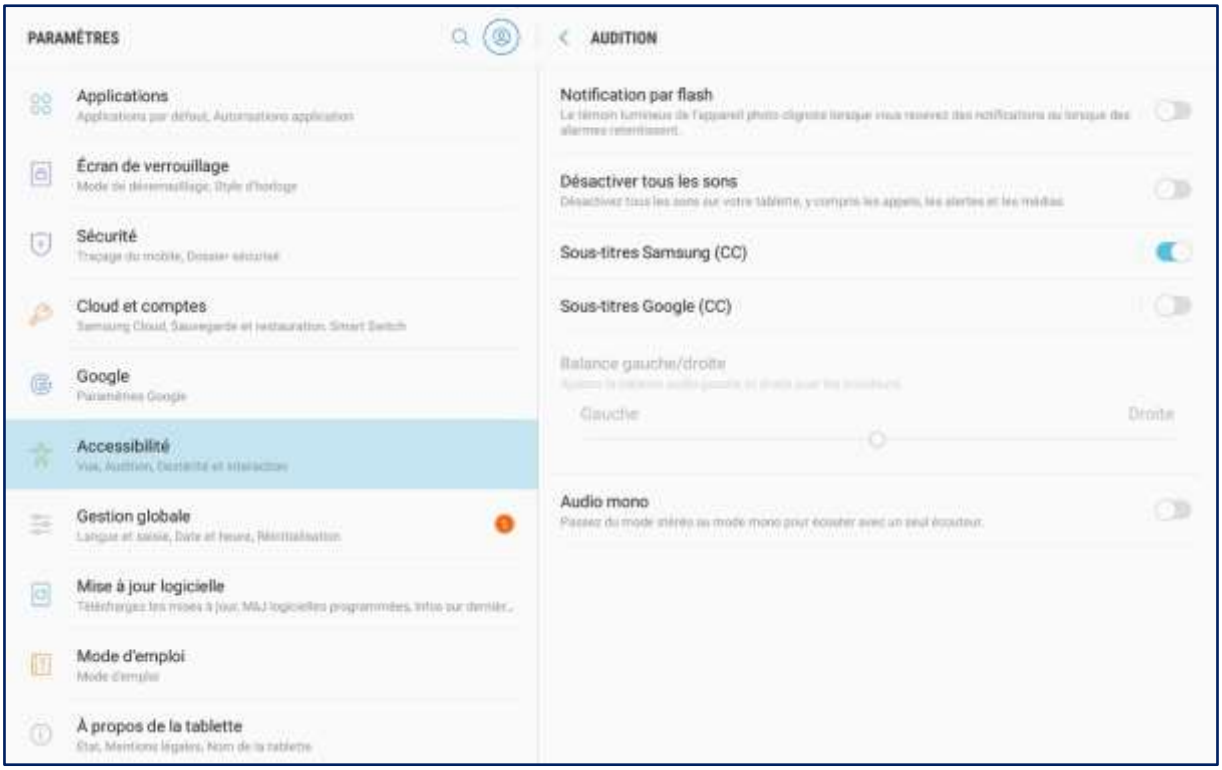
Accessibilité : Cet onglet vous permet d'affiner la configuration de vos affichages et modes d'utilisation. Il vous donne de multiples possibilités de personnalisation. Si vous avez des problèmes de vue, d'audition ou de manipulation, vous avez de grandes chances de pouvoir configurer votre mobile afin qu'il puisse répondre au mieux à vos besoins. Nous ne détaillerons pas ici tous les outils possibles, mais n'hésitez pas à tester toutes les options proposées pour trouver celles qui vous conviennent le mieux.



Vue :



Audition



Google Play

- Votre tablette est entièrement personnalisable. Vous pouvez installer des applications via Google Play, gratuites ou payantes pour de nombreuses utilisations.

- Google Play est divisé en plusieurs catégories : Applications, Films, Musique, Livres. Chacune est à nouveau répartie en plusieurs catégories pour vous permettre d'explorer plus finement les applications.

- En cliquant sur les trois traits en haut à gauche, vous accédez aux options et paramètres de Google Play, liés à votre compte.

- Sur la barre supérieure, un champ de recherche, signalé par une loupe, permet de réaliser une recherche par mots-clés.

- Pour installer une application, sélectionnez-la et cliquez sur « Installer ». Une barre de progression s'affiche pour montrer l'évolution.

- Une fois installée vous pouvez la lancer directement de Google Play ou du raccourci installé sur le bureau.

- Pour désinstaller une application vous pouvez le faire dans Google Play ou dans les paramètres de la tablette.

Dix régles de sécurité

1. Utiliser des **mots de passe de qualité**. Le dictionnaire définit un mot de passe « comme une formule convenue destinée à se faire reconnaître comme ami, à se faire ouvrir un passage gardé ». Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficile à retrouver à l'aide d'outils automatisés, et difficile à deviner par une tierce personne (ex : majuscules, minuscules, lettres, chiffres, caractères spéciaux).

2. Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc. La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de **mettre à jour tous ses logiciels** afin de corriger ces failles.

3. Effectuer des **sauvegardes régulières**. Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de ses données est une condition de la continuité de votre activité.

4. **Désactiver par défaut les composants ActiveX et JavaScript**. Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes, mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. En dépit de la gêne que cela peut occasionner, il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.

5. **Ne pas cliquer trop vite sur des liens**. Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.

6. **Ne jamais utiliser un compte administrateur pour naviguer**. L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'Internet. En limitant les droits d'un utilisateur, on limite aussi les risques d'infection ou de compromission de l'ordinateur.

7. **Contrôler la diffusion d'informations personnelles**. L'Internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir…

8. **Ne jamais relayer des canulars**. Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.

9. Soyez prudent : l'Internet est une rue peuplée d'inconnus ! Il faut rester vigilant ! Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou toute autre langue) il convient de ne pas l'ouvrir. En cas de doute, il est toujours possible de confirmer le message en téléphonant. D'une façon générale, **il ne faut pas faire confiance machinalement au nom de l'expéditeur** qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.

10. **Soyez vigilant avant d'ouvrir des pièces jointes à un courriel** : elles colportent souvent des codes malveillants. Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme une pièce jointe appelée photos.pif) ; .com ; .bat ; .exe ; .vbs ; .lnk. À l'inverse, quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus « inerte » possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations.

Et quelques curiosités...

Démarches administrative

- Applications bancaires
- Compte Ameli de la CPAM
- Impots.gouv.fr
- Retraite …

S'informer

- Cocm.fr
- HappyVisio
- Ouest-France, La Manche Libre, Météo
- Yuka, Frigo Magic, BuyOrNot …

Se divertir

- Replay TV
- Ciné Seniors
- Jeux de mémoire
- Code de la route …

Bouger Voyager

- Blablacar
- Transports.manche.fr
- Tripadvisor, Kayak, Trivago
- Ministère des affaires étrangères …

Communiquer S'organiser

- Boîte mail, Agendas
- Photos
- Facebook, Instagram, Snapchat
- WhatsApp, Messenger, Signal, Skype …

Sport Santé

- Activ'dos
- Medisafe
- Exercices à la maison
- VisoRando …

Loisirs

- Jardinage : Gardening, Calendrier du potager, Lune et jardin
- Cuisine : Marmiton, P'tit Chef
- Et tous vos centres d'intérêt …