# Atelier numérique du 15 octobre

*Protéger ses données personnelles*

Ateliers numériques Orange

# Protéger ses données personnelles



Bonjour et Bienvenue à toutes et tous pour cet atelier numérique qui aujourd'hui est dédié à la Protection des données personnelles.
En effet cet atelier fait partie d'un plus large programme proposé par l'entreprise Orange qui a pour Objectif d'accompagner dans leurs usages du numériques toutes les personnes qui le souhaitent qu'elles soient clientes Orange ou pas. Ainsi Orange veut favoriser l'égalité numérique et rendre ce numérique, devenu quasi incontournable dans notre quotidien, accessible à tous.

| | |
|---|---|
| Une donnée personnelle, c'est quoi ? | 2 – Protéger vos données personnelles. |
| 3 – Sécuriser vos équipements | 4 – Questions |

## Les données personnelles sont partout


Les données sont donc partout et vont très variées :
Un nom, prénom, adresses email et postale, un numéro de téléphone, une géolocalisation, une photo/vidéo, des traces de connexion et navigation, un numéro de sécurité sociale, un identifiant en ligne, un mot de passe, un numéro de carte bancaire …

Il en existe une définition officielle qui a été fixée en 1978 par la loi informatique et Libertés .

« Une donnée personnelle est toute information se rapportant à une personne identifiée ou identifiable directement ou indirectement ( y compris dans le domaine professionnelle)

## Communiquer des données personnelles facilite le quotidien

- **Démarches administratives**
- **Géolocalisation**
- **Achat / vente en ligne**
- **Ecoute de musique, lecture d'un livre ou d'un journal,**
- **Réseaux sociaux**
- **Sécurisation du domicile, veille sur sa santé, contrôle d'accès…**

**Mais attention à ne partager que celles qui sont utiles !**

5

Communiquer, s'informer, se divertir, … utilisez des applications et services à partir de votre mobile /tablette/PC vous simplifie la vie au quotidien, vous permet de gagner du temps, d'éviter des déplacements….

Par exemple :

- Effectuer des démarches administratives : demander une copie d'acte de naissance, remplir sa déclaration d'impôt,
- Se géolocaliser et se déplacer : trouver rapidement un itinéraire, un restaurant, un cinéma ou une station service, une place de parking à proximité de son lieu de RDV
- Rechercher un emploi, …
- Télécharger et écouter de la musique, un livre, lire le journal, …
- Acheter / vendre en ligne : acheter un billet de train, envoyer un recommandé, réserver une place de cinéma, acheter/vendre sur le bon coin …
- Sécuriser son domicile, surveiller son poids avec un pèse-personne connecté,… grâce à des objets connectés - appelé internet des objets (IOT).
- Partager des photos/vidéos … sur les réseaux sociaux

Ensemble, nous venons de prendre conscience de la masse de données personnelles que nous laissons circuler, de ce qu'elles disent de nous, et la manière dont elles sont collectées, stockées et peuvent être exploitées.

Qui d'entre vous a été démarché par téléphone, mail ou exposé à des bannières publicitaires non souhaité suite à une recherche internet ? Comment se protéger efficacement et vous préserver des publicités ciblées en fonction de votre localisation, vos traces de navigation … ?

| | |
|---|---|
| 1 – **Une donnée personnelle, c'est quoi ?** | **Protéger vos données personnelles.** |
| 3 – **Sécuriser vos équipements** | 4 – **Questions** |

Exemple : vous ne donnez pas vos coordonnées personnelles ou clefs à n'importe qui dans la rue. Sur internet, c'est pareil.

Comment se protéger efficacement et garder la maitrise des données diffusées ?

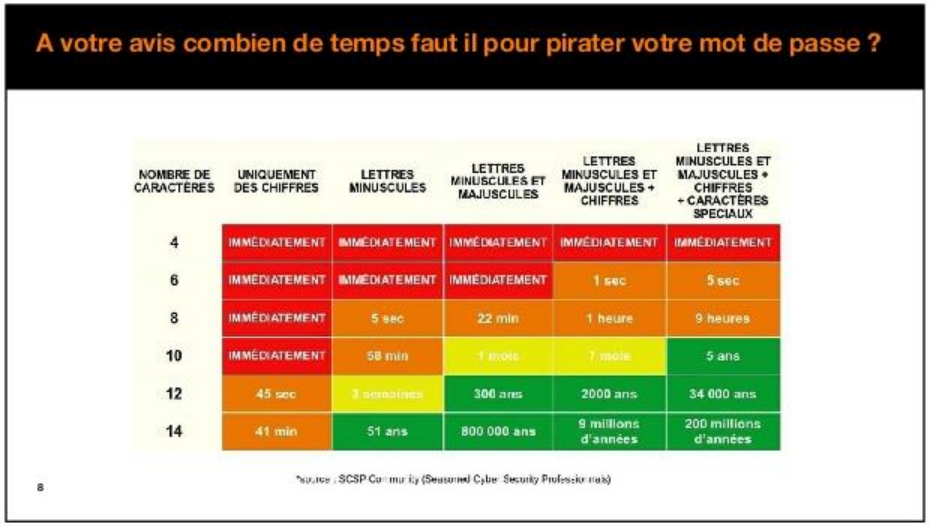
## Protéger ses données personnelles sur Internet

- Choisir un mot de passe robuste
- Sécuriser ses achats sur Internet
- Prévenir l'usurpation d'identité
- Effacer ses traces de navigation
- Gérer régulièrement les paramètres de confidentialité de ses navigateurs/terminaux

7

Il suffit d'être prudent, d'adopter quelques conseils simples pour vous protéger et de ne communiquer que ce qui est strictement nécessaire

Voici 5 conseils utiles … que nous allons développer




1er conseil : définir un mot de passe robuste, facile à retenir et qui ne dit rien sur vous !

Imaginons que votre mot de passe de messagerie soit votre date de naissance. Il est alors très facile pour une personne peu scrupuleuse de deviner ce mot de passe, d'accéder à votre boite mail et de prendre le contrôle de votre vie numérique.

Comment est-ce possible ?

- de nombreuses données personnelles sont stockées dans vos emails archivés
- le pirate pourra également demander à réinitialiser le mot de passe sur les sites sur lequel vous faites des achats en ligne, en cliquant « mot de passe perdu »

Le choix d'un mot de passe difficile à deviner **est donc la première action** à mener pour sécuriser l'accès aux données personnelles enregistrées sur vos équipements (tablette, téléphone, ordinateur mais aussi les objets connectés) et vos comptes sur internet (messagerie, banque, sécurité sociale, réseaux sociaux,…).

A privilégier :
- Choisir un mot de passe long (minimum 12 caractères – recommandation de la CNIL), composé de chiffres, de lettres minuscules et majuscules et de caractères spéciaux
- Utiliser un mot de passe spécifique pour chaque compte sensible (banque, messagerie,…) et le changer au moins deux fois par an

## Comment choisir un mot de passe robuste ?

**Un mot de passe long (minimum 12 caractères), pour le retenir facilement:**

- **Choisir le titre d'un livre/film/chanson/slogan/phrase**
  - **Lepetitprince**
  - **Onconnaitlachanson**
- **Ajouter au moins un chiffre et un caractère spécial (* ! $...) : 24***
- **Choisir les deux premières lettres en majuscule du site internet/service concerné : OR pour Orange / EN pour Engie**

**Lepetitprince24*OR**

**La méthode des premières lettres peut aussi être utilisée**
**Exemple : le proverbe « On n'est jamais mieux servi que par soi même » donnera**

9 **On'ejmsqpsm24**

Prenons un exemple :
Pour créer un mot de passe robuste et qui ne dit rien sur vous, vous pouvez par exemple : prendre la première lettre du titre d'un livre/ un film ou d'une chanson ou d'une phrase que vous retenez facilement : **Lepetitprince** / **Onconnaitlachanson**

- ajouter des chiffres et un symbole : 24*
- personnaliser avec les deux premières lettres en majuscule du site internet nécessitant un mot de passe : OR pour Orange (ce qui le rendra unique et facilite votre mémorisation)

**Lepetitprince24*OR (OR comme Orange)**
**Onconnaitlachanson24*EN (EN comme ENGIE)**

Veillez lors du paramétrage de vos équipements cad votre smartphone mais aussi vos objets connectés (pèse-personne, capteur météo….) à choisir aussi un mot de passe robuste et ne communiquez que les informations pertinentes (cad le moins possible).
Pensez aussi à choisir un code de verrouillage de votre smartphone/tablette robuste (préférez un nombre aléatoire à une année).
Et surtout, … ne jamais écrire son mot de passe sur un support non sécurisé (exemple : post-it collé sur l'ordinateur ou le mobile).

Quand vous ne les utilisez pas, veillez à déconnecter, voire à débrancher, vos objets connectés : comme tous les équipements numériques, ils peuvent être la cible de cyber-attaques visant à les intégrer à un «Botnet ».

Combien de mots de passe avez-vous ? (sondage dans la salle)

**Pour vous aider, il existe des solutions sécurisées libres sur le marché pour conserver ses mots de passe dont la sécurité a été évaluée par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) :**
**(Exemple : l'application keepass.fr que vous pouvez télécharger sur internet, véritable « coffre-fort pour mot de passe »)** *Je ne sais pas dans quelle mesure cette solution est aussi efficace que celle que nous utilisons, avec un clé PKI à l'appui*

## Comment sécuriser vos achats sur Internet ?

- **Se renseigner sur le site avant d'effectuer un achat**
- **S'assurer que le champ adresse de son navigateur est bien en httpS://**
- **Eviter de stocker son numéro de carte bancaire et son mot de passe sur un site internet**
- **Sur le mobile / tablette : préférer les sites connus et vérifier les notes et le nombre de téléchargements sur le store consulté**

10

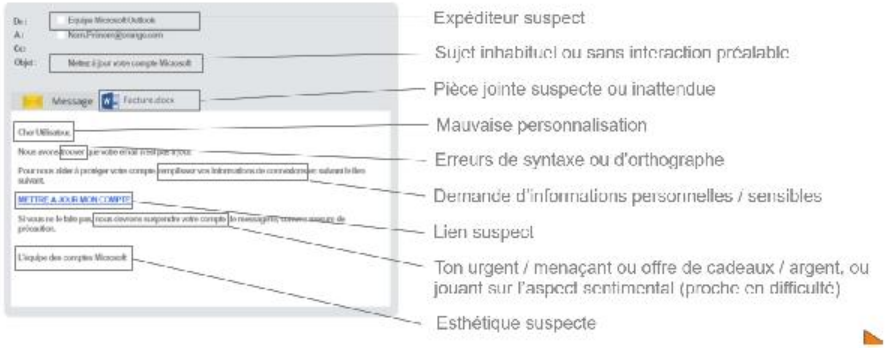
Il est désormais courant de faire ses achats en ligne, mais il est important d'être vigilant pour éviter qu'une personne mal intentionnée n'usurpe vos moyens de paiement.
Si vous avez enregistré vos cartes bancaires sur un site de commerce en ligne et qu'en plus, votre mot de passe est 1234, vous *pouvez* avoir des surprises !
En ligne, comme dans la vie quotidienne, faites appel à votre bon sens et agissez avec prudence.

A privilégier :
- Chercher des informations ou des avis clients si l'enseigne est inconnue en tapant « avis + Nom de l'enseigne » sur un moteur de recherche
- Limiter ses achats aux sites proposant un système de paiement sécurisé en « https:// » (conseil valable également pour les achats réalisés sur smartphone)
- Ne pas enregistrer son numéro de carte bancaire et le cryptogramme visuel sur les sites marchands. Ces informations ne doivent être conservées que le temps de la réalisation de la transaction.
- Lors du paiement sur internet, ne jamais donner son code confidentiel à 4 chiffres
- Pour un achat sur mobile, préférer les applications les plus téléchargées sur des stores/places de marché reconnus et regarder les notes des applications


L'hameçonnage (en anglais: « phishing ») constitue une « attaque de masse » qui vise à abuser de la « naïveté » des clients *en utilisant une fausse qualité (le fraudeur se fait passer pour telle ou telle entreprise)* ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire… ou autres données.

## Comment reconnaître un mail de Phishing ?

Voici comment ce type d'attaque peut être détecté par les utilisateurs :




Comment reconnaitre un « phishing » ?

- Des informations confidentielles sont systématiquement demandées
- Les e-mails frauduleux contiennent souvent (mais pas toujours) des fautes d'orthographe ou de syntaxe
- L'adresse de l'expéditeur ou le site vers lequel vous êtes redirigé sont approximatifs (www.micosoft.com) : vous pouvez le vérifier en mettant votre souris sur le lien du texte qui est souvent inhabituellement long et compliqué
- Le fraudeur insiste sur le caractère urgent du mail (compte bloqué, facture en impayée, ami en détresse,…) ou sur un gain potentiel (remboursement, loterie,…)

## Savoir reconnaitre une tentative d'usurpation d'identité

- **Ne jamais répondre aux mails ou SMS vous demandant des informations confidentielles**
- **Ne jamais cliquer sur les liens/pièces jointes d'un interlocuteur que vous ne connaissez pas**
- **En cas de tentative de phishing, signalez auprès de :**
  - **abuse@orange.fr**
  - **l'entité/organisme concerné ou la plateforme https://www.signal-spam.fr/**
- **S'il s'agit d'un SMS frauduleux, répondez STOP* et en cas de récidive ou de spam vocal, contactez ou transférez-le gratuitement au 33700**

A retenir :
- Sachez que jamais Orange ne vous contactera ~~pas~~ *jamais par* mail pour vous demander des données personnelles
- Si vous recevez un phishing par mail,
  . ne cliquez pas sur les liens/pièces jointes inclus dans l'email.
  . Si c'est une tentative au nom d'Orange, vous pouvez transférer le mail à abuse@orange.fr qui procèdera aux vérifications nécessaires.
  . Sinon signalez-le à la société/organisme concerné ou vous pouvez contacter la plateforme https://www.signal-spam.fr/
- S'il s'agit d'un SMS frauduleux, répondez STOP pour faire cesser l'envoi. En cas de récidive, transférez-le au 33700, plateforme de signalisation multi-opérateurs.

En cas d'usurpation *de votre* identité,
- Contactez au plus vite le service relations clients du service concerné ~~ou conseiller bancaire~~
- Surveillez vos comptes et contestez l'opération auprès de votre Banque et déposez plainte auprès de la police (démarche en ligne).

Autre point d'attention, votre historique de navigation ou une conversation sur webcam peuvent être enregistrés pour servir de moyen de pression.
Votre historique de navigation ou une conversation sur webcam peuvent être enregistrés pour servir de moyen de pression. Ces phénomènes sont observés dans le cas, d'une usurpation d'identité ou d'un contrôle à distance de son équipement (Cf. slide pensez à mettre un mot de passe robuste).
*Attention, on parle de vrais enregistrements ? Parce qu'en général il s'agit uniquement de chantage (cf sur les prétendues détentions d'images pornographiques)*

## Se préserver des appels indésirables et démarchage illégal

- **Une application téléchargeable sous Android et iPhone**
- **Gratuite et sans publicité**
- **Accessible à tous***

**Orange Téléphone**

* Fonctions avancées pour les clients Orange

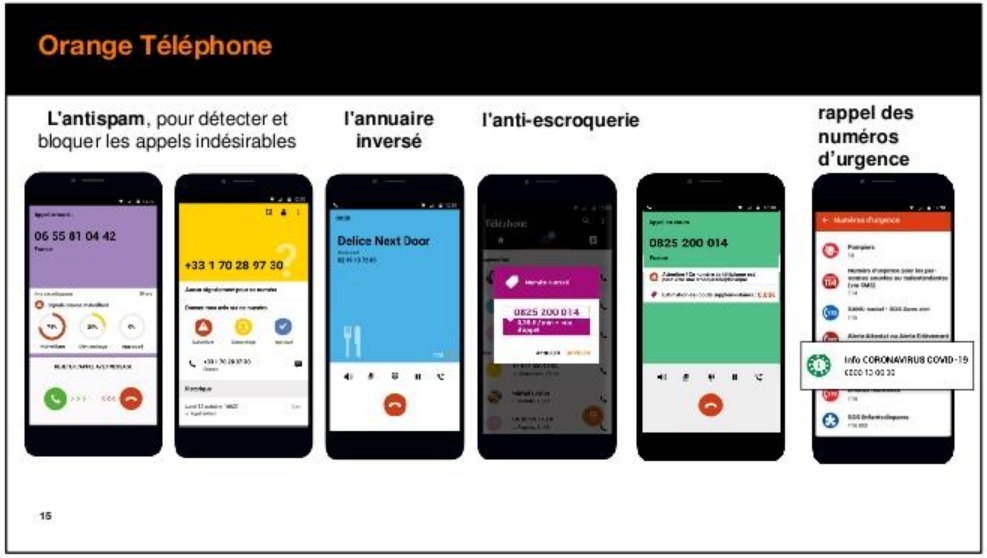
**Comment lutter contre le démarchage abusif ?**

Les appels indésirables et le démarchage illégal envahissent de plus en plus la vie privée des utilisateurs de téléphones fixes et mobiles. Qu'il s'agisse de messages préenregistrés ou bien de démarchage publicitaire sous un faux numéro, les consommateurs souhaitent des solutions pour lutter contre ces nuisances devenues insupportables au quotidien.
Gratuite et accessible à tous sur Android et iOS,S, l'application Orange Téléphone renforce la protection contre les appels indésirables et les « arnaques » sur les mobiles.

Cette application permet d'obtenir des informations sur la nature des appels entrants grâce à une protection contre les appels indésirables (qui informe ou bloque en cas d'appel malveillant ou de démarchage). Elle possède aussi une fonctionnalité d'annuaire inversé qui affiche le nom des professionnels même s'ils ne sont pas enregistrés dans les contacts.
Orange Téléphone protège enfin ses utilisateurs contre les « mauvaises surprises » téléphoniques en les informant lorsqu'ils composent par exemple un numéro surtaxé.

Ce service a été mis en place conformément à la décision de l'ARCEP du 11 juillet 2019, en coordination avec l'ensemble des acteurs.
Cette application dénombre déjà plus d'1,5 million d'utilisateurs actifs mensuels.

Orange est également engagé dans la liste d'opposition au démarchage téléphonique (Bloctel), et ce depuis la création de celle-ci. Cette liste permet aux consommateurs inscrits de ne plus être dérangés par les entreprises dont ils ne sont pas clients.




*Démonstration*

**1ère fonction: L'antispam**, pour détecter et bloquer les appels indésirables
Quand je reçois un appel téléphonique, avant même de décrocher, je vois à l'écran que l'appel est malveillant : c'est un spam, probablement un escroc : je rejette l'appel pour être tranquille !
Et je peux facilement signaler les appels malveillants pour alerter les autres utilisateurs.

**2ème fonction : l'annuaire inversé**, Lorsque je reçois un appel téléphonique, je vois «le nom de la société» même si ce contact n'est pas dans son carnet d'adresses. À partir de maintenant, avec l'annuaire inversé, Philippe sait qui l'appelle.

**3ème fonction**: **l'anti-escroquerie**
Enfin, quand je veux rappeler un numéro inconnu ou un numéro surtaxé, je peux avoir des surprises sur le coût d'appel !
Heureusement, avant d'appeler, des informations sur le prix de la communication s'affichent sur mon écran !
*(j'appelle un numéro surtaxé : 118 707)* je vois sur l'écran qu'il est payant (2,99€ par appel + 2,99 € par minute) avec la couleur rose (code couleur utilisé en France) et le cout de l'appel s'affiche en temps réel lors de l'appel.
***4ème rappel des numéros d'urgence***

## Pourquoi effacer ses traces de navigation ?

**Vous vous renseignez sur un site de vente d'électroménager pour acheter une télé 4K.**

**Et quand vous visitez le site d'information 20 minutes :**


16

Imaginons que vous souhaitez acheter une télévision Ultra Haute Définition pour suivre le Mondial de football.
Vous effectuez quelques recherches sur internet pour comparer les différents modèles et les prix.
Quelle n'est pas votre surprise de retrouver sur de nombreux sites Internet que vous consultez, une publicité pour le modèle que vous aviez pré-sélectionné !

C'est ce que l'on appelle de la publicité ciblée qui est rendue possible par l'utilisation de vos données de navigation, localisation …
Comment cela fonctionne-t-il ?

## Comment effacer ses traces de navigation ?

1. **Supprimer son historique de navigation et ses cookies**
2. **Naviguer en mode privé**

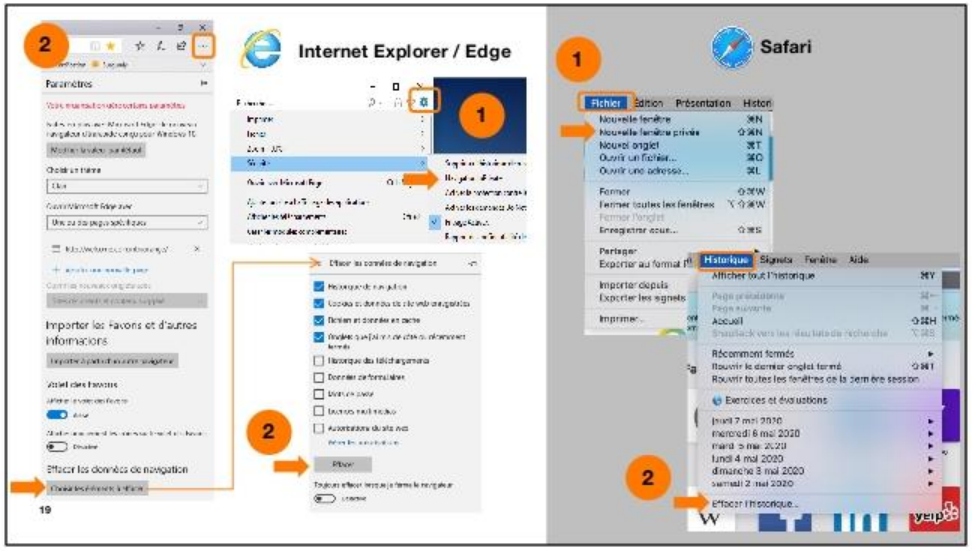
17

Les recherches que nous effectuons chaque jour en disent énormément sur qui nous sommes : des infos sur vos prochaines vacances, une recherche sur une maladie, une carte pour savoir quelles routes empruntées, un produit que vous avez *envie* d'acheter ?

Certains annonceurs/entreprises utilisent des « cookies » pour suivre vos visites sur les différents sites web où ils ont mis de la publicité. Un « cookie », qu'est-ce-que c'est ?

Un cookie est un petit fichier texte, enregistré sur votre ordinateur lorsque vous effectuez des recherches sur Internet. Il contient un certain nombre de données obtenues par le concepteur du site lui permettant de personnaliser ses pages et de les adapter à votre profil.
La réglementation prévoit que les sites internet doivent recueillir votre consentement avant le dépôt de ces cookies (« opt in »). Ils doivent également vous indiquer à quoi ils servent et comment vous pouvez vous y opposer.

Comment les désactiver facilement ?




Sur internet explorer
Dans les paramètres , aller dans sécurité
Et utilisation des données de navigation

Dans Safari ( sur Mac)
Fichier / Nouvel fenêtre en mode privée
Historiques / Effacer l'historique

## Navigation privée sur son smartphone – apple / iphone


Démonstration sur votre smartphone

Désactivation de partage automatique :

- Allez dans réglages / paramètres de confidentialité /
- Désactivez l'accès des applications à vos contacts, photos …

Mise en place de la navigation privée :

- Sur iphone, téléchargez et ouvrez l'application chrome *Par définition sur iPhone on utilisera Safari, donc pas sûre de l'opportunité de l'exemple*
  → Appuyez sur plus en haut à droite choisissez « Nouvel onglet de navigation privée »
- Sur Android,
  → Ouvrez l'application Internet, puis cliquez sur l'icône en haut à droite représentant 3 petits points verticaux, puis sur « Nouvel onglet de navigation privée »

## Navigation en mode privée sur son smartphone – android




Démonstration sur votre smartphone

<u>Désactivation de partage automatique :</u>

- Allez dans réglages / paramètres de confidentialité /
- Désactivez l'accès des applications à vos contacts, photos …

Mise en place de la navigation privée :

- Sur Android,

  → Ouvrez l'application Internet, puis cliquez sur l'icône en haut à droite représentant 3 petits points verticaux, puis sur « Nouvel onglet de navigation privée »

| | |
|---|---|
| 1 – Une donnée personnelle, c'est quoi ? | 2 – Protéger vos données personnelles. |
| Sécuriser vos équipements | 4 – Questions |

## Sécuriser ses équipements (PC, smartphone, tablette, objets connectés)

- **Mettre à jour ses logiciels.**
- **S'équiper d'un antivirus ou suite de sécurité.**
- **Sauvegarder ses données.**
- **Eviter de connecter ses appareils numériques à des accès wifi public comme votre liseuse électronique ou votre tablette plus susceptibles d'être piratés.**

23

Quelques conseils pour protéger et sécuriser vos équipements … et donc vos données :

Installer un antivirus et mettre à jour régulièrement vos logiciels est une façon simple d'éviter la plupart des attaques. Pour cela, je vous conseille d'accepter les mises à jour automatiques qui vous sont proposées pour améliorer la sécurité de votre ordinateur, mobile ou tablette/objet connecté.

Attention, sur vos équipements mobiles, veillez à ne faire les mises à jour qu'en wifi, à la maison, faute de quoi votre forfait données pourrait diminuer rapidement.

Les éditeurs de logiciels mettent tout en œuvre pour renforcer leur sécurité, les cybercriminels étant à l'affut de la moindre faille. Equipez vous d'un anti-virus efficace pour ne pas vous retrouver face à un écran noir (à cause d'une panne ou d'un piratage) et programmez sa mise à jour très fréquemment (une fois par semaine au moins)
Protéger tous vos équipements (votre webcam, …)
Sauvegarder régulièrement vos données/fichiers (et ceux/celles de vos proches) contenus sur son ordinateur, sa tablette ou son smartphone sur un support externe et mettez les, en lieu sûr avec

- **→Les sauvegardes physiques**

Selon le volume qu'occupent vos fichiers, vous pouvez utiliser une clé USB ou un disque dur externe. Vous pouvez également stocker vos données en les gravant sur un DVD. Attention, ces supports physiques ont l'inconvénient d'être relativement fragiles.
Les sauvegardes virtuelles : déposez vos fichiers sur un service de stockage dématérialisé comme le « cloud » (nuage en français) qui est un espace de stockage en ligne privé et confidentiel sur lequel vous pouvez sauvegarder, consulter et partager vos fichiers pour les consulter où vous voulez, quand vous voulez, sur l'écran de votre choix (ordinateur, smartphone, tablette vos photos, vidéos…
Par exemple : Icloud / Google Drive / Dropbox / Microsoft Drive / PCloud…
- Enfin, évitez de connecter vos appareils numériques à des accès wifi public comme votre liseuse électronique ou votre tablette plus susceptibles d'être piratés.
- N'installez pas d'applications tierces quand vous n'en avez pas besoin ou si vous considérez que la masse d'informations collectées est disproportionnée par rapport au service rendu.

Rebond : invitez les participants à se renseigner auprès d'un conseiller Orange sur la suite de sécurité Orange.

(Client orange Internet ) L'option Suite de Sécurité Orange, grâce à la technologie Kaspersky Lab (société spécialisée dans la sécurité des équipements, partenaire d'Orange), assure une protection robuste et complète pour vos ordinateurs, Windows ou Mac OS et pour vos smartphones et vos tablettes Android. Si vous êtes détenteurs d'une offre Livebox Jet ou Open Jet (1), installez gratuitement la Suite de Sécurité Orange, elle est incluse dans votre offre (sinon 5 euros/mois). Vous pouvez protéger jusqu'à 5 appareils (10 pour les professionnels, mais attention le prix est plus cher). Elle comprend notamment un firewall, un anti-phishing, un anti-spam et une protection bancaire pour des achats en ligne en toute sérénité. En cas de vol de votre smartphone, par exemple, votre Suite sécurité vous permettra de le localiser et, si besoin, de supprimer à distance certaines informations confidentielles.


**Nous voici arrivés à la fin de cet atelier, j'espère que ce moment d'échange vous a plus et qu'il a répondu à vos attentes. Je vais vous transmettre par mail le support de présentation. Dans ce mail, vous retrouverez aussi le lien pour vous connecter au site d'inscription des ateliers numériques. Je vous rappelle qu'il existe 7 thématiques différentes toujours sur les usages du numérique. N'hésitez à vous inscrire je serai ravie de vous accueillir de nouveau.**
**Vous allez aussi recevoir d'ici 48h un questionnaire de satisfaction et je vous encourage vraiment à y répondre. C'est rapide, quelques minutes et entièrement confidentiel. Vous allez pouvoir nous dire ce qui vous a plus mais aussi nous préciser ce qui pourrait être amélioré : vos remarques, suggestions sont précieux pour nous car ils nous permettent d'optimiser ces ateliers pour qu'ils répondent au mieux à vos attentes.**
**C'est fini je vous ai tout dit, je vous remercie pour votre écoute et vous souhaite une bonne journée.**

Annexes:
Orange a développé le site « Bien vivre le digital » afin de vous donner des conseils et des astuces pour vivre le monde digital en toute sérénité.
Vous y retrouverez l'ensemble des conseils, vidéos, paroles d'experts, quiz et bien plus encore dans la rubrique « mes données, mon identité ».

Orange propose aussi des prestations individuelles pour vous accompagner dans la découverte et usages de votre smartphone. La prise de rendez vous s'effectue auprès de vos conseillers.
- Configuration mobile flash (9 euros) : **activer votre nouveau mobile, transférer vos contacts**
- Configuration mobile experte (24 euros) : **activer votre nouveau mobile, transférer vos contacts,**

**transférer vos photos, vidéos, SMS/MMS**
**configurer votre boîte email, configurer votre compte Store, télécharger l'application Orange et moi**
**+ découvrir des bonnes pratiques pour le bon fonctionnement de votre mobile**
→ http://basic.sso.francetelecom.fr/basic/ccil_custom/common/genericrenderer.jsp