LIVRET RESSOURCE INTERACTIF POUR LES AIDANTS NUMERIQUES

Auteurs : Jean-François Cauche et Lucia Debévère

Date : 15 juin 2021

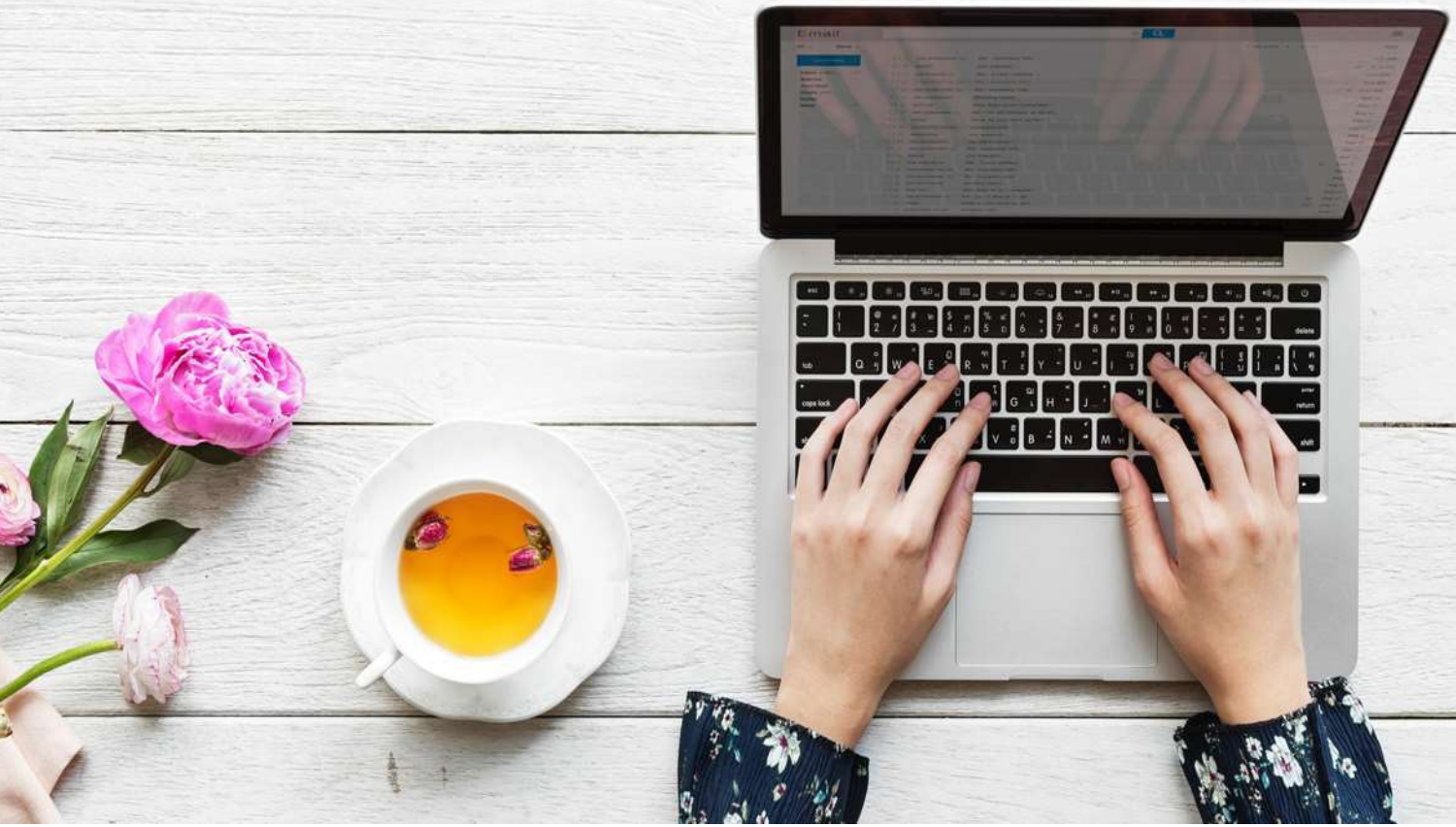


TABLE DES MATIÈRES

LICENCE CREATIVE COMMONS DU LIVRET

Le livret est publié sous licence Creative Commons. Vous pouvez l'utiliser librement, en respectant ces conditions :

- Maintenir la paternité du contenu (citer les noms des auteurs)
- Aucune utilisation commerciale y compris pour de la formation rémunérée,
- Aucune modification du livret.

Toute personne qui ne respecte pas ces conditions, s'expose à des poursuites.

DEMATERIALISATION ET FRACTURE NUMERIQUE

Alors que le Gouvernement veut **dématérialiser 100% des démarches administratives d'ici 2022** dans le cadre d'Action publique 2022**, l**e numérique fait apparaître de nouvelles inégalités, entre ceux qui maîtrisent cette technologie et ceux qui en sont exclus : **la fracture numérique .**

- **Près de 30%** de la population reste **éloignée du numérique.**
- **« L'illectronisme" = l'illettrisme numérique** qui dissuade ceux qui ne savent pas utiliser Internet à accomplir certaines tâches, notamment leurs démarches en ligne.

Axes de la transformation numérique dans le cadre d'action publique 2022 :

- Tendre vers 100% de démarches administratives numérisées à l'horizon 2022
- Développer un État plateforme offrant des services numériques nouveaux et optimisés
- Repenser, avec l'ouverture des données publiques notamment, les relations entre les citoyens et l'administration
- Transformer les politiques publiques et les méthodes de l'administration à l'aune du numérique

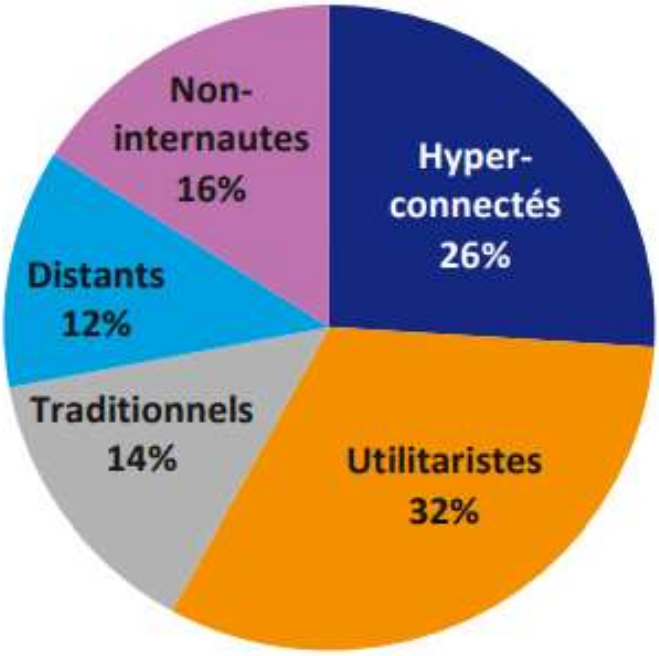
De plus, l'Etat n'est pas le seul à dématérialiser :

- Les collectivités locales le font aussi pour leurs services
- Ainsi que les entreprises

Par exemple les banques et les assurances dématérialisent de plus en plus les comptes et les démarches de leurs clients, via des applications ou des sites internet.

C'est pourquoi, il est important que les usagers soient compétents dans l'utilisation des outils numériques et puissent acquérir une culture numérique.

Les profils des internautes



Source : M@rsouin, enquête Capacity 2017

- 16% sont des « **non-internautes »** qui ne se connectent jamais à Internet

- 12% sont des **« internautes distants »** qui disposent de compétences numériques très faibles

- 70% des **« internautes distants »** n'ont jamais effectué au moins une démarche administrative en ligne

- Alors que **80% de l'ensemble des internautes français**, ont déjà effectué une démarche en ligne.

Les groupes 1 et 2

(Les moins pénalisés par la dématérialisation)

GROUPE 1

Usages des hyper connectés

Groupe 1 : Les hyper connectés (26% de la population)

Les spécialistes des échanges entre pairs sont des utilisateurs experts

- Les membres de ce groupe sont plutôt des hommes (53%)
- soit jeunes adultes (38% de 25-39 ans)
- soit hauts diplômés (51% sont diplômés du supérieur)
- On les retrouvent principalement parmi les cadres (17%)

Les usages les plus fréquents des spécialistes des échanges entre pairs sont :

- Préparation d'un achat en ligne (96%) - Achat en ligne (86%)
- **Réalisation de démarches administratives, fiscales (90%)**
- Participation aux réseaux sociaux (82%)
- Ecoute et téléchargement de musique (73%)
- Consultation des notes et avis (88%)

- Recherche d'information santé (77%)
- Regarde la télévision en direct ou replay (68%)
- Regarde des films vidéos (73%)
- Téléphone via Skype (65%)
- Vend en ligne (72%)
- Donne des notes, des avis (58%)
- Recherche un emploi (42%)
- Recourt à un usage contre rémunération (89%)
- Propose un usage contre rémunération (87%)
- Echange sans rémunération (43%).

PROFIL 2

Usages des traditionnels

Groupe 2: Les « touche-à-tout » (14% de la population)

Les « touche-à-tout » utilisent, comme leur nom le laisse supposer, la plupart des activités étudiées avec des taux importants comme le groupe 1, mais à la différence des premiers, ils ne sont pas très attirés par les échanges entre pairs.

Comme le groupe 1, les « touche-à-tout » sont plus souvent des hommes

- et des jeunes adultes (42% ont entre 25 et 39 ans)
- le plus souvent diplômés (38% sont diplômés du supérieur).

- Tous les autres usages par contre sont massivement pratiqués :
- 93% écoutent de la musique,
- 76% regardent la télévision,
- **89% réalisent des démarches administratives**
- 50% recherchent un emploi,
- 94% achètent en ligne
- et 53% vendent en ligne.

PROFIL 3 (peu ou pas pénalisés par la dématérialisation +)

Les usages des utilitaristes

Groupe 3: les utilitaristes (32% de la population)

- **Les utilitaristes cantonnent internet à un outil pouvant simplifier la vie.**
- **Globalement plus âgés (48% d'entre eux ont entre 40 et 59 ans**, que les spécialistes des échanges entre pairs et les « touche-à-tout », les utilitaristes se distinguent par un niveau de vie très supérieur à la moyenne
- **Les utilisations se focalisent ainsi sur les démarches administratives, la préparation d'un achat, l'achat et la vente en ligne, la consultation des avis et commentaires, la recherche d'informations sur la santé, ou encore le téléphone via Skype**
- **Les utilitaristes sont ainsi peu attirés par les activités récréatives** que proposent internet (musique, télévision, vidéos), les réseaux sociaux ou les échanges entre pairs.

Les usages les plus fréquents des utilitaristes sont :

- Préparation d'un achat en ligne (92%)
- Achat en ligne (91%)
- **Réalisation de démarches administratives, fiscales (81%)**
- Consultation des notes et avis (75%)
- **Recherche d'information santé (63%)**
- - Téléphone via Skype (36%)
- - Vente en ligne (44%)
- Donne des notes, des avis (40%)

PROFIL 4 (assez pénalisés par la dématérialisation +++)

Les usages des jeunes

Groupe 5: les jeunes (14% de la population)

Principalement composé d'individus âgés de moins de 25 ans (6 cas sur 10)

- **le groupe des jeunes focalise les pratiques sur des activités récréatives**
- composé principalement d'élèves ou d'étudiants (55%) résidant en zone urbaine.

Les usages les plus fréquents des jeunes sont :

- Participation aux réseaux sociaux (81%)
- Ecoute et téléchargement de musique (96%)
- Regarde la télévision en direct ou replay (67%)
- Regarde des films vidéos (68%) - Téléphone via Skype (61%)

Et ceux en-dessous de la moyenne des internautes :

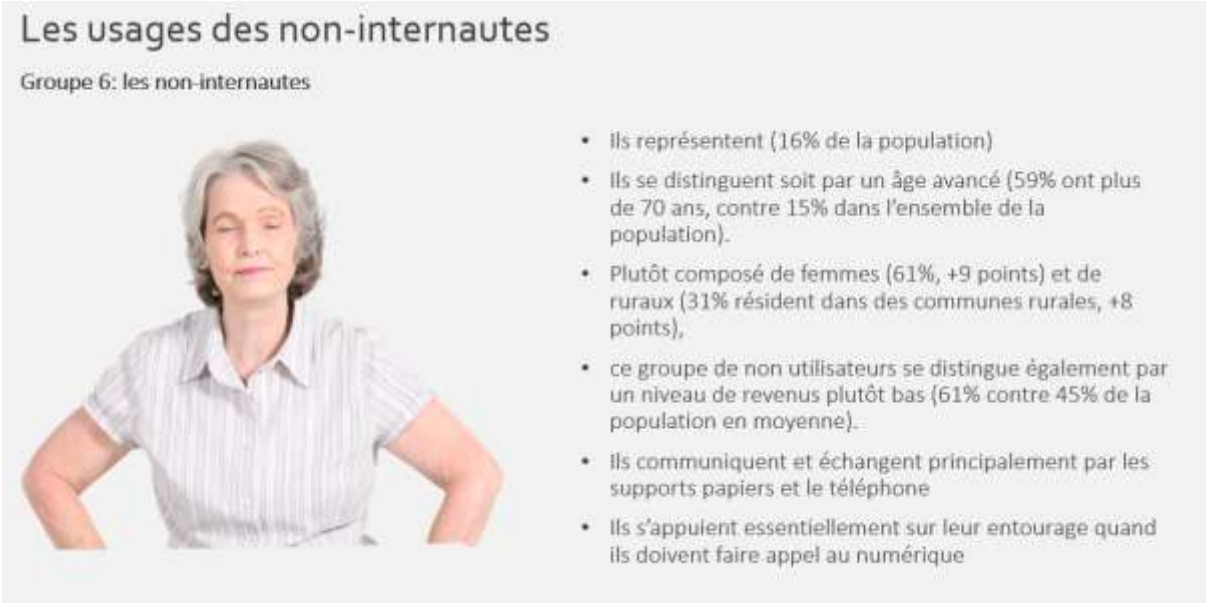
- Préparation d'un achat en ligne
- Achat en ligne
- **Réalisation de démarches administratives, fiscales**
- Consultation des notes et avis
- **Recherche d'information santé**
- Vend en ligne - Donne des notes, des avis
- **Recherche un emploi**
- Recourt à un usage contre rémunération
- Propose un usage contre rémunération
- Echange sans rémunération.

Les groupes 5 ET 6

(Les plus pénalisés par la dématérialisation ++++++)

PROFIL 5 (très pénalisés par la dématérialisation ++++)

PROFIL 6 (Fortement pénalisés par la dématérialisation ++++++)



Baromètre du numérique

D'après Le Baromètre du Numérique 2017, **81% de la population française possède un ordinateur, et 73% possède un smartphone**. Si ces chiffres progressent globalement sur les années suivantes, nombreuses sont encore les personnes qui ne possèdent pas d'équipement informatique ou de connexion internet.

Certains Français, même bien équipés en outils numériques, ont un usage moins développé des démarches administratives et fiscales en ligne.

En 2017, un Français sur trois n'a pas eu recours à l'e-administration et principalement :

- Des personnes âgées de 70 ans et plus
- Des non-diplômés
- Et des personnes aux bas revenus.

14 millions sont éloignés du numérique, soit 28% de la population de plus de 18 ans.

Rapport 2018 au « bénéfices d'une meilleure autonomie numérique »

L'objectif est de détecter les publics les plus éloignés du numérique et de les rendre les plus autonomes possible. 1,5 million de personnes doivent être formées par an.

La Mission Société Numérique, au sein de l'Agence du numérique, est chargée de mettre en œuvre cette stratégie avec les outils suivants :

La création d'un "pass numérique"

https://societenumerique.gouv.fr/pass-numerique/

Destiné aux personnes les plus en difficulté face au numérique, ce pass est remis par des agents des services publics (Pôle emploi, les caisses d'allocations familiales, les départements, les communes, etc.) ou des aidants numériques.

La mise en place de "hubs France connectée"

Il s'agit de structures locales référentes dans l'inclusion numérique, destinées à fédérer les acteurs du numérique à l'échelle locale et à aider les territoires à répondre aux besoins de leurs populations. 5 millions d'euros sont engagés en 2019-2020 par la Banque des territoires pour faire émerger 11 hubs territoriaux

Un plan de formation pour les aidants numériques

Par exemple, l'État a soutenu la coproduction d'un **MOOC** Enjeux et bonnes pratiques de la médiation numérique pour les territoires | CNFPT

- Un **site " Aidants Connect"** afin de sécuriser la connexion des aidants pour les démarches qu'ils font pour autrui. https://aidantsconnect.beta.gouv.fr/

- **Deux plateformes de ressources** sont également à disposition **des collectivités locales** (pass numérique) et **des aidants numérique (kit d'intervention rapide)**

- Elle propose notamment une **cartographie de France des lieux de médiations numérique** http://carto.assembleurs.co/

Stratégie nationale pour un numérique inclusif

En septembre 2018, une stratégie nationale pour un numérique inclusif a été présentée par le Gouvernement. Lors du 3e comité interministériel de la transformation publique (CITP) du 20 juin 2019

3 axes :

- La consolidation de l'outillage des médiateurs et des aidants numériques dans l'accompagnement des personnes
- Le développement de solutions d'accompagnement pour ceux qui peuvent et souhaitent être formés
- Et le soutien aux collectivités territoriales pour l'élaboration de réponses adaptées aux besoins des territoires

L'ouverture de **300 maisons "France Service"**

(Guichets uniques qui regroupent les principaux services publics)

- Un plan d'accessibilité téléphonique des administrations.

Le Conseil d'orientation de l'édition publique et de l'information administrative (Coepia) a publié, en janvier 2018, "Trente recommandations pour n'oublier personne dans la transformation numérique des services publics".

Une de ces recommandations est de "garantir aux usagers un accompagnement humain chaque fois que nécessaire".

C'EST NOTAMMENT LA MISSION DES AIDANTS NUMERIQUES

DEFINITION ET MISSION DES AIDANTS NUMERIQUES

Le terme « aidant numérique » peut renvoyer à différentes définitions.

Dans le rapport Plan National pour la formation des médiateurs et des aidants numériques, **le terme « aidant numérique » désigne les professionnels de l'accès aux droits et aux services publics, dont les pratiques sont bouleversées par la dématérialisation :**

- Les travailleurs sociaux,
- Les agents en charge des missions d'accueil, d'information, d'orientation des usagers des services publics, ...

Mais parmi les aidants, se trouvent aussi :

- Des salariés ou bénévoles d'association
- Des salariés d'entreprises qui aident ces publics
- Des membres de la famille d'un usager mis sous tutelle par exemple

- Ils sont en première ligne face aux usagers en difficultés avec le numérique alors que l'accompagnement des publics dans leurs usages numériques ne constitue pas toujours le cœur de leurs missions.
- Ils sont confrontés à des problèmes de formation sur les outils numériques et sur la manipulation de données personnelles des usagers. Ils ont besoin de sécuriser leurs interventions.

La mission des aidants numériques :

- Une information générale sur les démarches administratives (réponses aux questions, accompagnement des démarches administratives du quotidien comme la déclaration de revenus, la gestion du prélèvement à la source, le renouvellement des papiers d'identité, du permis de conduire et de la carte grise...)
- Un accompagnement plus ou moins poussé, au numérique pour en favoriser l'apprentissage et en développer les usages liés aux démarches administratives (création d'une adresse e-mail, impression ou scan de pièces nécessaires à la constitution de dossiers administratifs, création des identifiants pour accéder au service public en ligne...) : faire avec l'usager ou faire à sa place si besoin.
- Une aide aux démarches en ligne (navigation sur les sites des services publics, simulation d'allocations, demande de documents en ligne...)
- Des prestations de conseil pour la résolution des cas complexes en s'appuyant sur les correspondants au sein du réseau des partenaires.

Définition des médiateurs numériques

Ceux sont les personnes (professionnels, bénévoles…) qui accompagnent les usagers dans la « Médiation Numérique », qui désigne la mise en capacité de comprendre et de maîtriser les technologies numériques, leurs enjeux et leurs usages, c'est-à-dire développer la culture numérique de tous, pour pouvoir agir dans la société numérique.

Les médiateurs procèdent par un accompagnement qualifié et de proximité des individus et des groupes (habitants, associations, entreprises, élèves, étudiants, parents, professionnels...) dans des situations de formation tout au long de la vie facilitant à la fois l'appropriation des techniques d'usage des outils numériques et la dissémination des connaissances ainsi acquises. Ils sont donc au service, notamment, de l'inclusion numérique et favorise les coopérations utiles aux réalisations et aux innovations en faveur du bien commun.

- Ils sont confrontés à des enjeux de professionnalisation, de structuration et de valorisation de la filière
- A la différence des aidants numériques, leur cœur de métier est dédié à de la formation et de l'accompagnement numériques.

Les 4 postures de l'aidant numérique

- **FAIRE AVEC :**

Accompagner la personne pas à pas dans sa démarche, en favorisant au maximum la pratique autonome

- **FAIRE A LA PLACE :**

Faire la démarche en ligne pour la personne, en essayant de l'impliquer au maximum

Cette solution s'adresse aux personnes les plus exclues du numérique, qui ne veulent ou ne peuvent pas apprendre (situation de handicap, illettrisme...), ou sont face à une situation d'urgence immédiate.

- **DONNER UN COUP DE POUCE :**

Proposer à la personne de réaliser sa démarche en ligne, en restant à sa disposition pour répondre à ses éventuelles questions.

Cette solution s'adresse aux personnes de niveau avancé ou confirmé, qui maîtrisent déjà les compétences numériques les plus indispensables, et qui ont envie de devenir autonomes sur une démarche

- **REDIRIGER VERS UNE STRUCTURE** :

Cette solution s'adresse aux personnes de niveau débutant, intermédiaire ou avancé, qui ont envie d'apprendre et se former.


Quand je fais avec l'usager
LES ETAPES CLES
1. J'entre avec discrétion
2. J'informe sur ma mission en toute transparence
3. Je ne conserve pas d'informations de l'usager
4. Je repars en supprimant toutes les informations personnelles de l'usager


DISCRETION
TRANSPARENCE
PAS DE TRACES DES DONNES
SUPRESSION DES DONNES PERSONNELLES

Q


Quand je fais à la place de l'usager
LES ETAPES CLES
1. J'entre dans la mission en sécurisant mon intervention
2. Je démarre en expliquant ma mission en toute transparence
3. Lorsque je termine, je ne conserve aucune information
4. Je sors de la mission en supprimant
toutes les informations personnelles de l'usager


ACCORD ECRIT
TRANSPARENCE
CONFIDENTIALITE DES DONNEES
IDENTIFIANT ET MOT DE PASSE

Le mandat écrit : faire à la place de

- Dans certaines situations, la personne accompagnée ne peut réaliser ses démarches en ligne, il faudra alors recourir au **mécanisme du mandat** (ex. : personnes en situation de handicap et/ou personnes âgées qui ne sont pas en mesure de se déplacer au sein d'un espace public numérique et personnes qui n'ont pas de qualification numérique, etc.).
- Le mandat est un contrat par lequel une personne donne à une autre, le pouvoir de faire des actes juridiques en son nom et pour son compte. Ce contrat va ainsi permettre de recueillir l'accord de l'usager pour bénéficier de cet accompagnement.
- Le mandat permet à la fois à la personne concernée de contrôler les usages qui sont faits de ses données et à l'organisme de poser clairement le cadre et les règles de l'accompagnement qu'il propose.
- Pour garantir la validité du mandat, vous devez expliquer à l'usager :

- L'objet de votre intervention ;
- La raison pour laquelle ses informations sont collectées ;
- La possibilité pour l'usager de révoquer à tout moment le mandat.

- La CNIL recommande que le mandat soit effectué **par écrit** avant le début de la prestation, afin de faciliter la preuve de l'accord.
- Elle propose à cet égard un modèle de mandat, adaptable selon le niveau d'accompagnement proposé au bénéficiaire, permettant d'encadrer l'utilisation des données de l'usager par le professionnel.
- Ajoutez une phrase qui stipule que les informations fournies par l'usager relèvent de sa responsabilité et que l'organisme ne pourra être tenu responsable d'informations erronées
- Le mandat, **signé par le bénéficiaire (le mandant) et par vous-même (le mandataire)**, précise votre champ d'action et les tâches que vous allez être amené à effectuer à la place et en l'absence de l'usager.
- N'oubliez pas de fournir un exemplaire à l'usager et de conserver un exemplaire dans un endroit sécurisé (tiroir qui ferme à clé ou fichier sécurisé par mot de passe dans votre ordinateur).

LE MANDAT ECRIT PROPOSE PAR LA CNIL

Attention : *ce document est un exemple de mandat permettant exclusivement d'encadrer la collecte et l'utilisation des données personnelles d'un usager, par un intervenant du secteur social, dans le cadre d'un accompagnement au numérique. Il n'a pas vocation à encadrer l'accompagnement de manière générale.*

Je soussigné, M. ou Mme X (ci-après le mandant) autorise M. ou Mme. Y (ci-après le mandataire), professionnel de l'action sociale au sein de (*nom de l'organisme Z*) à réaliser en mon nom, mes démarches sur Internet, conformément aux dispositions des articles 1984 et suivants du Code civil.

1. Missions

Le mandataire s'engage à accomplir, au nom et pour le compte du mandant, les missions suivantes :

(*Il convient de lister de manière exhaustive l'ensemble des démarches qui vont être réalisées par le professionnel.*)

[Par exemple] :

- Création d'une adresse de messagerie ;
- Enregistrement des identifiant et mot de passe de la messagerie ;
- Création d'un compte personnel sur le site de la Caisse nationale d'assurance vieillesse (CNAV) ;
- Enregistrement des identifiant et mot de passe de mon compte personnel CNAV ;
- Réalisation de l'ensemble des démarches en ligne relevant de la CNAV ;
- Suppression ou mise à jour des informations me concernant lorsqu'elles ne sont plus à jour.

2. Enregistrement et utilisation des données à caractère personnel

Le mandataire ne doit collecter et enregistrer que les seules informations strictement nécessaires au regard des démarches susvisées.

Le mandataire ne doit utiliser les informations concernant le mandant que pour les seules démarches susvisées. S'il a besoin de les utiliser pour d'autres démarches, il doit au préalable en informer le mandant et en demander l'autorisation.

Le mandataire s'engage à mettre à jour puis à supprimer l'ensemble des informations relatives au mandant lorsqu'elles ne sont plus nécessaires à la réalisation des démarches lui incombant au titre du mandat.

3. Information et transparence

Le mandataire informe le mandant des droits dont il/elle dispose, prévus par les articles 13 à 22 du Règlement général sur la protection des données (RGPD), et notamment de la possibilité de retirer à tout moment son consentement.

Le mandataire doit s'assurer que l'information a été réalisée de manière concise, transparente, compréhensible et aisément accessible conformément aux dispositions de l'article 12 du RGPD.

Le mandataire doit informer régulièrement le mandant de toutes les actions qu'il effectue à sa place (ex. : mise à jour d'informations, courrier électronique envoyé à la CNAV etc.).

4. Confidentialité

Le mandataire est soumis à une obligation de confidentialité. Il ne doit en aucun cas divulguer les informations du mandant à des tiers lorsque cette divulgation n'est pas nécessaire à l'accomplissement des démarches dont il est responsable (ex. : il ne doit pas communiquer des informations concernant le mandant à son collègue de travail).

Le mandataire enregistre les informations du mandant de manière sécurisée et notamment prend toutes précautions conformes aux usages et à l'état de l'art pour assurer la sécurité physique et logique de ces données.

5. Durée du mandat

Le présent mandat est accepté et consenti pour la durée nécessaire à l'accomplissement des missions du mandataire.

Le mandat prend fin lorsque la réalisation des démarches susvisées a été accomplies, ou à tout moment si le mandant ou le mandataire décide de révoquer le mandat.

6. Responsabilités

Le mandataire est tenu d'accomplir le mandat tant qu'il en demeure chargé, et répond des dommages et intérêts qui pourraient résulter de son inexécution conformément à l'article 1991 du Code civil.

7. Signature des parties

Fait à [*lieu*], le *[…]*

Le mandant

Fait à [*lieu*], le *[…]*

Le mandataire

Le mandat oral : Faire à la place de

A utiliser exceptionnellement, lorsqu'il est impossible pour l'organisme de recueillir le consentement écrit de l'usager en raison notamment de l'extrême urgence de la situation, le mandat pourra être donné oralement (art. 1984 et suivants du Code civil).

Dans ces cas exceptionnels, la CNIL recommande que les garanties suivantes soient prises :

- procéder à un « contrôle d'identité » plus ou moins poussé au regard du risque pour la personne concernée, et des possibilités dont disposent les agents traitant les demandes (ex. : procédure de rappel par l'agent d'accueil pour écarter d'éventuelles « usurpations de numéro », mise en perspective des données déjà fournies par l'usager dans le cadre de son accompagnement social et médico-social avec celles figurant dans la base de données de l'organisme) ;

- tracer en interne par écrit chaque demande de façon nominative et horodatée dans un tableau ;

- adresser le plus rapidement possible une confirmation écrite de la démarche réalisée à la personne concernée rappelant notamment la date de l'appel téléphonique, les actions réalisées, les nom et prénom de l'agent en charge de la requête (mandataire) et les coordonnées de la structure ;

- informer la personne concernée de la possibilité de révoquer à tout moment son mandat.

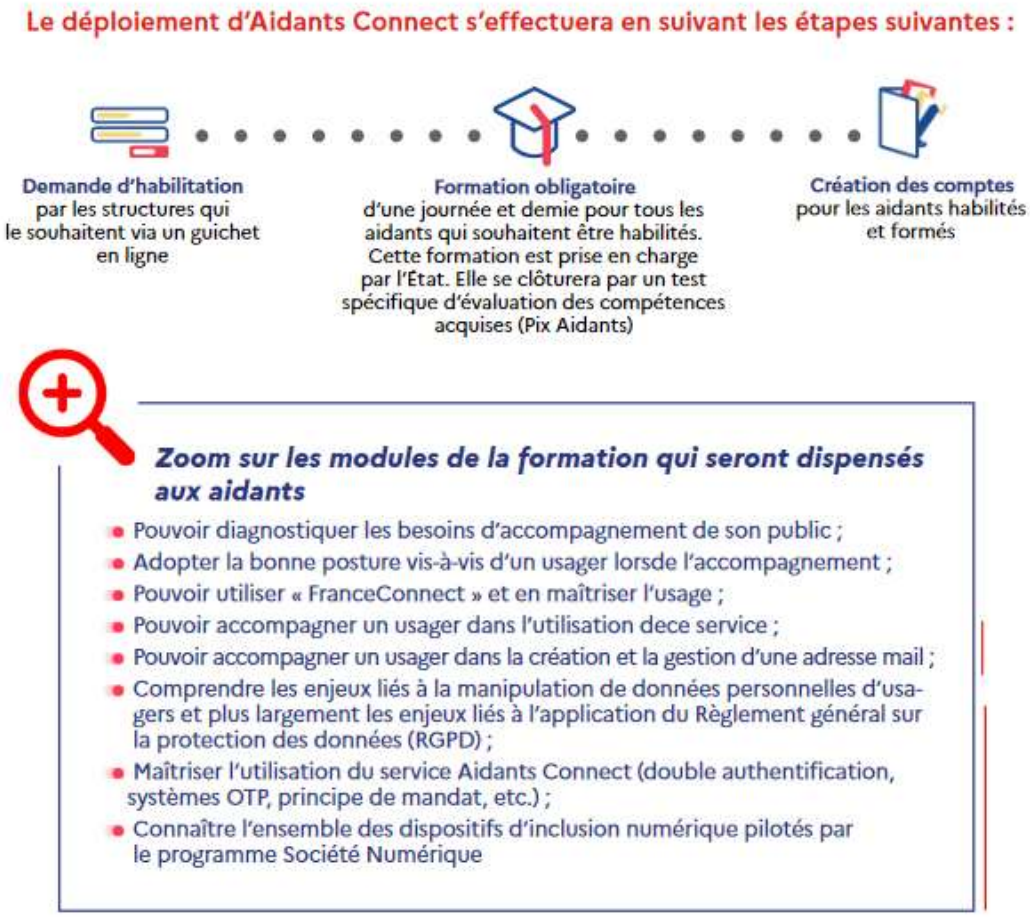
Le mandat AidantsConnect

- À partir du 15 mars 2021, toute structure souhaitant être habilitée peut le faire via le guichet d'habilitation en ligne :

https://aidantsconnect.beta.gouv.fr/habilitation

- Pour les collectivités territoriales qui souhaitent rendre possible l'utilisation d'Aidants Connect sur l'ensemble de leurs services/démarches en ligne, elles peuvent bénéficier d'un soutien financier de l'État de 5000€ pour intégrer un bouton FranceConnect sur leurs sites, ce qui leur permettra automatiquement de bénéficier du service Aidants Connect. Toutes les informations ici :

https://france-relance.transformation.gouv.fr



Identification avec FranceConnect

https://franceconnect.gouv.fr/nos-services

FranceConnect est un dispositif qui permet aux internautes de s'identifier sur plusieurs services en ligne par l'intermédiaire d'un seul compte existant (impots.gouv.fr, ameli.fr ...).

Un coffre-fort numérique pour les partenaires : https://partenaires.franceconnect.gouv.fr/login

Ce téléservice public gratuit permet aussi à l'usager de créer son propre portail de e-services administratifs avec un identifiant personnel unique, de personnaliser ses contenus favoris et, de gérer et utiliser ses données à caractère personnel grâce à **un espace de stockage**

DES BESOINS D'ACCOMPAGNEMENT ET DE FORMATION

Aujourd'hui, 54% des Français adultes ont acquis des compétences numériques seuls

- **41% des personnes ayant de bas revenus n'ont jamais appris à se servir des outils numériques**
- **48% souhaitent être formées.**
- 23% sont favorables à une formation en milieu professionnel.

Ceux qui se présentent comme **les moins habiles pour utiliser un ordinateur sont aussi les plus réfractaires** à un tel apprentissage, ne se disent pas prêts à adopter de nouvelles technologies et nécessiteront donc d'être accompagnés :

- les non diplômés (57%)

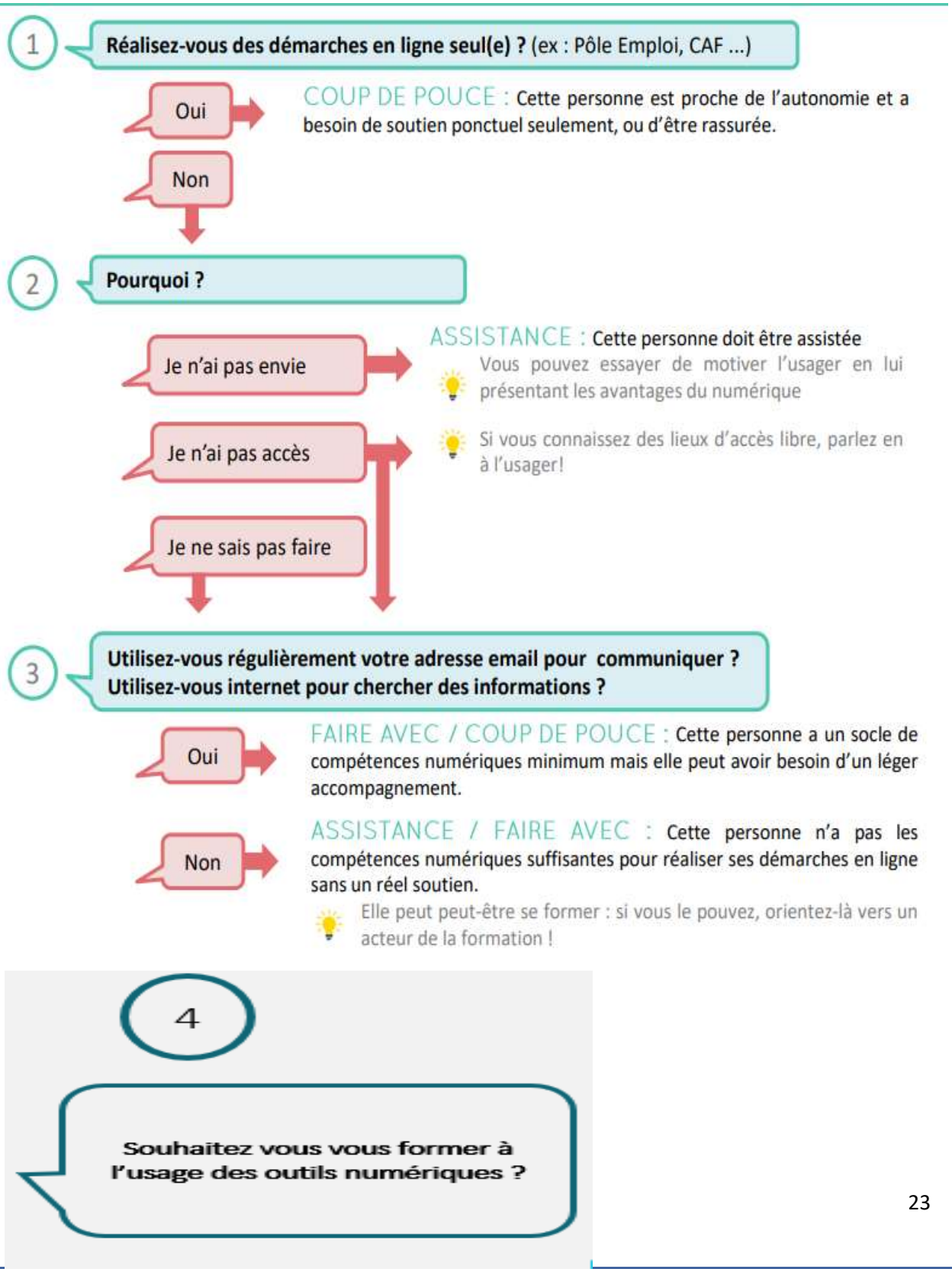
- les plus âgés (59% des 70 ans et plus).

- 33% des Français pensent qu'un accompagnement personnel ou collectif dans un lieu dédié, autre que le lieu de travail, est le plus adapté pour mieux maîtriser le numérique.
- 19% des Français se sentent capables d'effectuer leur première démarche en ligne seulement à condition d'être accompagnés.

Les personnes au foyer ou vivant seules se sentent moins compétentes pour utiliser un ordinateur :

Enfin, 85% des internautes distants s'appuient sur leur entourage lorsqu'ils rencontrent une difficulté.

REALISER UN DIAGNOSTIQUE DES BESOINS NUMERIQUES DE L'USAGER



Les cartographies des partenaires et des lieux ressources

- Les bons clics :
  https://www.lesbonsclics.fr/fr/

- Les assembleurs :
  http://carto.assembleurs.co/

- Carte France services - ANCT (anct-carto.github.io)

Carte France services - ANCT (anct-carto.github.io)

- France services :
  https://anct-carto.github.io/france_services/

France services est un guichet unique qui donne accès dans un seul et même lieu aux principaux organismes de services publics : les Finances publiques, la Caisse d'allocations familiales (CAF), l'Assurance maladie, l'Assurance retraite, le ministère de l'Intérieur, Pôle emploi, la Poste, la Mutualité sociale agricole (MSA) et le ministère de la Justice.

Les outils ressources pour réaliser un diagnostique

https://pix.fr/abc-diag/

https://www.lesbonsclics.fr/fr/

La plateforme officielle des démarches en ligne : service-public.fr
https://www.service-public.fr

https://www.service-public.fr a pour mission d'informer l'usager et de l'orienter vers les services qui lui permettent de connaître ses obligations, d'exercer ses droits et d'accomplir ses démarches administratives. C'est le site officiel de l'administration française, le portail unique de renseignement administratif et d'accès aux services en ligne, réalisé en partenariat avec les administrations nationales et locales.

Un coffre-fort gratuit pour les usagers

Ce téléservice public gratuit permet aussi à l'usager de créer son propre portail de e-services administratifs avec un identifiant personnel unique, de personnaliser ses contenus favoris et, de gérer et utiliser ses données à caractère personnel grâce à **un espace de stockage de 20 Mo permettant de conserver les informations le concernant et les documents et pièces justificatives qui lui sont nécessaires pour l'accomplissement de démarches administratives**.

Sur cet espace personnel gratuit situé sur un serveur appartenant à l'Etat et accessible depuis n'importe quel ordinateur, pourront être stockés documents officiels qui, peu à peu, prennent une forme électronique, par exemple les bulletins de paie, certificat de travail, attestation Assedic, relevé IJSS….

Arrêté du 18 juin 2009 « mon.service-public.fr » et Décret 2009-730 du 18 juin 2009 relatif à l'espace de stockage accessible en ligne.

GESTION DES DONNEES PERSONNELLES

Peut être considéré comme donnée personnelle toute donnée permettant d'identifier une personne. Le champ est donc très large.

Cette identification peut être directe :

- Nom,
- Prénom,

ou indirecte :

- Identifiant de connexion,
- Numéro de client,
- Numéro de téléphone,
- Donnée biométrique (empreintes digitales, adn...),
- Donnée audio, vidéo ou photo,
- Enfin un ensemble d'informations physiques, physiologiques, génétiques, psychiques, relatives à la santé, la situation économique, culturelle ou sociale.

Cette identification se fait soit à partir d'une seule donnée (numéro de client, adn), soit par recoupement de plusieurs données (homme de plus de 50 ans, client de la plateforme X, habitant en région parisienne...). La publicité ciblée se fonde sur cette technique du recoupement pour analyser les informations, identifier des profils, voire déduire et produire de nouvelles informations.

Une donnée personnelle peut être considérée comme privée ou publique en fonction de son statut de base ou du caractère privé ou public qu'on lui donne à titre personnel. Ainsi une appartenance religieuse est considérée comme privée de manière naturelle mais on peut l'exprimer publiquement et ainsi en faire une donnée publique.

On parle de traitement de données quand un certain nombre de données sont collectées et analysées. Cependant, ce traitement doit avoir été porté à la connaissance de l'utilisateur, posséder un objectif clair et ne doit pas sortir du cadre qui lui a été fixé, par exemple ne pas collecter plus de données que nécessaires.

Obligations de l’aidant : Données Personnelles

Ces actions impliquent en fonction des usages de collecter, utiliser, mais ne surtout pas conserver des données personnelles appartenant aux utilisateurs.

Les obligations de l'accompagnant peuvent se résumer en trois points :

- ***Discrétion et confidentialité** : ne pas s'immiscer dans les actions de l'utilisateur, ne pas divulguer les informations qu'il vous fournit (vie personnelle, identifiants de connexion, adresse email...),*
- ***Sensibilisation et information** : informer l'utilisateur du rôle que l'on joue à ses côtés, lui suggérer des bonnes pratiques, logiciels ou services pouvant l'aider dans ses démarches ou étant plus respectueux de sa vie privée, l'informer de ses droits Informatique et Libertés sans entrer dans un jargon complexe,*
- ***Nettoyer :** lorsque l'utilisateur a terminé ses démarches, veiller à ce que ce dernier se soit bien déconnecté de tous les services, à ce qu'aucune trace de ses activités ne persiste (historique, identifiants de connexion, mots de passe...) sur l'ordinateur utilisé si celui-ci est public.*

L'aidant est également tenu d'informer l'utilisateur de l'ensemble des données pouvant être conservées dans un journal concernant des questions de sécurité (logs, heures de connexion, sites consultés...) vis-à-vis des obligations légales.

La collecte des données doit comme pour tout traitement avoir un objectif et respecter le cadre fixé. On ne collecte pas plus de données qu'il n'en faut et ne les conserve que le temps nécessaire.

L'aidant sécurise également en veillant à ce que les logiciels utilisés soient à jour, évitant ainsi les failles de sécurité, et en sensibilisant la personne à l'utilisation de mesures de protection efficaces.

Enfin, l'aidant s'il doit effectuer des démarches à la place de l'utilisateur doit demander explicitement l'accord et le contractualiser via un mandat spécifique, permettant de formaliser ainsi l'accord. On y indique entre autres l'objet de l'intervention et sa raison, la durée de l'intervention, enfin la possibilité pour l'usager de révoquer à tout moment le mandat si cette intervention s'avère récurrente.

COOKIES

Un cookie est un fichier généré par un site web et déposé sur l'ordinateur de l'utilisateur des fins de conservation d'un ensemble d'informations et de paramètres.

À l'origine, les cookies avaient un but strictement positif car facilitant l'usage du site. Ainsi certains moteurs de recherche permettent la conservation des paramètres de confidentialité, évitant ainsi à l'utilisateur de les saisir à chaque usage.

Cependant leur usage a été peu à peu dévoyé. De nombreux sites utilisent des cookies tout à fait bénins et légitimes mais d'autres ont été créés à des fins publicitaires, les cookies stockant alors des informations non nécessaires à la navigation, voire les partageant avec d'autres sites.

C'est pourquoi il est recommandé de ne conserver que les cookies véritablement utiles, de refuser tout cookie n'ayant aucun rapport avec la navigation, enfin de les effacer après chaque session sur un ordinateur public ou même sur son ordinateur personnel.

Des sites comme YouTube par exemple profilent l'utilisateur même non connecté au fil de ses choix à l'aide de cookies. Si le cookie est effacé, les données disparaissent et l'utilisateur est perçu lors de sa nouvelle connexion au site comme un utilisateur neuf.

RGPD

Le RGPD (Règlement Général sur la Protection des Données) est une directive européenne encadrant la collecte et le traitement des données en Europe, notamment via le biais des cookies. Il vise à mieux protéger les données personnelles et la vie privée des personnes.

Le RGPD oblige les sites à obtenir le consentement des visiteurs pour la collecte des données, ce qui n'était pas le cas auparavant, laissant la porte ouverte à tous les abus. Le citoyen peut ainsi reprendre le contrôle sur ses données. Il s'étend également à toutes les données personnelles récoltées en ligne ou par d'autres moyens pour toute organisation publique ou privée agissant sur le territoire européen ou à destination des résidents européens.

Le RGPD peut être considéré par le grand public plus comme une nuisance que comme un bienfait. En effet, les fenêtres pop-up surgissant et masquant le contenu du site avant l'accès pour obtenir le consentement des utilisateurs à l'utilisation des cookies ou leur rejet peut sembler fastidieux et gêne grandement la navigation, qui plus est lors de la consultation de sites sur tablettes ou smartphones. Il peut être tentant d'installer une extension gérant automatiquement ces questions sur le navigateur mais cela peut être extrêmement dangereux car cela implique d'effectuer un choix générique pour l'ensemble des utilisateurs du poste, ne respectant donc pas ainsi leurs possibles choix et forçant ces derniers à partager des données personnelles si les cookies sont acceptés de manière automatique.

.

BONNES PRATIQUES DE NAVIGATION

Naviguer / utiliser Sur un ordinateur public

Il est important d'être vigilant sur un ordinateur public du fait de son caractère partagé et donc la possibilité pour d'autres utilisateurs d'avoir accès aux informations personnelles d'autres usagers par manque de prudence. Cela implique les ordinateurs des cyber centres / cyberbases mais aussi les bornes utilisées dans les centres sociaux et services publics par exemple pour l'accès aux démarches administratives en ligne.

Ces conseils constituent donc les bases les plus importantes :

- Utiliser la navigation privée : ce mode permet de ne pas conserver l'historique de la navigation, ainsi que les données saisies.
- Ne pas utiliser la fonction "enregistrer les mots de passe" du navigateur, celle-ci donnant alors accès aux données personnelles d'un utilisateur à l'ensemble des utilisateurs de l'ordinateur.
- Vérifier que l'on s'est bien déconnecté proprement de l'ensemble des services utilisés ; fermer une fenêtre ou le navigateur ne suffit pas à se déconnecter. La connexion peut en effet rester effective encore un certain temps (variable en fonction des sites), pendant lequel il est toujours possible de prendre la main sur le service et donc d'usurper l'identité de l'utilisateur.
- Ne pas stocker de fichiers personnels sur l'ordinateur utilisée ; on préférera l'usage d'une clé USB ou d'un disque dur externe.

Sur tout ordinateur (dont ordinateur personnel)

- Vérifier que les sites que l'on consulte sont sécurisés (https) avec la présence du cadenas à côté de l'adresse

- Prendre connaissance des règles de confidentialité des sites utilisés pour vérifier s'ils sont bien conformes à mes souhaits en matière de protection des données personnelles
- Avoir toujours conscience que peu d'espaces sont réellement privés sur Internet : je ne publie donc pas d'éléments trop personnels
- Ne pas ouvrir les pièces jointes provenant d'inconnus pour les emails
- Ne jamais communiquer les mots de passe et identifiants
- Activer la double authentification pour les comptes les plus importants (emails par exemple)

Attention avec la double authentification : il faut qu'elle soit bien comprise par l'usager car le fait de devoir recevoir un code sur son portable par exemple peut être vu comme une complication. Par ailleurs, il faut chercher la solution la plus simple mais la plus sécurisée possible en fonction de l'usager, par exemple éviter une double authentification nécessitant un téléphone portable si l'usager n'en a pas ou au contraire change régulièrement.

Approches

Approche zéro trust

L'approche zéro trust est une méthodologie quelque peu paranoïaque mais efficace. On peut la moduler à différents degrés sans pour autant nuire à son efficacité.

Il s'agit tout simplement de n'avoir confiance en rien et d'utiliser des biais permettant de vérifier les informations données.

Par exemple, un logiciel que j'utilise au quotidien me signale dans une fenêtre pop-up sur mon ordinateur que j'ai droit à une offre d'abonnement et qu'il me suffit de cliquer sur le lien qui apparait dans la fenêtre pour accéder à la page de paiement. Il pourrait s'agir d'une tentative de phishing (hameçonnage) si mon ordinateur a été piraté. Pour vérifier cela, je me connecte au site du logiciel via mon compte : l'offre est bien présente et il ne s'agit donc pas d'une tentative de phishing. Je peux donc procéder au paiement en toute confiance.

Dans le même état d'esprit, on privilégiera des logiciels open source, c'est-à-dire dont le code est accessible et peut être examiné par la communauté. Ces logiciels doivent toujours être téléchargés à partir des sites des créateurs / créatrices (plutôt que des sites comme Clubic), donnant ainsi accès à la dernière version etcertifiant que le code source n'a pas été trafiqué.

Approche zéro empathie

Au-delà de l'approche zéro trust, on parle aussi parfois d'approche "empathie zéro". L'utilisation du web implique de savoir garder la tête froide. La plupart des arnaques se fondent en effet sur la peur, l'émotion ou la colère qui diminue la réflexion de l'utilisateur et pousse à des réactions impulsives. On aime réagir, venir en aide, profiter des bonnes affaires tout comme on a peur d'être éjecté d'un service ou de perdre un privilège pour non-paiement. Les attaquants visent en premier lieu les personnes peu à l'aise avec le numérique qui auront plus facilement tendance à croire les fausses informations qui lui seront envoyés. Garder la tête froide permet d'éviter de tomber dans ces pièges en privilégiant la réflexion à l'émotion.

Ainsi une récolte de fonds sur un réseau social pour un enfant malade peut certes être réelle mais aussi cacher une arnaque. Si l'on se précipite en suivant uniquement nos bons sentiments, il est possible de prendre des risques

Approche complexité

Plus les mesures de protection sont fortes, plus elles nécessitent de compétences pour être brisées. C'est pourquoi plus on ajoute de couches de protection, moins on a de chances d'être piraté. Imaginons une maison comportant une seule clé. Celle-ci donne alors accès à l'ensemble des pièces et notamment au coffre-fort. La protection est faible. Si chaque pièce en revanche possède une porte fermée par une clé différente, que le coffre ferme avec deux clés et une combinaison à quatre chiffres, qu'enfin la maison est dotée d'une alarme, la protection est alors très forte et va rebuter tous ceux qui ne possèdent pas les compétences techniques et le temps nécessaire pour briser les différentes protections.

Encore faut-il que cela en vaille la peine. Si le coffre contient un collier valant plusieurs dizaines de millions d'euros, on trouvera des candidats. S'il ne contient que quelques centaines d'euros, personne ne tentera de briser les protections.

Dans le domaine numérique, la situation est similaire. Il est important de multiplier les protections sans tomber dans la paranoïa. À moins de posséder plusieurs millions d'euros sur un compte, il est fort peu probable qu'un pirate s'attaque à un individu en particulier. C'est pourquoi la plupart des attaques se font de manière anonyme au filet comme à la pèche plutôt qu'à la ligne en visant une personne en particulier.

Mots de passe

On évite d'utiliser un compte Google ou Facebook pour se connecter à divers sites. En effet, si ce compte est compromis, il donne accès à des tas d'autres services facilitant ainsi l'usurpation d'identité.

De même réutiliser un même mot de passe sur plusieurs comptes est à proscrire car, si un service est compromis et le mot de passe deviné, de nombreux autres services seront compromis. C'est un peu comme si vous utilisez la même clé pour votre maison, votre voiture, un coffre, une pièce sécurisée.

Attaques

Les attaques pour deviner les mots de passe se font de diverses manières :

- De manière ciblée, en se basant sur des données personnelles, par exemple votre date de naissance, le prénom de vos enfants, le nom de votre chien, votre passion, le lieu de vos vacances,
- De manière non ciblée, sur la base de dictionnaires de mots de passe courants,
- Par attaque dite de "force brute", en testant toutes les combinaisons possibles ; dans le cas d'un code de carte bleue à 4 chiffres, l'attaquant va tester toutes les combinaisons de "0000" à "9999" soit 10000 possibilités.

La plupart des attaques sont non ciblées car cibler une victime nécessite beaucoup de temps et ne se fait que si le jeu en vaut la chandelle (attaque ciblée d'une personne en vue de pénétrer un réseau plus large d'un établissement pouvant par exemple faire l'objet d'un rançon à la suite du cryptage générale des fichiers).

Les attaques de "force brute" sont inefficaces face à des mots de passe forts. Plus le mot de passe est complexe, plus l'attaque sera longue. Elles peuvent prendre des heures, des semaines voire des années en fonction du mot de passe et du matériel alloué à l'attaque.

Créer un mot de passe fort

Mieux vaut opter pour un mot de passe long et fort. On recommande souvent de prendre une suite de caractères aléatoires, par exemple pour un mot de passe de 16 caractères : #h4F56lkqgs@489% ; efficace mais difficile à retenir. Pour cela, on peut utiliser une gestionnaire de mots de passe mais aussi une autre méthode, celle de la "phrase pass". Il s'agit d'utiliser une phrase facile à retenir plutôt qu'une suite de caractères aléatoires. Pour la rendre plus complexe, on lui apporte des modifications. Ainsi par exemple :

Pierre qui roule n'amasse pas mousse.

Devient :

P13rr3Qu1RoulenAm@sseP@sMou55e

En respectant les règles suivantes :

- La première lettre de chaque mot est en majuscule.
- Les "i" sont transformés en "1".
- Les "e" du premier mot sont transformés en "3".
- Les "a" minuscules sont transformés en "@".
- Enfin, les "s" du dernier mot sont transformés en "5".

Cette méthode qui peut paraître complexe au premier abord est avec un peu d'habitude en fait beaucoup plus facile à retenir qu'une suite de caractères aléatoires.

Une autre méthode est utilisée pour les courts codes ne comportant que des chiffres. Beaucoup de personnes ne se souviennent ainsi pas de leur code de carte bleue et ont tendance à le noter imprudemment sur un papier dans leur portefeuille, voire sur une étiquette collée sur la carte, ce qui peut s'avérer très dangereux. Plutôt que leur code, on peut noter un nombre qui les aider à se souvenir de ce dernier.

Imaginons un code de carte bleue étant 4287. Si la date de naissance du propriétaire de la carte est le 5 mars, soit 0503, nous pouvons soustraire ou ajouter ce chiffre au code et inscrire ainsi les nombres 3784 ou 4790. Il suffit alors de faire l'opération inverse pour retrouver le bon code.

Gérer les mots de passe

La multiplication des services en ligne et donc des mots de passe pose de nombreux problèmes car il devient difficile de les retenir tous. L'utilisateur est tenté de reprendre le même mot de passe, ce qui pose alors un problème de sécurité.

L'utilisateur peut enregistrer les mots de passe sur son ordinateur lorsque le navigateur le propose mais l'ordinateur devient alors vulnérable si une personne mal intentionnée obtient un accès physique à la machine.

On peut utiliser un gestionnaire de mots de passe, une sorte de coffre-fort sous forme logicielle permettant de conserver (voire de générer) l'ensemble des mots de passe de l'utilisateur.

Ceux-ci sont inscrits dans un fichier crypté accessible à l'aide d'un mot de passe global. Ce type de logiciel est assez simple d'utilisation avec un peu d'habitude.

L'un des meilleurs gestionnaires de mots de passe : reste KeePass (disponible sur la quasi-totalité des plateformes, Android inclus). Il permet le cryptage et la conservation des mots de passe, ainsi que leur génération, voire une aide à la connexion des services.

Site web : https://keepass.info/download.html

Certains navigateurs proposent des trousseaux de connexion permettant de stocker de manière sécurisée les mots de passe. Ce n'est cependant pas une solution que nous recommandons, le partage entre plusieurs dispositifs (ordinateur, smartphone, tablette...) pouvant constituer une faille de sécurité.

L'outil de la CNIL pour générer un mot de passe sécurisé :

https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

Paiements en ligne

Les paiements en ligne doivent toujours être faits dans un espace sécurisé (https) car ils constituent un risque important de la vie numérique. Par ailleurs, ils doivent s'effectuer sur des sites de confiance (enseignes reconnues) et non sur des sites à risque. Il ne faut pas hésiter à rechercher des avis de consommateurs avant d'effectuer des achats sur une plateforme. Certes, il peut y avoir de faux avis dans le sens positif comme négatif mais la tendance générale donne le ton.

On privilégie de même la double authentification quand les sites de vente le permettent, de même que les sites offrant une sécurisation du paiement par l'envoi par exemple d'un code par SMS pour vérifier l'identité de la personne effectuant l'achat.

Cependant, cette dernière méthode est peu à peu délaissée au profit de l'utilisation obligatoire de l'application bancaire sur smartphone. Cela peut poser un problème pour les personnes ne possédant pas de smartphone ou ne souhaitant pas installer cette application. Pour ces derniers, comme pour ceux ne souhaitant pas utiliser leur carte bleue peuvent créer un compte sur PayPal mais cela complique les opérations. À réserver aux plus avertis.

RESSOURCES NUMERIQUES

Navigateurs

De préférence, un navigateur libre et gratuit comme Firefox, Brave ou Chromium. Le caractère libre permet l'accès au code-source par la communauté et donc à l'entière connaissance du fonctionnement du logiciel. Il n'existe pas de zones d'ombres et donc d'inquiétudes possibles quant à la sécurité des données sur le plan logiciel.

- *Firefox : https://www.mozilla.org/fr/firefox/*
- *Chromium : https://www.chromium.org/*
- *Brave : https://brave.com/fr/*

Firefox et Brave sont également disponible sur smartphone et tablette.

Par ailleurs, Firefox intègre des outils de détection des sites frauduleux, prévenant l'internaute avant l'accès à un site de sa dangerosité et des risques qu'il encourt.

Extensions

Les extensions permettent d'étendre la sécurité des navigateurs en leur offrant de nouvelles fonctions. Les extensions ci-dessous sont accessibles avec Firefox mais aussi pour certaines avec Chrome.

Dans Firefox, elles sont accessibles via le menu "Outils" puis "Extensions et thèmes".

Attention ! Si ces extensions permettent de protéger au maximum la vie privée des utilisateurs, elles peuvent aussi parfois bloquer par inadvertance des fonctions essentielles de certains sites et les rendre difficilement utilisable. Ainsi, par exemple, l'utilisation de Privacy Badger et uBlock Origin ne permettait pas d'accéder au descriptif complet des itinéraires sur le site d'Ilévia, gestionnaire des transports en commun sur la métropole de Lille. Il est conseillé alors de les désactiver uniquement pour ces derniers sous forme de "liste blanche". Privacy Badger ou uBlock Origin par exemple acceptent dans leurs paramètres une liste de sites fiables.

HTTPS Everywhere (HTTPS partout)

Le protocole HTTPS permet de chiffrer les données entrantes et sortant d'un site web. Il est intégré par défaut à de nombreux sites, l'utilisateur n'ayant rien à faire de spécial pour l'utiliser. Il garantit la confidentialité des échanges de données entre le serveur (site web) et le client (utilisateur).

L'extension HTTPS Everywhere permet de sélectionner automatiquement le protocole HTTPS d'un site si celui-ci est disponible mais pas actif par défaut.

Facebook Container

Facebook a la fâcheuse manie "d'écouter" ce qui se passe sur les autres sites web que vous consultez tout en étant connecté à ses services. L'extension Facebook Container permet de l'isoler dans un conteneur distinct, une sorte de prison numérique qui ne lui permet pas

d'avoir accès aux informations que vous partagez ou consultez sur d'autres sites, ni d'examiner les cookies utilisés par les autres sites.

Location Guard

La géolocalisation de l'utilisateur, sa position géographique, constitue une donnée intéressante pour le monde économique. Elle peut être obtenue de diverses manières (adresse IP, données WIFI...) et souvent d'une grande précision mais relève de la vie privée. Il est possible de refuser la collecte de cette donnée mais son efficacité est laissée au bon-vouloir des entre

Location Guard ajoute du "bruit", des éléments aléatoires dans les informations fournies rendant ainsi plus difficile la géolocalisation précise de l'utilisateur. L'aire où se trouve l'utilisateur est ainsi étendue, beaucoup plus floue, plutôt qu'un point précis.

Privacy Badger

Privacy Badger est un bloqueur automatique de traqueurs. Il les repère sur les sites visités par leur comportement et les ajoute à sa liste de blocage. Il évite ainsi à l'utilisateur d'être pisté de site en site. La plupart de ces traqueurs espionnent le comportement de l'utilisateur et sont à but publicitaire, permettant ainsi de délivrer une publicité ciblée sur les différents réseaux utilisés par l'internaute.

Privacy Badger envoie par défaut aux sites visités un signal indiquant qu'il est interdit de vous traquer. Cependant, ce signal international n'a pas d'obligation légale. Si votre choix n'est pas respecté, Privacy Badger bloque les traqueurs encore en service.

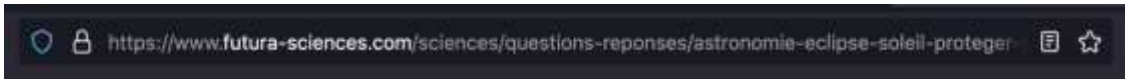
UBlock Origin

UBlock Origin est une extension complémentaire à Privacy Badger, bloquant les publicités et les pisteurs. Contrairement à Privacy Badger, son filtrage se base sur des listes (traqueurs publicitaires, sites reconnus comme étant fournisseurs de spam...). UBlock Origin peut être activée ou désactivée en fonction des sites en cours de consultation, permettant ainsi de créer une sorte de liste blanche.

En bloquant les publicités, uBlock Origin permet de gagner en rapidité et en clarté sur les sites, facilitant ainsi leur consultation par l'utilisateur.

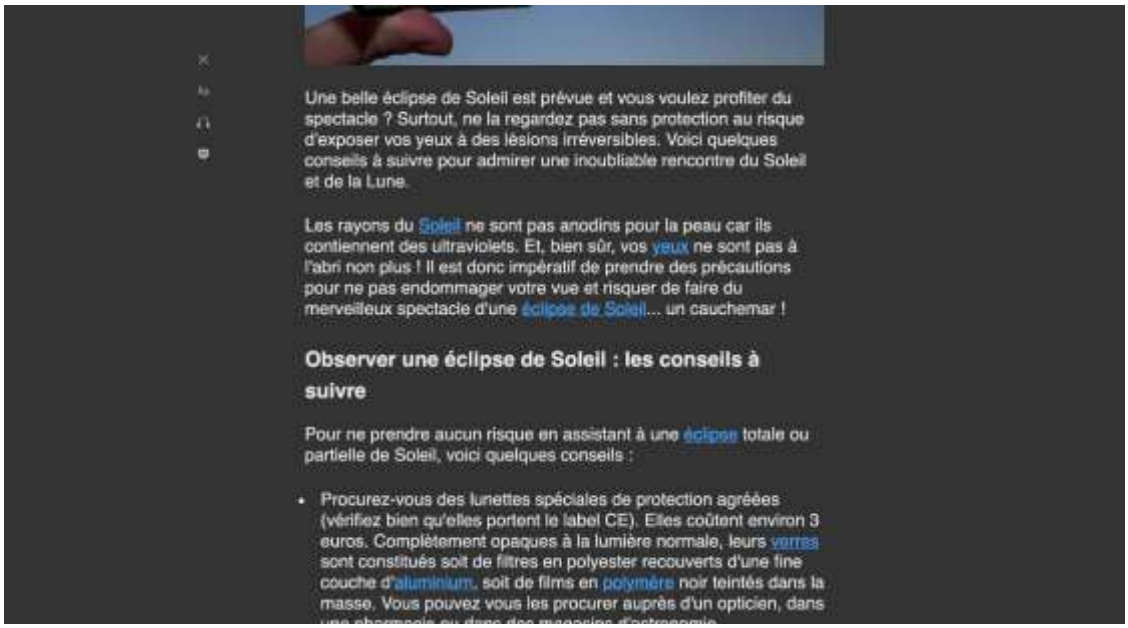
Mode lecture

Ceci n'est pas une extension mais une fonction du navigateur Firefox pouvant faciliter la lecture des sites. À côté de la barre d'adresse, une icône en forme de page permet d'y accéder et de transformer la page web.



La page débarrassée de tout ce qui ne concerne pas le texte devient plus accessible et des boutons sur le côté permettent de modifier la couleur de fond, la taille de la police, voire d'utiliser un lecteur audio d'écran.

En sus des extensions comme uBlock Origin qui supprime la publicité, cela permet de clarifier la présentation et la lecture de nombreuses pages.



Moteurs de recherche

Les moteurs de recherche ci-dessous préservent la vie privée de leurs utilisateurs en ne collectant pas de données et donc ne permettent pas la création peu à peu d'un profil ""utilisateur".

Attention ! Si la majorité du public est de plus en plus sensible à la question des données personnelles et aux risques que cela engendre, beaucoup d'utilisateurs prennent encore les moteurs de recherche comme des carnets d'adresse et ne comprennent pas leur caractère mouvant. Cela leur pose ainsi un problème lorsqu'ils constatent des résultats différents pour la même requête entre leur ordinateur (où peu à peu un profil s'est mis en place) et un ordinateur public (où aucun profil n'a pu être généré). Il est bon de les initier à l'utilisation de marque-pages pour conserver les adresses les plus utilisées.

L'ensemble des moteurs de recherche ci-dessous peuvent être installés par défaut dans Firefox (ainsi que les navigateurs courants).

Duck Duck Go

Duck Duck Go est un moteur de recherche dont le modèle économique repose sur l'affichage de publicités et la recommandation. A contrario de Google, il ne collecte aucune donnée personnelle, ne permettant pas ainsi la création progressive d'une publicité ciblée. Duck Duck Go a connu un essor important depuis les révélations d'Edward Snowden en 2013.

L'entreprise par ailleurs consacre une parte de ses revenus au financement de projets open source.

Site web : https://duckduckgo.com/

Startpage

Startpage est un métamoteur de recherche, c'est-à-dire qu'il constitue une passerelle vers plusieurs moteurs de recherche différents (AOL, AlltheWeb, Altavista, Ask/Teoma, Bing,

EntireWeb, Gigablast, Google, Open Directory, Wikipédia) dont il collecte les réponses et les synthétise.

Startpage est un des moteurs les plus privés au monde, ne recueillant aucune donnée personnelle, pas même l'adresse IP. Il permet un haut niveau de personnalisation au travers de ses paramètres. Ceux-ci peuvent être sauvegardés dans un cookie ou intégrés dans une adresse web (URL), évitant ainsi la conservation de données sur l'ordinateur.

Site web : https://www.startpage.com/

Qwant

Seul français de la liste, Qwant existe depuis 2013 fonctionne comme Duck Duck Go sur l'affichage publicitaire et la recommandation mais ne recueille aucune donnée personnelle, ce qui permet un affichage neutre. Qwant fait partie de la liste des logiciels libres préconisés par l'État français. Cependant, le moteur de recherche n'est pas entièrement open source.

Qwant possède une version junior largement utilisée dans les collèges et plus généralement par l'Éducation Nationale.

Site web : https://www.qwant.com/

Partage de fichiers

Utiles lorsque l'on veut partager de gros fichiers impossibles à mettre en pièces jointes d'un mail, la page FramaDrop (https://alt.framasoft.org/fr/framadrop)propose une liste de services ci-dessous ne traquant pas les utilisateurs au contraire de services comme WeTransfer.

Outils de cryptographie

Les outils de cryptographie ne sont utiles que si l'on veut crypter / chiffrer des données et fichiers sensibles. Pour les mots de passe, il vaut mieux passer par un gestionnaire de mots de passe comme indiqué plus haut.

À ce titre, le logiciel open source VeraCrypt (https://veracrypt.fr/en/Home.html) constitue la référence.

De manière plus simple, la plupart des banques proposent actuellement des services de coffre-forts numériques en ligne, permettant de sauvegarder et protéger les fichiers importants (papiers, certificats...).

TYPES D'ARNAQUES

Dark patterns

Les "dark patterns" sont des méthodes utilisées pour tromper et obliger l'utilisateur à consentir à certains choix, accepter des offres ou lui compliquer la tâche lorsqu'il. Elle souhaite par exemple résilier un service. Ces méthodes s'appuient le plus souvent sur le design de la page ou sur l'obfuscation (complication des termes) pour perdre l'utilisateur et le pousser vers le chemin désiré.

Exemple avec les cookies et capture d'écran de Météo France.

Cet exemple reste peu risqué mais nombre de contrats abusifs utilisent le principe des "dark patterns" souvent en précochant des cases sur des formulaires pour que le client s'abonne ou choisissent des options non désirées (renouvellement régulier du paiement d'un abonnement à un service par exemple).

Que faire ? Deux principes essentiels :

- Prendre son temps. Les dark patterns exploitent notre propension à cliquer rapidement après avoir lu le texte rapidement en diagonale, ainsi que nos habitudes de clic. Par exemple, si le bouton d'annulation d'un service particulier est situé en haut à droite et le bouton d'acceptation en bas à droite, subitement leurs positions seront inversées, l'utilisateur cliquant alors sur "accepter" alors qu'il comptait cliquer sur "annuler".
- Bien vérifier les différentes cases précochées d'un formulaire.

Spam / Scam

Le spam ou courrier / publicité non désirée est plus considéré comme un envahissement qu'une attaque contre l'utilisateur. Cependant, de nombreux emails de spam sont des scams, c'est-à-dire des emails frauduleux renvoyant vers une arnaque. Alors que le spam tente le plus souvent de vendre des produits miracles, le scam est une véritable escroquerie : invitation à rejoindre de pseudo-sites de rencontres, offre alléchante (par exemple réduction importante sur des produits de luxe), gain inespéré à une loterie (sachant que l'utilisateur n'y a bien évidemment pas joué...), offre de partenariat sur des investissements soi-disants sans risques et aux gains faciles, donsou héritages soudains.

Quelques exemples de spams / scams classiques :

- Une offre hyper avantageuse sur une marque connue,
- Une publicité pour un produit amaigrissant particulièrement efficace,
- Une invitation à rejoindre quelqu'un sur un site de rencontres,
- Un gain inespéré à un concours ou une loterie,
- Une demande d'aide pour recouvrer une somme importante pour laquelle il suffit de payer les frais administratifs (arnaque dite du prince nigérian),
- Une tentative d'extorsion de fonds en prétendant que votre correspondant possède des photos ou vidéos indiscrètes...

Que faire ?

Mettre l'email à la corbeille directement est la seule solution viable. Il ne faut surtout pas tenter de se désabonner car cela valide l'existence de l'adresse mail. L'envoi de spam est en effet effectué le plus souvent par millions à l'aveuglette. Y répondre consiste à "s'abonner" à la réception d'autres spams, voire à ce que l'adresse email soit enregistrée en vue d'autres arnaques ultérieures. L'envoi de plusieurs millions d'emails frauduleux ne coûte que quelques centaines d'euros sur le marché noir. Les bénéfices peuvent donc être très importants malgré un faible nombre de personnes tombées dans le panneau.

Si le service fournissant l'adresse mail (Gmail, La Poste, Outlook...) le permet, il faut signaler le mail comme étant du spam (disponible dans les choix de gestion de l'email), afin de permettre au système de le repérer plus facilement par la suite et de le supprimer automatiquement. De nombreux services font en effet un tri préalable et envoie automatiquement dans la catégorie "spams" les emails repérés comme tels.

Phishing (hameçonnage)

On résume souvent le phishing en une petite histoire.

Une petite épicerie se trouve seule au milieu d'une grande rue. Les maisons à sa gauche et à sa droite sont rasées pour laisser la place à deux grands supermarchés qui risquent de lui prendre toute sa clientèle. Nullement effrayé l'épicier, coincé entre ces deux géants, décroche son enseigne et y installe une nouvelle où y est simplement inscrit "Entrée principale".

Le phishing est donc une arnaque visant à l'usurpation d'identité. Le phishing peut être considéré comme un sous-groupe du spam / scam, en fait une attaque plus ciblée, mieux préparée mais heureusement pas exempte d'erreurs. Le phishing joue souvent sur l'émotion et / ou la peur pour pousser la victime à ne pas réfléchir : facture impayée et menace de résiliation d'un service, annonce d'un remboursement important vis-à-vis des impôts, annonce d'un colis non livré à cause de renseignements erronés...

Que faire ?

- Faire preuve de réalisme et de logique en se demandant si la situation présentée correspond bien à la nôtre (colis non livré alors que l'on n'attend pas de colis par exemple).
- Ne pas cliquer trop vite : une bonne nouvelle (remboursement, cadeau...) n'est peut-être qu'une arnaque.
- Être attentif aux fautes d'orthographe et erreurs contenues dans les emails (mauvaise traduction, mise en forme erratique...).
- Examiner les noms de domaine, par exemple : "https://impotss.gouv.fr" est différent de "https://www.impots.gouv.fr/" ; le "s" n'est pas forcément visible si l'on n'est pas attentif.
- Examiner l'adresse de l'expéditeur : "service-impots-nepasrepondre@sushy.com" fait moins sérieux et crédible que "service-impots@gouv.fr".
- Être attentif à tout ce qui sort de l'ordinaire, par exemple votre beau-frère qui vous envoie un message avec un simple lien vidéo alors qu'il n'envoie quasiment jamais de message, tout au moins jamais aussi laconique, ou bien un appel à l'aide reçu par mail d'une personne que vous connaissez à peine, pourtant écrit sur un ton familier comme si vous étiez amis depuis l'enfance.

Faux profils

Ils sont légion sur le web et se mettent en quatre pour faire croire à leur réalité. La plupart des faux profils sont assez peu travaillés et visent à une arnaque rapide : amadouer, émouvoir leur interlocuteur / interlocutrice et lui soutirer au mieux de l'argent, sinon usurper son compte sur un réseau social pour ensuite s'en servir pour d'autres arnaques.

Il faut savoir que la grosse majorité des faux profils sont créés de manière rapide et peu efficace. On est loin de ce que présentent les films et séries qui lorgnent du côté de l'espionnage. C'est pourquoi usurper un compte déjà existant est particulièrement intéressant car basé sur une personne réelle.

Les faux profils se repèrent cependant à quelques indices basiques.

S'ils ne se basent pas sur un compte usurpé, ils sont ce que l'on appelle des nouveau-nés, c'est-à-dire peu ou pas d'amis qui n'ont pour la plupart aucun contact entre eux, très peu de photographies, tout autant de contenu le plus souvent de faible valeur, soit des informations basiques repompées d'autres sites, des images et animations humoristiques, des messages peu intelligibles.

Ces faux profils sont peu animés et le contenu varie donc très peu. Il faut savoir qu'un seul pirate peut en gérer une cinquantaine en même temps et qu'ils sont parfois partagées entre plusieurs "gestionnaires". Difficile donc de créer une vie sociale intéressante et cohérente.

Les photographies sont usurpées et issues soit de banques d'images, soit de profils volés sur les réseaux sociaux. On peut s'en convaincre en sauvegardant leur photo de profil et en cherchant via un moteur de recherche d'images :

- Google Images : https://images.google.com/
- Mais surtout TinEye (https://tineye.com/) qui permet de rechercher l'image dans de nombreuses banques et sites, voire d'en retracer l'historique.

Une recherche sur TinEye a ainsi permis de montrer qu'une image utilisée par un faux profil était recensée sur plus d'une dizaine de sites de rencontres, à l'insu de sa propriétaire, une scientifique russe, dont les photos avaient été volées sur Linkedin.

Les faux profils convient systématiquement leur interlocuteur / interlocutrice à les rejoindre sur une autre plateforme pour discuter. L'objectif est simple : migrer vers une plateforme (hangout, whatsapp, mail...) où leur activité pourra être plus difficilement détectée.

Que faire ?

- Garder la tête froide et ne pas se leurrer sur les intentions de la "personne" rencontrée : celle-ci n'est pas ce qu'elle prétend être.
- Vérifier si besoin la photographie utilisée à l'aide d'un moteur de recherche d'images
- Supprimer purement et simplement la demande d'ami ou de contact