

Maîtriser son identité numérique

1. Définition de l'identité numérique
2. Je choisis ma photo et mon pseudo
3. Gérer son profil
4. Les traces que je laisse avec mon ordinateur
5. Les mots de passe

Définition : 10 mn
Photo et pseudo : 10 mn
Profil : 10 mn
Les traces : 15 mn
Mots de passe : 10 mn

Total : 55 mn

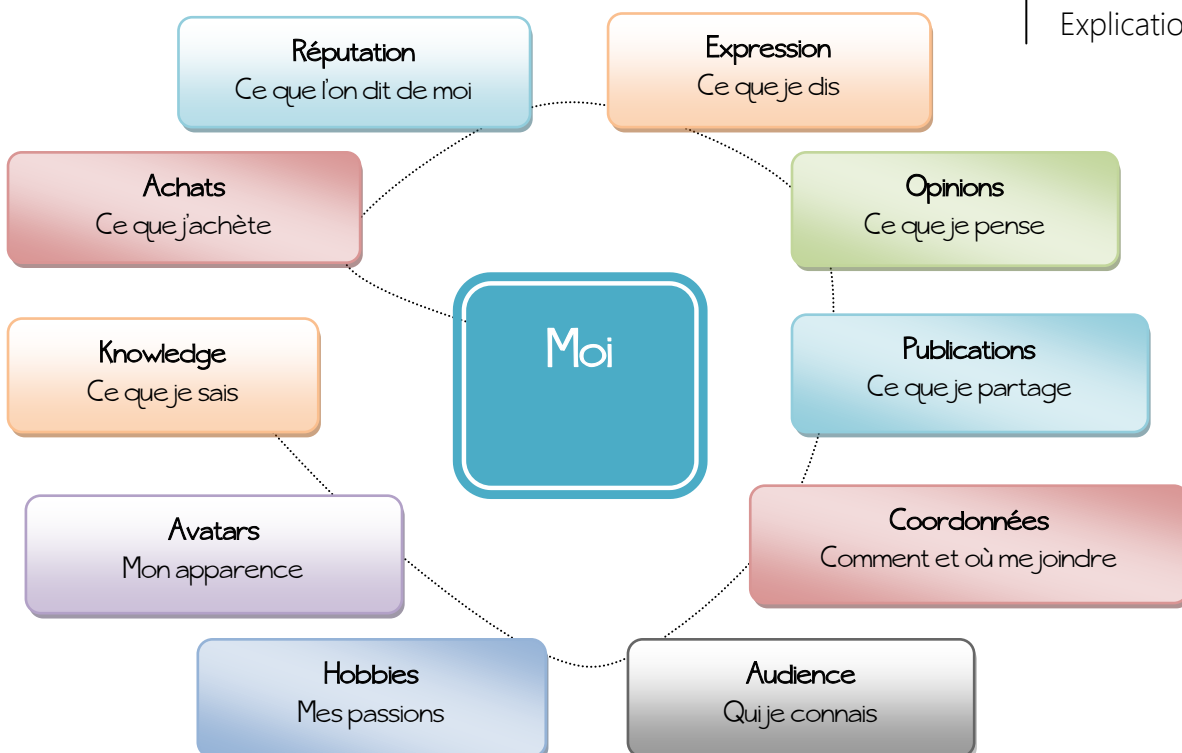
Objectifs :

L'objectif principal est de faire réfléchir les élèves à leur identité numérique, à leur e-réputation et aux traces qu'ils laissent sur la toile. Le propos n'est pas de dire que tout est un danger, mais de les accompagner dans leur réflexion sur ce qu'ils souhaitent pour eux et comment y parvenir.

1. Définition de l'identité numérique

Animation :

Explication du Schéma



L'Agence Départementale du Numérique est financée par le Conseil général des Pyrénées-Atlantiques

2. Je choisis ma photo et mon pseudo

- Ne jamais mettre d'info personnelle d'ordre privé comme votre nom complet, votre numéro de téléphone, votre adresse ou autre numéro de portable dans votre pseudo... sinon vous ne serez plus anonyme.
- Un ou plusieurs pseudos? Il peut être intéressant de prendre un pseudo différent pour chaque compte : un pour jouer en réseau, et pour son blog, ... ! Ainsi, on peut compartimenter les informations que l'on communique et mieux maîtriser qui y a accès.
- Choisir un pseudo neutre: ni féminin ni masculin et éviter les pseudos pouvant avoir une connotation sexuelle: Sexyboy, Priscilla, lapinou, bambi, etc.
- Pourquoi ne pas choisir des pseudos qui signifient vos goûts pour inciter ceux qui partagent vos passions plutôt que les autres à vous contacter?
- Vous pouvez aussi inventer des noms qui n'existent pas et miser sur un pseudo original!

3. Gérer son profil

Conseils clés

- Paramétrage
 - Prendre le temps d'explorer les options disponibles, ne pas se contenter des options par défaut.
 - Se poser les bonnes questions : qu'est-ce que je veux montrer à qui ?
 - Public ou privé ? Ce n'est pas le même type d'échange
 - Vérifier régulièrement que l'on est à jour - Les services évoluent vite et les nouvelles versions peuvent modifier vos choix.
- Données personnelles
 - Inutile, à l'inscription, de fournir les informations facultatives
 - Ne livrer qu'un nombre limité d'informations personnelles, et surtout pas ses coordonnées, numéro de téléphone, etc.
 - Lire les conditions générales d'utilisation, même si elles sont longues !
 - Ne pas mentir sur son âge.

Animation :

A partir de ces informations pratiques, créer « le pseudo parfait »

Choisir la meilleure photo pour le profil (au choix parmi 3)

Animation :

1 - Vidéo Dave le Voyant

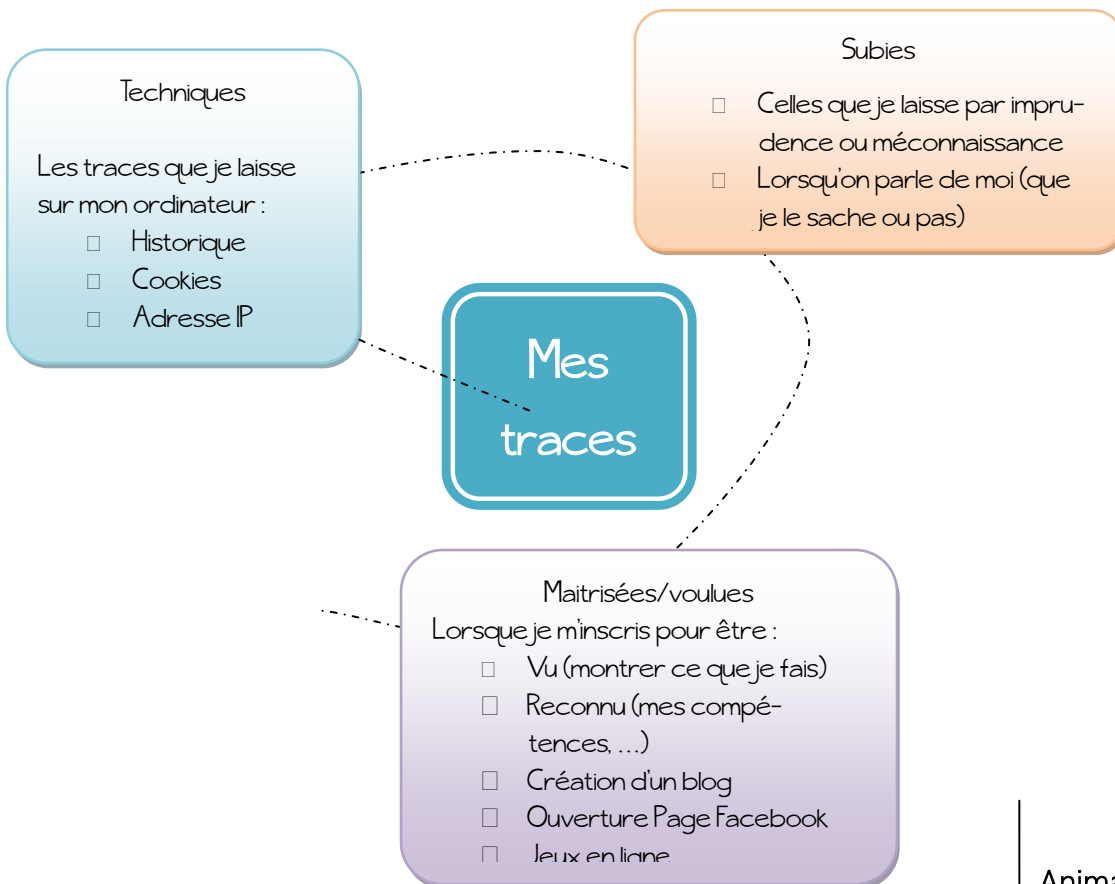
2 – Affichage de la fausse page facebook

Leur faire dire ce qui ne va pas sur cette page :

- Avatar
- Pseudo
- Informations
- Photos
- Age...

- Gérer son identité en ligne
 - Eviter la publication de textes ou d'images dévalorisantes de soi et des autres : elles pourraient être utilisées plus tard, par exemple par vos futurs employeurs
 - Utiliser régulièrement des moteurs de recherche pour savoir ce qui est visible de soi sur le net
 - En cas d'image ou info problématique détecté, réagir rapidement en demandant leur retrait à la personne/site qui l'a publié. Voire en signalant au réseau social le problème, en saisissant la CNIL ou portant plainte si cela ne fonctionne pas.

4. Les traces que je laisse sur Internet et sur mon ordinateur



Light Beam

Lightbeam est une extension pour Firefox qui fait appel à des visualisations interactives pour vous montrer avec quels sites tiers vous communiquez sans le savoir. À mesure que vous naviguez, Lightbeam vous révélera les coulisses du Web d'aujourd'hui, y compris les parties les moins visibles pour l'utilisateur moyen.

Animation :

Aller sur le site de TF1 et lancer LightBeam. Que remarquez-vous ? Voulez-vous aller sur les sites tiers ? Que cela peut-il avoir comme conséquences ?

L'Historique des géolocalisations

Il suffit que vous soyez équipé d'un smartphone ou une tablette tactile fonctionnant sous le système d'exploitation Android et que vous ayez accepté de partager des données de géolocalisations.

Elles sont très utiles lorsque vous cherchez une rue ou un restaurant... Que vous circuliez en voiture, à pied, en vélo, Google sait exactement où vous êtes 365 jours sur 365, 24h/24.

En consultant cette carte, c'est même Google qui vous rappelle ce que vous avez fait l'avant-veille. C'est une véritable carte de votre vie quotidienne.

Le droit à l'oubli

Vieil article de journal, fausses informations, « blog de jeunesse » ... L'absence de droit à l'oubli sur Internet peut poser de vrais problèmes à certains particuliers, notamment dans le cadre de leur vie professionnelle. C'est dans le but de protéger la vie privée des citoyens européens qu'une décision récente de la CJUE (Cour de justice de l'Union européenne) a conduit Google Europe à mettre en place une procédure de demande de suppression de contenu en faveur de ses utilisateurs.

5. Les mots de passe

Moyen mnémotechnique :

Voici un bon moyen de créer des mots de passe solides, tout en les retenant facilement : **les moyens mnémotechniques !**

Transformez par exemple une phrase simple comme "J'ai été acheter du pain" en mot de passe : **GeThTdup1** pour obtenir un mot de passe ayant une résistance de **plusieurs jours**.

Si vous rajoutez un seul caractère spécial comme par exemple "@", votre mot de passe **GéThTdup1@** est alors doté d'une résistance de **plusieurs années** aux programmes pirates !

Tester votre mot de passe

<https://howsecureismypassword.net>

Animation :

4

Montrer au tableau un exemple de Géolocalisation

Les faire aller sur le questionnaire. Lien sur les postes

Aller sur HowsecureIsMyPassword et faire trouver le mot de passe le plus long à trouver en 8 caractères

Mots de passe à éviter

- votre identifiant
- votre nom
- votre prénom ou celui d'un proche (conjoint, enfant, etc.) ;
- un mot du dictionnaire ;
- un mot à l'envers (les outils de cassage de mots de passe prennent en compte cette possibilité) ;
- un mot suivi d'un chiffre, de l'année en cours ou d'une année de naissance (par exemple « password1999 »).

En conclusion :

Ne dévoile pas ta vie privée

Ne mets pas de photos et vidéos provocatrices

Ne donne jamais ton adresse ou numéro de téléphone

N'accepte pas d'inconnus dans ton réseau d'amis

Protège tes mots de passe

En cas de problème, parles-en à un adulte