

Place de la Cybersécurité dans les enseignements SNT/NSI

Place de la Cybersécurité dans les enseignements SNT/NSI

« [...] l'enseignement de sciences numériques et technologie en classe de seconde a pour objet de permettre d'appréhender les principaux concepts des sciences numériques, mais également de permettre aux élèves, à partir d'un objet technologique, de comprendre le poids croissant du numérique et les enjeux qui en découlent. »

Programme de SNT, préambule

Place de la Cybersécurité dans les enseignements SNT/NSI

Décret n° 2019-919 du 30 août 2019 relatif au développement des compétences numériques dans l'enseignement scolaire, dans l'enseignement supérieur et par la formation continue, et au cadre de référence des compétences numériques (CRCN)



JORF n°0203 du 1 septembre 2019

<https://app.pix.fr/campagnes/JBKZDH685>

Place de la Cybersécurité dans les

2.4 S'insérer dans le monde numérique

Maîtriser les enjeux de la présence en ligne, développer des stratégies et des pratiques autonomes en respectant les règles, les droits et les valeurs qui leur sont liés, pour se positionner en tant qu'acteur social, économique et citoyen dans le monde numérique, et répondre à des objectifs (avec les réseaux sociaux et les outils permettant de développer une présence publique sur Internet, et en lien avec la vie citoyenne, la vie professionnelle, la vie privée...).

dans l'enseignement scolaire dans

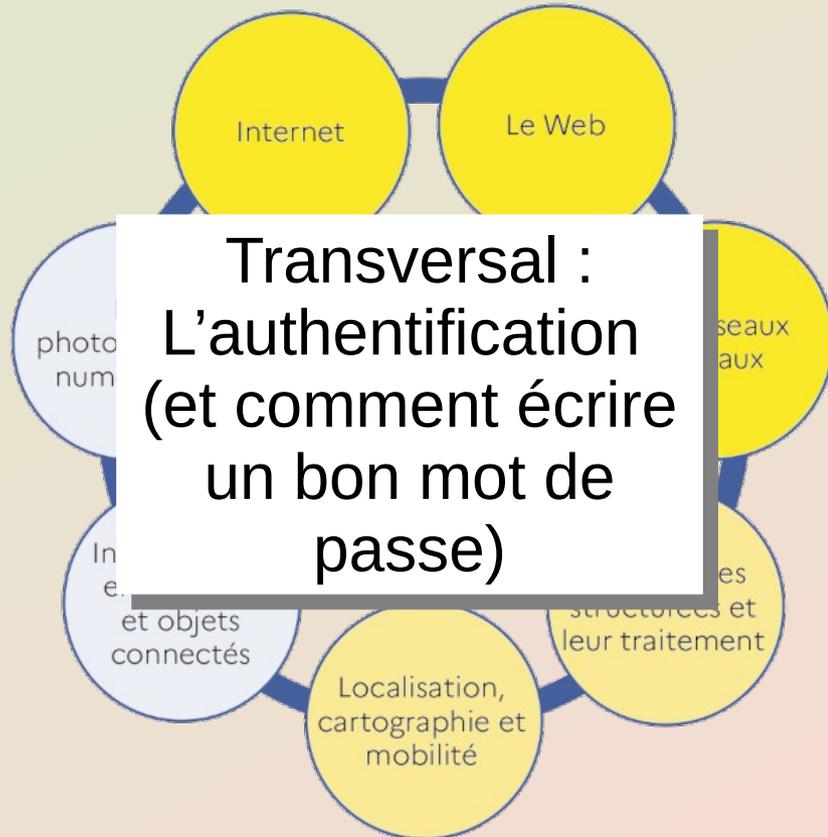
4.1. Sécuriser l'environnement numérique

Sécuriser les équipements, les communications et les données pour se prémunir contre les attaques, pièges, désagréments et incidents susceptibles de nuire au bon fonctionnement des matériels, logiciels, sites internet, et de compromettre les transactions et les données (avec des logiciels de protection, la maîtrise de bonnes pratiques...).

4.2. Protéger les données personnelles et la vie privée

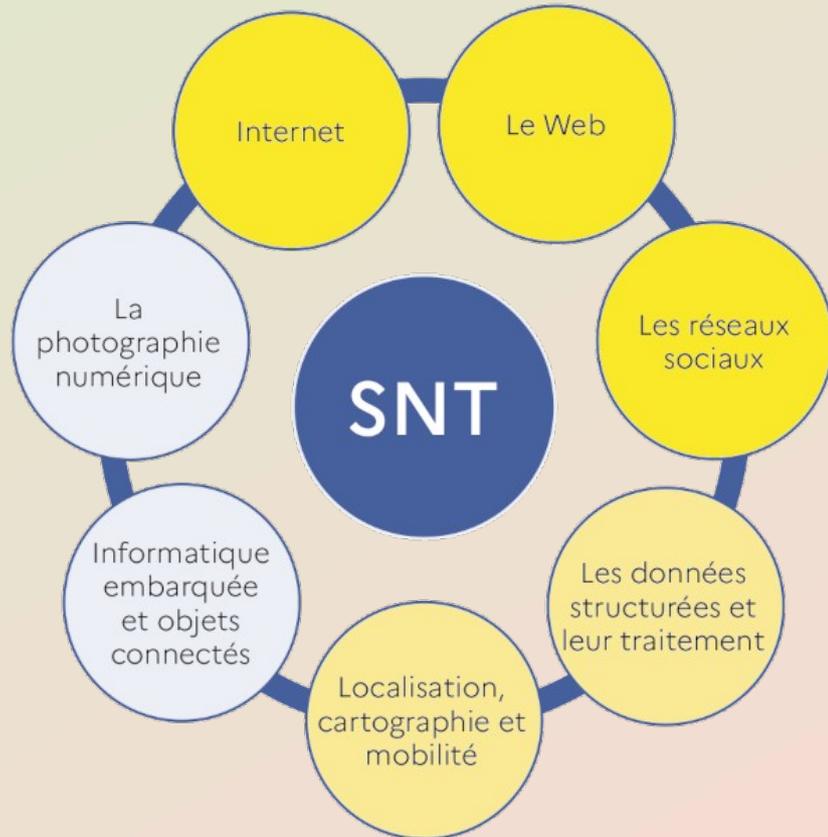
Maîtriser ses traces et gérer les données personnelles pour protéger sa vie privée et celle des autres, et adopter une pratique éclairée (avec le paramétrage des paramètres de confidentialité, la surveillance régulière de ses traces...).

Place de la Cybersécurité dans les enseignements SNT/NSI



- Internet
- Le Web
- Les réseaux sociaux
- Les données structurées...
- Localisation, cartographie et mobilité

Place de la Cybersécurité dans les enseignements SNT/NSI



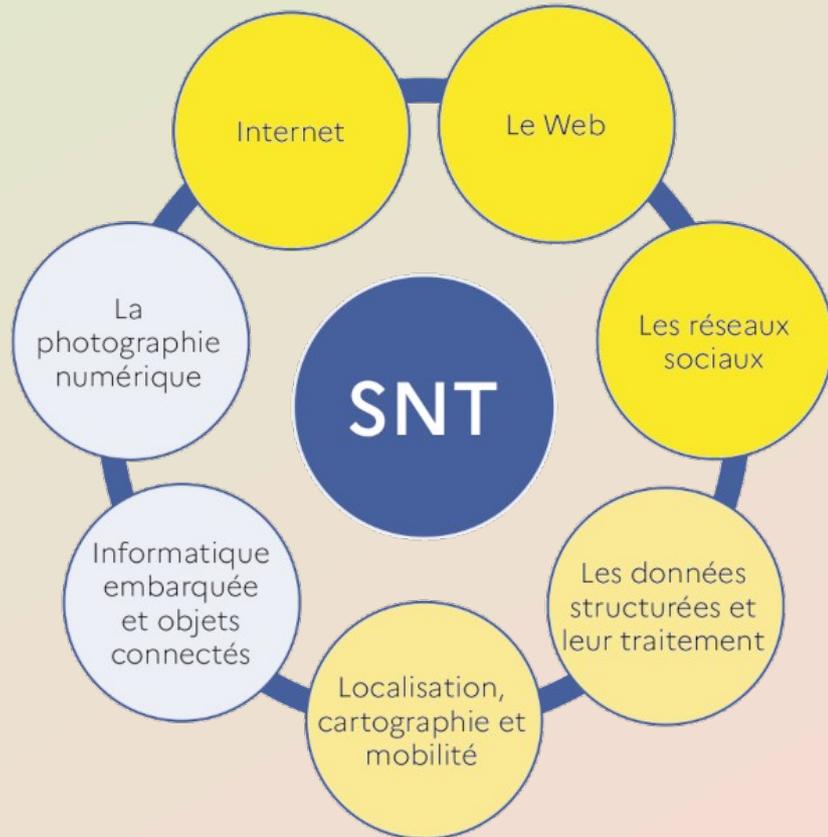
- Internet

- Protocole TCP/IP,
- Rôle d'un serveur/routage/peer to peer.

- Le Web

- Comprendre une URL,
- HTTP vs HTTPS,
- Notions juridiques,
- Cookies, navigation privée

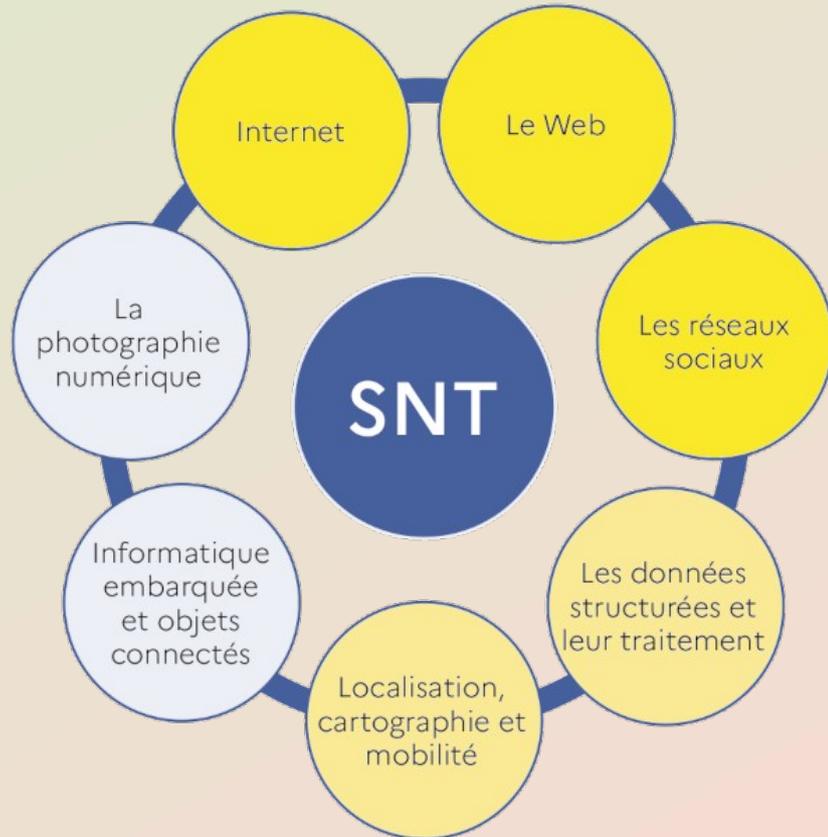
Place de la Cybersécurité dans les enseignements SNT/NSI



- Les réseaux sociaux

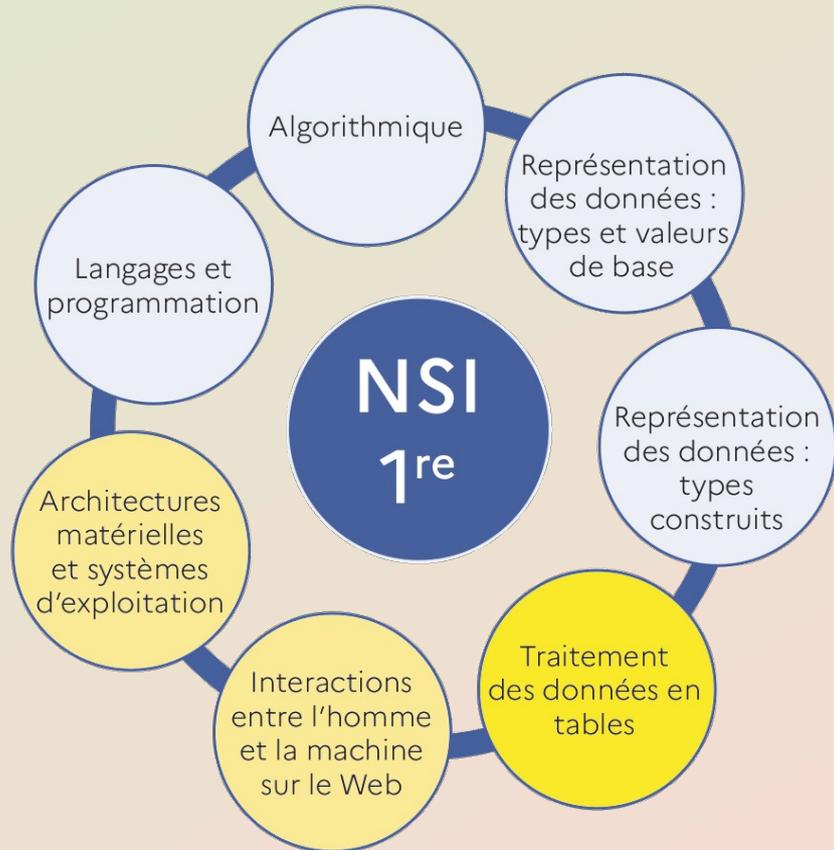
- Paramétrer ... pour assurer la confidentialité des données personnelles,
- Identifier les sources de revenus des entreprises de réseautage social,
- Connaître les différentes formes de cyber violence... pour lutter contre [...] et art. 222-33-2-2 du code pénal

Place de la Cybersécurité dans les enseignements SNT/NSI



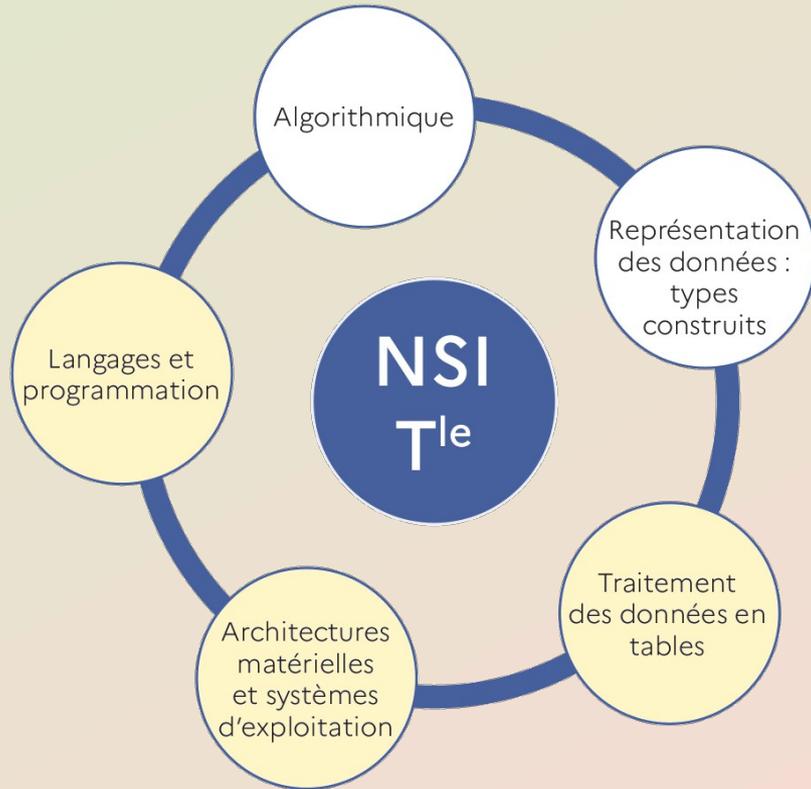
- Les données structurées...
 - Définir une donnée personnelle,
- Localisation, cartographie et mobilité
 - La localisation est une donnée à caractère personnelle.

Place de la Cybersécurité dans les enseignements SNT/NSI



- Traitement des données en tables
 - Rappel SNT : Données personnelles
 - hors programme : données sensibles (et RGPD)
- Interaction Humain-Machine sur le Web
 - Requêtes HTTP POST/GET : rappel HTTPs
 - A la limite du programme : Injections SQL
- Architectures matérielles et SE
 - hors programme : Quel est le modèle économique des éditeurs de SE libre ?
 - hors programme : Neutralité du Net

Place de la Cybersécurité dans les enseignements SNT/NSI



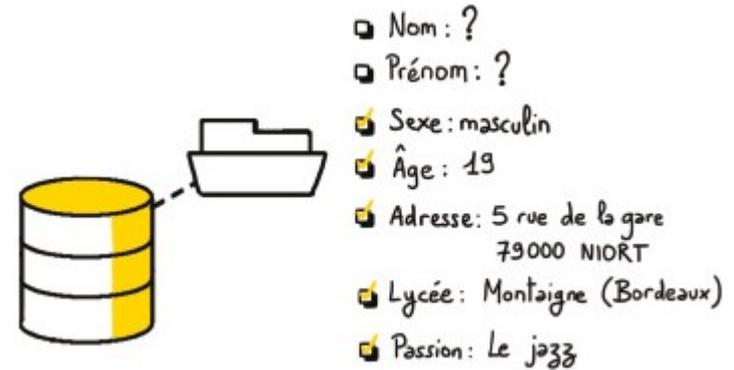
- Traitement des données en tables
- Architectures matérielles et SE
 - Matériel embarqué, IoT,
 - Matériel médical,
 - NIS2
- Langages et Programmation
 - Si API : authentification ?

Données personnelles

Une « donnée à caractère personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

- **directement** (exemple : nom, prénom)
- **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).
- **par croisement** d'un ensemble de données (le centenaire du village, une mère célibataire dans l'immeuble Y, etc.)



Données sensibles

Une « donnée sensible » est « une donnée personnelle » qui concerne l'une de ces catégories :

- opinions politiques ou syndicales,
- origine ethnique ou raciale,
- convictions religieuses ou philosophique
- données médicales, génétiques ou biométriques,
- orientation sexuelle ou vie sexuelle.



Injections SQL



The screenshot shows a web page titled "Login". A white box with a black border and a grey drop shadow is overlaid on the top left, containing the text "cbedos is logged" in black. Below this, a message says "Please sign-in". There are two input fields: "Username" containing "cbedos" and "Password" containing ".....". A "Login" button is below the fields. At the bottom, it says "Dont have an account? [Please register here](#)". A green arrow points from the "cbedos" text in the message box to the PHP code on the right.

```
// code php  
$sql = "select * from user  
where username = '". $_POST['username'] . "'  
and password = '". $_POST['password'] . "'";
```



```
select * from user  
where username = 'cbedos'  
and password = 'mot de passe'
```

Rappel : en SQL la syntaxe pour définir un commentaire jusqu'à la fin de la requête est --

Injections SQL



The screenshot shows a web page titled "Login". At the top, a message says "cbedos is logged". Below this, there is a "Please sign-in" section with two input fields: "Username" containing "cbedos' --" and "Password" containing ".....". A "Login" button is positioned below the fields. At the bottom of the form, there is a link: "Dont have an account? [Please register here](#)". A green arrow points from the "cbedos' --" input field towards the PHP code on the right.

```
// code php  
$sql = "select * from user  
where username = '". $_POST['username'] . "'  
and password = '". $_POST['password'] . "'";
```

↓

```
select * from user  
where username = 'cbedos' -- '  
and password = 'mauvais mot de passe'
```

```
select * from user where username = 'cbedos'
```

```
-- ' and password = 'mauvais mot de passe'
```

Attention : le vademecum donne un exemple avec le symbole # qui commente jusqu'à la fin de la ligne → source d'erreurs.

Neutralité du Net

Pour aller plus loin :

- En 6 min, source Le Monde
<https://youtu.be/A3dElmSY8q4?si=yn-Ez-isPn7-cKSS>
- En 20 min, source M. Bidouille, avec un rappel du routage par paquets
https://youtu.be/A7sOxBgajuo?si=U-LH_j_jdfn1lkKU
- La Quadrature du Net
https://www.laquadrature.net/neutralite_du_net/

Sécurité des matériels embarqués

Les IoT sont embarqués dans :

- des objets dont le cycle de vie est très long en termes informatique (voiture, IRM, avion...),
- des secteurs sensibles (transport, médical, sécurité, énergie, défense),
- des systèmes difficiles à mettre à jour (fonctionnent sur batterie, connexion intermittente voire inexistante)

Sécurité des matériels embarqués

La législation est en évolution :

- NIS, NIS2 (Network and Information Security),
- IoT-SSF : IoT Security and Safety Framework,
- Directive RED : Directive relative aux équipements hertziens,
- MDR : Medical Devices Regulation, DMDIV : In Vitro Diagnostic Medical Devices Regulation,
- EN 303 645 : Norme européenne sur la cybersécurité des objets connectés,
- CEI 62443-4-2 : Norme internationale sur la cybersécurité des systèmes industriels

Sécurité des matériels embarqués

Vidéo de Micode sur les nouvelles techniques de car-jacking

<https://www.youtube.com/watch?v=...>

Voir aussi, le mouse-jacking :

<https://media.roole.fr/quotidien/voitures-quelle-est-la-technique-de-lampleur>



Une authentification forte

Mon mot de passe ?

minuscules /
 majuscules / chiffres /
caractères spéciaux

Il coche toutes les cases !



Une authentification forte

Pour créer un mot de passe fort, il est recommandé de suivre ces quelques règles d'or :

- longueur d'au moins 12 caractères,
- au moins une majuscule,
- au moins une minuscule,
- au moins un chiffre,
- au moins un symbole/caractère spécial accessible au clavier.



Une authentification forte

Le mot de passe ne doit pas être significatif :

- ce n'est pas une date ou une année,
- ce n'est pas un prénom, même transformé,
- ce n'est pas un mot, même transformé,

Bannir tout mot issu d'un dictionnaire, même
sous forme de leet speak.

Une authentification forte

Le mot de passe ne doit pas être significatif :

- ce n'est pas une date ou une année,
- ce n'est pas un prénom, même transformé,
- ce n'est pas un mot, même transformé,
- **il ne dit rien sur vous.**



Source & image : <https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe>

Une authentication forte

Mon mot de passe



n'est pas unique

Une authentification forte est à double facteur !

- Je connais un secret, ➤ Mot de passe
- Je possède un objet, ➤ OTP via SMS
- Je suis physiquement présent. ➤ Biométrie

2 techniques sur les trois => Authentification à 2 facteurs (2FA)

Une authentification forte est à double facteur !



Merci pour votre attention.