DANE INFO INFO N°9

janvier 2017

Pour un bon usage d'Internet

SOMMAIRE

Avec l'évolution des technologies de l'internet, les relations sociales utilisent de plus en plus les outils numériques qui ont déjà supplanté certains moyens de communication traditionnels. La majorité des citoyens français a d'ores et déjà massivement recours à ces moyens de communication souples et modernes et tous en auront besoin demain tant pour leurs usages professionnels que personnels. Les échanges sont facilités, les possibilités de diffusion de la connaissance multipliées. Mais cette nouvelle ère des relations sociales ouvre aussi aux individus de nouvelles possibilités de nuire les uns aux autres, transposant dans le numérique des comportements déviants qui lui sont antérieurs, les facilitant, en faisant apparaître de nouveaux. Dérives, usages malveillants, diffusion de contenus illégaux ou inappropriés aux mineurs, mais aussi comportements à risques d'adolescents se mettant eux-mêmes en danger, ne régressent pas à l'ère du numérique.

Dans ce contexte, l'Éducation travaille depuis des années à sensibiliser les élèves dont elle a la charge, chacun selon son âge et les risques qu'il encourt aux usages responsables de l'internet. La gendarmerie nationale propose en partenariat depuis des années, des actions au sein des écoles ou des établissements secondaires pour sensibiliser personnels, parents et élèves aux conséquences des mauvais usages de l'internet.

Il nous a donc semblé tout naturel, sur le territoire de l'académie de Nancy-Metz, de joindre nos efforts dans le chantier de la formation des jeunes générations aux usages de l'internet.

Gigantesque chantier parce qu'il touche tous les futurs citoyens et que la population d'âge scolaire en Lorraine représente plus de 400 000 personnes (dont 190 000 environ pour l'enseignement secondaire), réparties sur un vaste territoire. Il faut aussi que notre action s'adapte à des intérêts et à des usages très différents d'un âge à l'autre. Enfin, l'évolution rapide et la diversité croissante des services numériques demandent une adaptation constante des messages à faire passer.

Ce document permet de souligner les sujets sur lesquels les équipes de l'académie et de la gendarmerie travaillent à mieux sensibiliser et informer les enseignants et les élèves : la cybercriminalité et la sécurité informatique, la protection de l'identité numérique, etc.

Nous espérons qu'il constituera un premier pas au service des jeunes lorrains.

Marie Reynier
Recteur de la région académique Grand Est
Recteur de l'académie de Nancy-Metz,
Chancelier des universités

Général de division Thibault Morterol, commandant la région de gendarmerie d'Alsace-Champagne-Ardenne-Lorraine et la gendarmerie pour la zone de défense et de sécurité Est

académie Nancy-Metz
RÉGION ACADÉMIQUE GRAND EST
MINISTÈRE DE L'ÉDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

Du côté des élèves

L'élève victime...

1. D'adultes

L'internet (réseaux sociaux, applications, messageries en tout genre) permet à des adultes de se faire passer pour des mineurs en se dissimulant sous une identité d'emprunt. Il est donc un moyen privilégié de l'agression sur les enfants, piégés ainsi plus facilement.

2. D'autres élèves

•*happy-slapping* : il consiste à se rendre complice d'une agression en filmant des violences en les diffusant sur internet : il est punissable comme l'agression elle-même ;

•*sexting* et *dedipix* : des mineurs imprudents communiquent des images ou des messages de type SMS, à caractère sexuel, dont il est impossible ensuite d'arrêter ou de maîtriser la diffusion sur le réseau ;

•enfin, le cyber harcèlement, où un mineur devient la victime d'agressions répétées de camarades. L'outil numérique peut ainsi prolonger une violence qui prend naissance dans l'établissement scolaire ou en dehors.

3. De lui-même

Sans que cela diminue en rien la responsabilité des agresseurs, force est de constater qu'un élève peut se mettre en danger en communiquant à autrui des informations confidentielles. À cela il faut ajouter :

- une dépendance excessive aux outils numériques qui peut couper l'élève de ses relations amicales ou familiales et mettre en danger ses résultats scolaires ;
- une diffusion imprudente d'informations personnelles sur les réseaux sociaux : désormais, les recruteurs consultent les réseaux sociaux et beaucoup peuvent renoncer à une embauche en fonction de ce qu'ils y trouvent.

4. Le rôle des parents

Les responsables légaux des élèves ont un rôle à jouer dans la prévention des risques liés à l'Internet et au numérique notamment par :

- la mise en place d'un dispositif de protection des mineurs sur les appareils connectés (ordinateurs, *smartphones* et autres) ;
- l'installation d'un ordinateur dans un espace commun à toute la famille (mais cela suppose que l'enfant n'ait pas de smartphone susceptible de naviguer sur Internet) et l'exercice d'une surveillance adaptée à l'âge des enfants considérés.

Rappel juridique

La cybercriminalité est constituée d'infractions pénales dans le domaine numérique. Un infraction suppose trois choses :

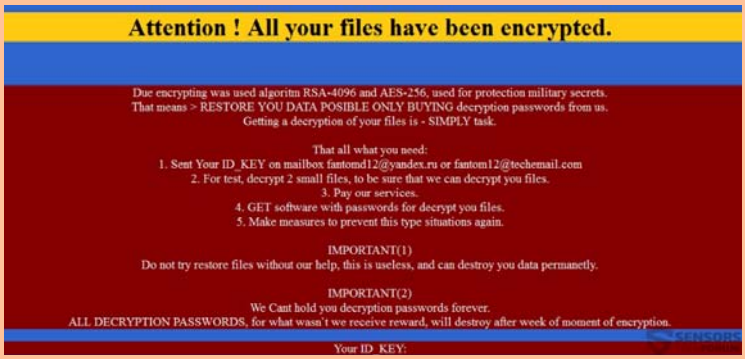
- un élément légal, c'est-à-dire une règle juridique enfreinte : « pas de peine sans loi » ;
- un élément matériel, c'est-à-dire la commission ou l'omission d'un acte ;
- un élément moral, imprudence ou volonté de commettre la faute pénale en question.
- Les infractions peuvent être plus ou moins graves, de la contravention (punie d'une amende jusqu'à 3000 €) au crime en passant par le délit.

Du côté des adultes

Un impératif de sécurité

Chacun est responsable des données dont il a la garde :

- sécuriser les fichiers contenant des données confidentielles ;
- mettre à jour de manière systématique et régulière les systèmes d'exploitation, applications, antivirus et autres programmes de sécurité ;
- **veiller à la protection de ses identifiants et mots de passe, ne jamais les communiquer ni les laisser accessibles, le changer régulièrement ;**
- **utiliser des mots de passe différents pour des services différents.**



Attention au hameçonnage (ou phishing)

Il s'agit d'une technique destinée à faire croire que l'on s'adresse à un tiers de confiance (banque, administration, etc.) pour extorquer des renseignements confidentiels (coordonnées bancaires, numéro de carte bancaire, identifiant et mot de passe) et en faire une utilisation frauduleuse. Ne communiquer de telles données que lorsque la connexion est sécurisée : c'est-à-dire lorsque l'adresse commence par https://.

Des conseils de prudence

- N'entrer en relation qu'avec des personnes que **l'on connait par ailleurs.**
- **Il y a des données qui ne doivent pas être rendues accessibles à tout le monde, d'autres qui peuvent être communiquées à des proches, d'autres enfin qui doivent rester absolument secrètes. Il faut prendre conscience ou se souvenir de la fragilité des relations humaines.**
- **Apprendre à utiliser des identités numériques différentes en fonction de ses activités.**
- **Ne pas utiliser de programmes contrefaits ou de faux antivirus.**
- **Si une conduite paraît un tant soit peu risquée, dans le doute, s'abstenir.**

Il n'y a pas de miracle sur internet

Une offre de transfert d'argent est une tentative d'escroquerie…
Un produit (*smartphone*, voiture, location de vacances, etc.) proposé à un prix trop bas est bien souvent une escroquerie, un objet contrefait, volé ou fictif, voire une prestation inexistante.

Les établissements

L'établissement ou son personnel peuvent aussi devenir victime :

- d'attaque sur sa réputation (dénigrement ou calomnie) ;
- de *défaçage* de site internet ;
- d'usurpation d'identité et d'intrusion dans le système d'information (par exemple pour falsifier des notes, détruire des données).

Et il n'est pas impossible que l'agression soit le fait d'élèves.

Les actions de prévention de la gendarmerie

- Intervention de prévention dans les collèges et les lycées par les brigades de prévention de la délinquance juvénile.
- Conférences sur la cybercriminalité par les enquêteurs en technologies numériques.
- Plateforme *Pharos* de signalement des contenus illégaux sur internet : https://www.internet-signalement.gouv.fr/.
- Veille continue sur l'internet au Centre de lutte Contre les Criminalités Numérique de Pontoise (C3N).
- Maillage territorial d'enquêteurs spécialisés (N'TECH et correspondants N'TECH)
- Cyber-infiltration.
- Mise en place du permis internet pour les élèves de CM2.

Les actions de prévention de la DANE

Le *Bon usage de l'internet* est un dispositif académique permettant d'informer les élèves sur les bonnes pratiques et les risques liés aux usages des outils numériques.
La DANE mène également les actions suivantes :

- éditions d'affiches d'information envoyées dans les établissements et disponibles sur demande ;
- veille sur les sites internet pédagogiques ;
- conseil pour la rédaction des chartes de bon usage ;
- animation, avec les collectivités partenaires de la commission locale de l'informatique et des libertés pour les E.N.T. ;
- informations et organisations de conférence sur ces thèmes à destination des référents aux usages pédagogiques du numérique.

Contacts :

Gendarmerie nationale

Brigade de prévention de la délinquance juvénile de Meurthe-et-Moselle
bpdj.ggd54@gendarmerie.interieur.gouv.fr
Brigade de prévention de la délinquance juvénile de Moselle
bpdj.ggd57@gendarmerie.interieur.gouv.fr
pour les établissements en zone gendarmerie

Délégation Académique au Numérique pour l'Éducation

CO 30 013
10, rue de Santifontaine
54035 NANCY CEDEX
ce.dane@ac-nancy-metz.fr

http://www4.ac-nancy-metz.fr/dane/
@Dane_nancy_metz