HYGIÈNE INFORMATIQUE

TD1 - 1H

1STI2D

1. Pourquoi l'hygiène informatique ?

Les formidables développements de l'informatique et d'Internet ont révolutionné nos manières de vivre et de travailler. La perte ou le vol de certaines informations ou l'indisponibilité du système d'information d'une organisation (une entreprise, une association, un établissement…) peuvent avoir de lourdes conséquences pour l'organisation : perte ou falsification de données, perte de confiance des clients, avantage pris par un concurrent, perte d'exploitation ou de services.

Pour se prémunir de ces préjudices, il existe des mesures techniques simples, qualifiées d'hygiène informatique car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire. Parmi ces mesures, on trouve la **charte informatique** et **10 règles de base à respecter proposées par l'ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information).

Une **charte informatique** est un document élaboré par une organisation, dont le but est de délimiter les droits et obligations en matière d'utilisation du système d'information et de communication des employés, membres ou adhérents de l'organisation en question.

2. Jurisprudence

Dans la jurisprudence donnée en exemple ci-dessous, quatre étudiants ont enfreint des articles du code pénal liés aux STAD.

Exemple de jurisprudence Tribunal de Grande instance de Vannes, jugement du 13 juillet 2005

IUT de Vannes. Quatre étudiants condamnés pour piratage

Quatre étudiants de l'IUT informatique de Vannes, qui s'étaient introduits illégalement dans le réseau de l'Université de Bretagne Sud, ont été condamnés chacun à une amende de 1000€ avec sursis, par le tribunal de Vannes. Étant donné « l' absence de condamnations antérieures et la jeunesse des quatre prévenus « , âgés de 19 à 20 ans , les juges ont décidé que cette condamnation ne figurerait pas à leur casier judiciaire ».
Tous les quatre avaient reconnu avoir téléchargé, puis utilisé un logiciel de décryptage de mots de passe, dont la détention est prohibée par une loi votée en juin 2004.
Ils avaient ainsi pu se procurer chacun au moins une centaine de mots de passe, permettant l'accès à des données confidentielles appartenant à d'autres étudiants (courriers électroniques , travaux pratiques , etc.) .
Dans cette même affaire, les quatre étudiants ont été sanctionnés, le 6 juillet dernier, par la commission disciplinaire de l'Université de Bretagne Sud. Le principal fautif a été exclu de l'UBS pour une durée de deux ans. Un autre a écopé de la même sanction, mais assortie du sursis et pour une durée d' un an . Les deux derniers ont quant à eux reçu un blâme.
Pour caractériser l'intention coupable, le juge se référait à la signature par les dits étudiants d'une charte de bon usage des ressources informatiques.
Considérant que ces quatre étudiants, âgés de 18 à 20 ans au moment des faits et jamais condamnés avant, ont fait preuve **« d'une attitude de défi sous une forme technologique propre à la jeunesse sans conséquence préjudiciable pour les comptes utilisateurs usurpés »**, le Tribunal les a condamnés à une peine d'amende avec sursis.

2.1 Recherchez et donnez la définition de STAD

2.2 Utilisez le document Législation et monde numérique.pdf pour répondre aux questions suivantes .

- Trouver quels articles du code pénal ont été violés.

- Expliquer avec vos mots, ce que signifient ces articles.

- Donner les peines encourues par les quatre étudiants.

- Expliquer ce qui pour le juge a fait basculer un défi technologique entre étudiants à une intention coupable qui entraîne la condamnation.

- Conclure sur l'utilité de la charte avant de la rendre signée par vous et un responsable légal si vous êtes mineur.

3. La charte du lycée

La charte informatique du lycée vous a été fournie dans le livret d'accueil. Vous avez dû la signer au même titre que le règlement intérieur. Elle vous engage à un bon usage et vous protège sur le réseau du lycée.

Charte de bon usage de l'Internet et des réseaux

(conforme à la charte nationale BOEN n°9 du 26 janvier 2004)

Les élèves de l'établissement : FELIX LE DANTEC, 22303 LANNION *s'engagent à respecter la présente charte. Leurs parents en ont communication, y adhèrent et s'engagent à faciliter sa mise en application.*

La charte a pour objet de définir les conditions d'utilisation des ordinateurs et des réseaux dans le cadre des activités du lycée. Elle engage l'établissement et tous les élèves utilisateurs, et concerne les activités pédagogiques, éducatives et administratives.
Elle s'appuie sur le respect des lois en vigueur et des valeurs fondamentales de la République, en particulier le principe de neutralité religieuse, politique et commerciale, le respect du droit de propriété.

Les services suivants sont proposés par l'établissement au service de la scolarité de l'élève :
La possibilité de disposer d'un dossier personnel de travail.
L'accès à l'ensemble des ressources et services de l'Internet autorisés par l'établissement.

L'établissement s'engage à :

Protéger, dans le respect de la loi, le droit de l'élève à la protection de sa vie privée.
Informer clairement les élèves de leurs droits et de leurs devoirs.
Filtrer et surveiller les accès à l'Internet afin d'éviter dans la mesure du possible toute forme d'agression à l'égard de l'élève aussi bien que vers l'extérieur de l'établissement,
Informer les autorités des délits constatés.

L'élève s'engage à :

Respecter la loi, en particulier ne pas consulter délibérément, publier ou promouvoir des documents à caractère diffamatoire, pornographique, raciste ou xénophobe, incitant aux crimes, aux délits, à la haine, ou portant atteinte à la vie privée, au droit à l'image ou au droit d'auteur.
Ne pas s'approprier le mot de passe ou l'identité d'un autre utilisateur.
Ne pas lire, modifier, détruire, copier, diffuser des informations sans s'être assuré qu'il a le droit de le faire.
Ne pas interrompre ou gêner le fonctionnement normal des réseaux, prendre soin du matériel informatique mis à sa disposition.
Ne pas produire ou introduire délibérément de virus ou tout dispositif destiné à contourner les mesures de sécurité ou détourner les installations de leur usage normal.
Ne pas utiliser les installations et ressources mises à sa disposition par l'établissement à des fins commerciales, de prosélytisme politique ou religieux, ou de domaine idéologique opposé aux valeurs de la République.
Ne pas tenter d'accéder dans le cadre des activités pédagogiques à des catégories de ressources sans rapport avec les objectifs d'apprentissage, documentaires, éducatifs de l'établissement.
Informer son responsable de toute anomalie constatée.

Sanctions :

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à ce que son accès aux ressources informatiques soit strictement limité aux actes pédagogiques décidés sous la responsabilité des enseignants. Il s'expose également aux sanctions prévues par le règlement intérieur et à des poursuites civiles et pénales*.
L'établissement se réserve le droit de procéder à des contrôles du bon usage des installations et des sites visités.
* Cf tableau ci-dessous

CIRCULAIRE N°2004-035 DU 18-2-2004 (NOR : MENT0400337C).

Exemple	Infraction	Textes légaux de référence	Sanction légale
Photos publiées sans autorisation	Droit à l'image	Art. 1382, 1383, 9 Code civil Art. L226-1, L226-2 Code pénal	1 an de prison 45000 euros d'amende
Caricature faite à partir d'une photo publiée sans autorisation	Représentation des personnes	Art. 1382, 1383 Code civil Art. L226-8 Code pénal	1 an de prison 15000 euros d'amende
Publication d'images ou de textes trouvés par exemple sur Internet, sans autorisation de disposer des droits	Droit d'auteur	Art. 1382, 1383 Code civil Art. L335-2, L335-3, L335-4 CPI (Code de la Propriété Intellectuelle)	3 à 5 ans de prison 300000 à 500000 euros d'amende
Publication d'un logo protégé	Droit des marques	Art. 1382, 1383 Code civil Art. 716-10 CPI	3 ans de prison 300000 euros d'amende
Commentaires racistes, injurieux ou diffamatoires sur un camarade ou un professeur	Diffamation	Art. 1382, 1383 Code civil Art. 23, 31, 32, 34 loi du 29 juillet 1881	Diffamation : 12000 euros Injure raciale : 6 mois à 1 an de prison, 22500 à 45000 euros d'amende
Langage vulgaire (Ex. : « N…. ta mère ! »)	Message contraire à la décence	Art. 1382, 1383 Code civil Art. R624-2 Code pénal	750 euros d'amende

Je m'engage à respecter cette charte et à adopter une conduite respectueuse des autres usagers.

À le

(NOM) (PRÉNOM) (SIGNATURE)

(NOM, PRÉNOM et SIGNATURE D'AU MOINS UN DES RESPONSABLES)

4. Les 10 règles de l'ANSSI : les 10 commandements de la sécurité sur l'Internet

Ouvrez et lisez le document « 10reglesanssi.pdf », notez ici les 10 points clefs.

1		6	
2		7	
3		8	
4		9	
5		10	

5. Comment bien choisir son mot de passe ?

Vous allez avoir différents accès au réseau dans l'établissement, pour sécuriser ces accès, changez rapidement vos mots de passe par défaut.

R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

6. Pourquoi ?

6.1 Visionnez les exploits des 4 candidats de la HACK academy.

Jenny : https://www.youtube.com/watch?v=lRqT3PtxA0Q

Dimitri : https://www.youtube.com/watch?v=SbfQLM7Az5s

Martin : https://www.youtube.com/watch?v=ytUhNkPWHqw

Willy : https://www.youtube.com/watch?v=OmH1oL0Op6k

6.3 à partir des documents disponibles sur le site, dressez une liste des recommandations de la HACK academy concernant les 9 sujets suivants :

- Le Phishing
- Le vol de mots de passe
- Les logiciels malveillants
- Les payements sécurisés
- Le social engineering
- La navigation sécurisée
- Les connexions internet publiques
- Les USB inconnues
- Réseaux sociaux

Le site : https://sin.ledantec-numerique.fr/wp-content/uploads/hack_academy.pdf