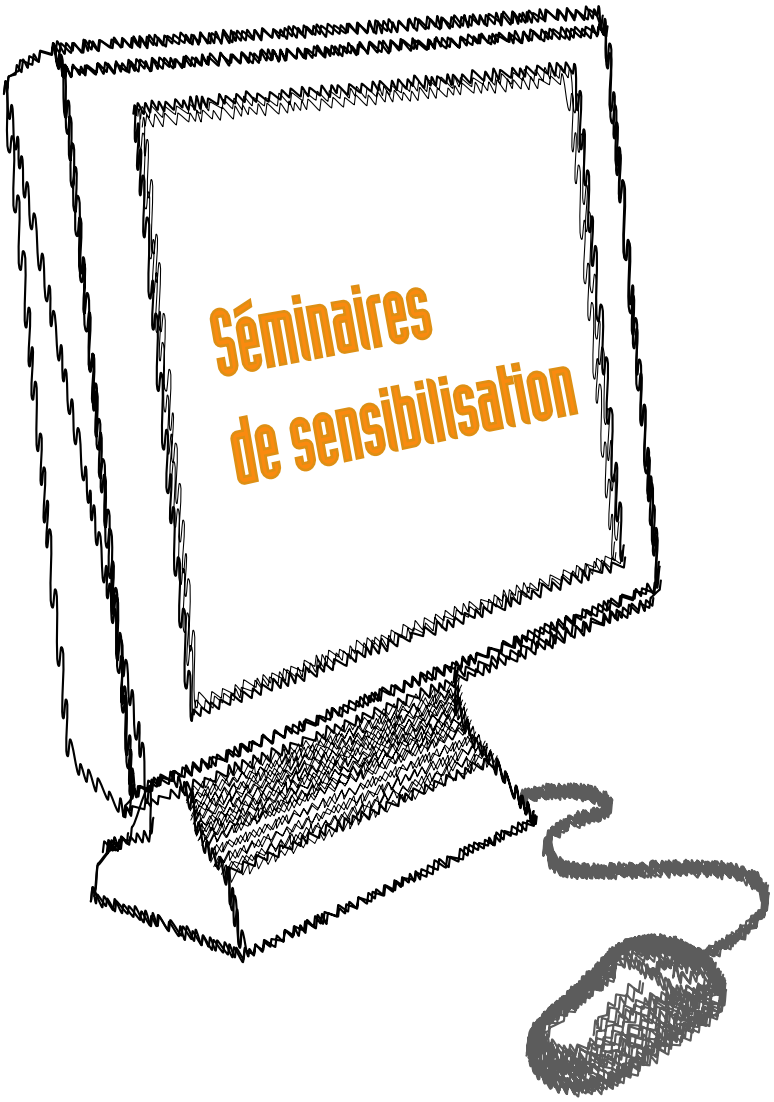
académie Roven

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Informatique : usages et sécurité



Mars/mai 2006

Sommaire

Les points clés de la sécurité : fiches pratiques

Aspects juridiques : fiches juridiques

Quizz sécurité en EPLE

Ont participé à la rédaction de ce document :
la cellule web - la DAJEC - la Divinfo - la Mission TICE du Rectorat de Rouen.
Nos remerciements à l'académie d'Aix-Marseille qui nous a aimablement autorisés à nous inspirer de son document (http://oasi.ac-aix-marseille.fr/).
Mars/mai 2006

La sécurité informatique de l'établissement

Fiche 1

Pourquoi une politique de sécurité en établissement ?

Présentation

L'informatique dans les établissements a considérablement évolué, par les technologies utilisées, les équipements, et les usages. Ces évolutions ont considérablement augmenté les risques qui y sont associés. Le système informatique de l'établissement contribue à son fonctionnement. La sûreté de celui-ci devient donc un impératif. Une politique de sécurité est un ensemble de règles qui régit le traitement de l'information et l'usage des ressources informatiques de l'établissement afin de garantir la sûreté du système d'information.

Les enjeux

L'intérêt repose sur le fait de disposer d'une base de référence pour les règles ou les pratiques de traitement de l'information et de l'usage des ressources informatiques. De la même façon que l'établissement est régi par un ensemble de règles ou procédures (gestion des personnels, gestion du planning), le système d'information doit être régi par un ensemble de règles qui en garantisse la sûreté.

Recommandations

La politique de sécurité se traduit concrètement par le plan sécurité. Ce dernier constitue un référentiel des règles applicables à l'établissement. Les principes généraux sont définis au niveau académique, ils peuvent être précisés en établissement selon les réalités de celui-ci.
Le référentiel comporte les éléments suivants :

- L'organisation mise en place pour la Sécurité des Systèmes d'Information au sein de l'établissement. Elle définit en particulier la chaîne d'alerte ;
- La sécurité physique ;
- La sécurité logique ;
- Le plan de secours.

Liens

Site académique : http://www.ac-rouen.fr, entrée Les Etablissements, rubrique Informatique: Usages et Sécurité.

En pratique

Pour la sensibilisation des personnels :

- Les notes sécurité émises par l'Académie doivent être consignées et portées à la connaissance des intéressés.
- Il est nécessaire de mettre en place une charte d'usage de l'internet et des équipements informatiques, annexée au réglement intérieur.
- Il est conseillé de consulter régulièrement le site de l'académie : http://www.ac-rouen.fr, entrée Les Etablissements, rubrique Informatique: Usages et Sécurité.
- Le dispositif chaîne d'alerte doit être opérationnel dans l'établissement.

Pour la sécurité logique :

- Les mots de passe doivent être gérés conformément aux préconisations académiques. Un mot de passe doit contenir au minimum huit caractères et doit à la fois contenir des lettres et des chiffres (ou des caractères spéciaux).
- L'ouverture d'accès sur les serveurs de sécurité AMON et SLIS de l'établissement doit faire l'objet d'une demande au Rectorat.
- Les mises à jour logicielles préconisées par l'Académie doivent être appliquées.

Pour la sécurité physique, vous devez vérifier que :

- Les accès physiques aux salles d'ordinateurs et au local informatique sont contrôlés.
- Les équipements informatiques les plus sensibles sont protégés d'un point de vue électrique.
- L'architecture réseau de l'EPLE est conforme aux recommandations académiques.

Pour le plan de secours :

- Les sauvegardes de vos données essentielles doivent être effectives.

Les risques liées aux nouvelles technologies

Fiche 2

Comment responsabiliser la communauté éducative ?

Présentation

Une politique de sécurité repose tout à la fois sur des procédures techniques, une organisation et l'implication de tous. Elle repose également sur une prise en compte de sa dimension par les personnels et élèves eux-mêmes.

Comprendre le risque informatique, c'est déjà le maîtriser. Face à l'accroissement du risque, le schéma directeur de la sécurité des systèmes d'information s'oriente aujourd'hui vers le concept de défense en profondeur.

Les enjeux

La lutte contre la criminalité informatique a longtemps été considérée comme une affaire de techniciens. La mise en œuvre de mécanismes de défense appropriés, aptes à lutter contre les attaques informatiques, a longtemps tenu lieu de seule politique de sécurité, la confinant ainsi dans un domaine d'expertise de seuls techniciens.

Face à l'évolution des risques, par leur nature et leur ampleur, une telle politique « techniciste » s'avère insuffisante aujourd'hui. L'idée de concept de défense en profondeur est une approche globale et dynamique qui vise à coordonner plusieurs lignes de défense couvrant l'ensemble du système d'information. Elle implique l'ensemble des acteurs de la communauté éducative, elle vise à une gestion des risques, une remontée d'information, une planification des réactions et l'enrichissement permanent grâce au retour d'expérience.

Les recommandations

La sécurité est le plus souvent vécue comme une contrainte or à l'instar d'un feu rouge, d'un stop qui assure la sécurité sur le réseau routier, les règles et mécanismes de sécurité pour les systèmes d'information concourent à des usages sûrs et maîtrisés de l'informatique et des nouvelles technologies.

L'implication des chefs d'établissements, dans une approche pédagogique, tend à informer la communauté éducative sur la sécurité, ses enjeux et à obtenir son adhésion.

Afin d'atteindre ces objectifs, nous recommandons comme un bon point de départ :

- la mise en place des chartes utilisateurs (élèves, personnels).
- la diffusion des notes ou procédures de sécurité.

Pour en savoir plus

Le site de l'académie : http://www.ac-rouen.fr, entrée Les Etablissements, rubrique Informatique: Usages et Sécurité.

En pratique

En préalable :

► la sécurité et les notes de procédures sont là pour protéger les élèves et personnels.
► il est nécessaire d'associer les personnels à la démarche sécurité.
► la responsabilité des personnels de l'Éducation Nationale peut être engagée.
► les chartes utilisateurs (élèves, personnels) doivent avoir été adoptées.

En pratique :

► les notes de sécurité académiques doivent être portées à la connaissance des personnels et consignées si possible dans un document unique.
► un bilan de la sécurité informatique peut-être fait annuellement lors du conseil d'administration de l'établissement. Celui-ci inclura, par exemple, les incidents, les notes de procédures diffusées, leur application au sein de l'établissement, les actions pédagogiques auprès des élèves, etc.

Le piratage

Fiche 3

Que faire en cas d'incident de sécurité ?

Présentation

On considère qu'il y a intrusion sur un système d'information lorsqu'une personne réussit à obtenir un accès non autorisé sur ce système. Ceci peut permettre au pirate de récupérer des données confidentielles, de les modifier ou encore d'utiliser la machine pour perpétrer des actions délictueuses.

Les enjeux

En cas d'intrusion, une gestion correcte de l'incident, définie préalablement, est nécessaire. Les effets néfastes d'une intrusion sur un système d'information découlent directement une mauvaise réaction après la découverte de l'intrusion, ou peuvent en être amplifiés. Les actions entreprises doivent être conformes à la politique de sécurité et aux procédures définies. Sur le point plus particulier de l'analyse de l'intrusion, il est préférable de confier cette analyse à des professionnels expérimentés qui en connaissent les aspects techniques et juridiques.
Aussi faut-il contacter le Rectorat au plus vite en cas de suspicion d'intrusion et ne rien tenter par soi-même car on risque d'effacer les traces qu'a pu laisser le pirate.

Les recommandations

Nos recommandations s'inspirent de celles préconisées par le Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA).

En préalable :

- L'analyse technique d'une intrusion doit être laissée à des personnels compétents ;
- De mauvaises réactions face à une intrusion peuvent avoir comme conséquence d'en amplifier les effets néfastes ;

Qu'est-ce qui peut trahir une intrusion ?

- Activité importante sur le réseau ou sur une machine, impossibilité de connexion à celle-ci ;
- Présence de logiciels référencés comme des chevaux de Troie par l'anti-virus (Trojan).
- Fichiers créés (en particulier fichiers mp3 ou divx), altérés, modifiés, disparus.
- Ouverture de services non autorisés.
- Altération, création ou destruction de comptes.

D'où peut venir l'intrusion ?

- Un logiciel permettant une prise de contrôle à distance par un pirate a pu être installé à l'insu des utilisateurs. Cela peut arriver si les mises à jour de sécurité ne sont pas passées, ou si des logiciels suspects ont été exécutés sur le poste (en particulier logiciels de «crack»).
- La malveillance ou la négligence peuvent aussi être internes, provenant d'un membre de la communauté éducative.

Pour en savoir plus

- Le site du CERTA : http://www.certa.ssi.gouv.fr
- Le site académique : http://www.ac-rouen.fr, entrée Les Etablissements, rubrique Informatique: Usages et Sécurité.

En pratique

Actions à réaliser immédiatement:

▶ Déconnecter la machine du réseau sans l'éteindre.
▶ Informer le chef d'établissement qui activera la chaîne d'alerte.

Dans un second temps:

▶ Prévenez les RSSI du Rectorat de Rouen (mèl: rssi@ac-rouen.fr) qui sont à même d'intervenir pour analyser l'intrusion.
▶ Porter plainte, en particulier si des tiers ont subi des dommages. C'est le chef d'établissement, personne juridiquement responsable, qui doit le faire.

Mineurs et Internet

Fiche 4

Quelle protection pour les mineurs ?

Présentation

L'internet donne accès à une masse impressionnante d'informations, source documentaire incomparable qui permet à chacun d'enrichir ses connaissances. Hélas, le meilleur y côtoie parfois le pire. Lors de nos balades sur le web, il n'est pas rare de rencontrer des pages, des images statiques ou animées, des messages qui nous choquent, ou nous agressent, et dont nous aimerions protéger notre famille, nos élèves si nous sommes enseignants.
Au-delà de ces contenus, l'Internet recèle des pièges pour les élèves.

Les enjeux

L'atteinte à l'intégrité des mineurs est sans conteste un risque majeur dans l'Education nationale. La protection de ceux-ci, dans le cadre des usages de l'Internet, est donc une priorité absolue. Elle a fait l'objet d'une circulaire, la « circulaire Darcos » (BO N° 9 du 26 février 2004), qui reste la référence dans ce domaine.
Afin de protéger nos élèves de sites illicites ou pornographiques, l'Education nationale déploie dans les établissements des mécanismes de filtrage. Les fournisseurs d'accès privés se voient imposer les mêmes obligations à compter du 1er trimestre 2006.

Les recommandations

- Une charte d'usage de l'Internet doit avoir été adoptée dans votre établissement, et annexée au règlement intérieur;
- Le Brevet Informatique et Internet, obligatoire dans les écoles et collèges, et bientôt dans les lycées, comporte un apprentissage des règles de bonne conduite sur Internet. Le Brevet atteste que l'élève utilise de manière autonome et raisonnée les TIC, pour lire et produire des documents, rechercher des informations et communiquer au moyen d'une messagerie. Le B2i sera intégré au brevet des collèges à l'horizon 2007.
- Le mécanisme de filtrage repose sur des listes noires qui sont régulièrement mises à jour grâce à une collaboration au niveau national. La détection de sites illicites ou inadaptés (pornographiques...), repose sur la vigilance de chacun. A cet égard, l'implication des équipes pédagogiques, de la direction de l'établissement, des élèves est nécessaire quand des sites illicites et non filtrés sont détectés. Dans un esprit de protection active, vous devez mettre en œuvre dans votre établissement le premier niveau de la chaîne d'alerte (voir la fiche «qu'est-ce que la chaîne d'alerte ?») ;
- Mais l'efficacité de ces listes noires ne pourra jamais être totalement garantie. Elle doit être complétée par une utilisation responsable de l'Internet.

Pour en savoir plus

La circulaire parue au Bulletin Officiel de l'Éducation Nationale du 18 février 2004, présente un plan global pour la sécurité des mineurs sur l'Internet dans le cadre pédagogique. L'Éducation nationale encourage aussi l'écriture de «Chartes de bons usages» inspirées de la nétiquette.
Circulaire n°2004-035 du 18-2-2004 : «Usage de l'internet dans le cadre pédagogique et protection des mineurs». Rubrique «Protection de l'accès Internet pour l'éducation» du site Educnet.

En pratique

En règle générale :

▶ Une charte d'usage de l'internet et des moyens informatique doit être annexée au règlement intérieur. Vous trouverez toutes les informations utiles à ce sujet sur le site académique (http://www.ac-rouen.fr/tice/Chartes-d-usage) ;

▶ La mise en place du B2i doit être systématique : il est un élément essentiel d'une politique de protection des mineurs.

▶ Vis à vis des sites illicites, la protection est assurée par des dispositifs de filtrage, reposant sur des moyens techniques et sur des moyens humains.

Moyens techniques :

▶ Le dispositif de filtrage est constitué par un logiciel actif sur votre passerelle AMON, et éventuellement le serveur SLIS. Ce logiciel interdit l'accès à certaines pages web jugées illicites ou inadaptées dans un cadre pédagogique. C'est un contrôle à priori. En complément, l'ensemble des consultations réalisées dans l'académie sont analysées à postériori par un système expert qui identifie de nouvelles pages ou documents à filtrer.
Si vous êtes équipés d'un serveur SLIS, l'ajout de sites à interdire peut être fait immédiatement, au niveau de l'établissement.

Moyens humains :

▶ La détection de sites illicites ou inadaptés (pornographiques,...), repose également sur la vigilance de chacun, afin de réactualiser constamment la liste noire. Le signalement doit se faire en activant la chaîne d'alerte.

▶ Vous pouvez signaler des sites incorrectement filtrés sur http://listesnoires.ac-rouen.fr ,et saisir la chaîne d'alerte à l'adresse netalert@ac-rouen.fr .

▶ Les sites à caractère pédophile doivent obligatoirement être signalés sur le site https://www.internet-mineurs.gouv.fr/signale/contacts

Sécurité du poste de travail

Fiche 5

Comment assurer la confidentialité du poste de travail ?

Présentation

Le poste de travail concourt à des fonctions vitales ou manipule des données essentielles du système d'information. Il est utilisé tout à la fois pour échanger, stocker de l'information et pour accéder à des applications sensibles.
En conséquence, la sécurité du poste de travail représente un enjeu essentiel.

Les enjeux

La sécurité du poste de travail constitue un des éléments essentiels de la sécurité dans l'idée de la défense en profondeur. Si les mécanismes opérationnels sur les réseaux, serveurs ou systèmes logiciels constituent la première ligne technique de défense, il est dangereux de considérer que son poste de travail est protégé parce que situé derrière ceux-ci. La nature même des données manipulées sur le poste de travail nécessite de le prendre en considération dans la politique de sécurité.

Les recommandations

► Général

- Ne quittez jamais votre écran lorsque vous effectuez une opération sensible ; si vous y êtes obligé avant de terminer, verrouillez-le.
- Fermez toujours correctement les applications utilisées lorsque vous quittez définitivement votre poste de travail, en particulier le navigateur.
- Installez un antivirus, un logiciel anti-spywares (veillez à leur mise à jour régulière) et laissez activé le pare-feu de votre station (situation par défaut des ordinateurs équipés de Windows XP SP2).
- Activez la mise à jour automatique du poste de travail (Windows Update sous Windows).
- Ne téléchargez pas des «cracks» de logiciels et ne visitez pas des sites mettant à disposition des logiciels pirates.
- L'utilisation de Windows XP en version SP2 est recommandée en particulier pour les postes sensibles.

► Mots de passe

- Ne divulguez jamais votre mot de passe, ni toute autre information sur votre compte à un utilisateur quel qu'il soit ; ne laissez jamais ces informations en vue, ni collées sous le clavier.
- Evitez d'utiliser un mot de passe simpliste: un bon mot de passe est composé d'au moins huit caractères et doit contenir des lettres ainsi que des chiffres ou des caractères spéciaux. Ne pas construire son mot de passe à partir d'un mot pouvant être trouvé dans un dictionnaire;
- Ne pas utiliser le même mot de passe pour plusieurs applications. Notamment, n'utilisez jamais un mot de passe à la fois pour des applications académiques et des applications extérieures (en particulier pour des sites web n'appartenant pas à l'Education nationale).

► Messagerie

- N'envoyez jamais d'informations confidentielles par courrier électronique.
- N'envoyez pas de fichiers exécutables par courrier électronique et n'ouvrez pas ceux que vous recevez.

► Poste en libre accès

- L'utilisation d'un logiciel de régénération automatique (type Deep Freeze) est recommandée.
- L'utilisation du navigateur Firefox (dans sa dernière version disponible) est recommandée. Il doit être configuré pour ne pas sauvegarder les formulaires, l'historique, les mots de passe, et pour effacer les cookies dès que le navigateur est fermé.

En pratique

Pour ce qui concerne la gestion des mots de passe :

► Les recommandations sur les mots de passe doivent être appliquées ;

► La mise en oeuvre d'un mot de passe pour bloquer l'accès à votre poste de travail est recommandée .

En ce qui concerne l'anti-virus :

► L'antivirus académique doit être utilisé pour protéger TOUS les postes de travail de l'établissement. Vous devez veiller à ce qu'il soit régulièrement mis à jour. Pour plus de détail, voir la fiche 8, «Les virus, comment se protéger efficacement»

► Ne restez pas sur des doutes ou des interrogations ; n'hésitez jamais à vous renseigner auprès du dispositif d'assistance académique.

Protection des mineurs

Fiche 6

Qu'est-ce que la chaîne d'alerte ?

Présentation

La circulaire n° 2004-035 du 18 février 2004 parue au Bulletin officiel de l'Éducation nationale du 26 février 2004, précise la mise en place d'une chaîne d'information qui doit être utilisée en cas d'incidents liés à l'usage des technologies de l'information et de la communication dans le cadre pédagogique.

La chaîne a essentiellement pour vocation de signaler dans les meilleurs délais des sites illégitimes ou illicites afin qu'ils soient référencés comme tels sur les listes noires de l'éducation Nationale. In fine, l'objectif est bien de protéger les élèves mineurs.

Les enjeux

Cette circulaire a été conçue dans une perspective de protection des mineurs. Elle vise à renforcer les dispositifs humains et techniques mis en œuvre pour garantir une utilisation sûre d'Internet. La mise en œuvre de cette chaîne d'alerte est un enjeu essentiel pour l'éducation Nationale.

Les recommandations

La chaîne d'information est définie et constituée comme suit :

- au sein de chaque établissement ou école, les membres de l'équipe pédagogique informent le chef d'établissement ou le directeur d'école des incidents constatés ;
- la cellule académique constituée autour du Conseiller TICE, avec l'appui du RSSI, est informée des incidents se produisant dans les établissements et écoles par les chefs d'établissement ou les directeurs d'école ;
- en cas de besoin, cette cellule académique informe la cellule nationale de coordination par l'intermédiaire des dispositifs d'assistance mis à disposition (interface web et courrier électronique). Au besoin, le haut fonctionnaire de défense du ministère est informé.

Elle doit être activée dans les situations suivantes :

- découverte d'un site Internet inapproprié dans le cadre pédagogique, et non bloqué ;
- découverte d'un site Internet approprié dans le cadre pédagogique et injustement bloqué ;
- demande de la part des médias d'explication en cas d'incident ;
- demande de blocage par des parents ou associations ;
- découverte d'un site Internet illégal au regard de la loi française ;
- réception par un élève d'un message à caractère « douteux ».

Par extension, vous pouvez saisir la chaîne d'alerte au niveau académique pour tout incident de sécurité.

Pour en savoir plus

Le site national : http://tice.education.fr/educnet/Public/services/securite/guide_securite?affdoc=1

En pratique

La chaîne d'alerte est organisée sur trois niveaux :

- l'établissement, les services académiques et le niveau national. La définition de chacun de ces niveaux et le rôle qu'ils jouent dans la chaîne d'alerte sont définis par la circulaire n° 2004-035 du 18 février 2004. Cette circulaire doit être portée à la connaissance des personnels. Elle est disponible sur le site du Bulletin Officiel (BO N° 9 du 26 février 2004) ;
- la cellule académique est constituée par l'équipe dirigée par le Conseiller TICE auprès du Recteur, appuyé par le RSSI
- la chaîne d'alerte peut être effectivement saisie par internet en complétant le formulaire disponible à l'adresse : http://listesnoires.ac-rouen.fr ou par courrier électronique à l'adresse : netalert@ac-rouen.fr .

Le spam

Fiche 7

Comment lutter à son niveau contre le spam ?

Présentation

Le spam est un message électronique non sollicité envoyé en masse. Autrement appelé pourriel, il pollue aussi bien la messagerie que les forums ou les chats. Des mécanismes sont mis en oeuvre au Rectorat, pour lutter de manière centrale contre le spam.

Pour information, nous bloquons environs 30 000 spams quotidiennement sur nos serveurs de messagerie, et c'est un chiffre en constante augmentation.

Les enjeux

La pratique du spam continue à évoluer rapidement. Le spam a une incidence négative croissante sur la sécurité des systèmes d'information.

La lutte contre le spam implique l'ensemble des acteurs de la communauté éducative, des utilisateurs à la hiérarchie, en passant par les équipes techniques.

Les recommandations

- Il ne faut jamais avoir une confiance absolue dans l'expéditeur du courrier, ceci est très facilement falsifiable.
- Un premier niveau de protection anti-spam est assuré au niveau de la messagerie académique. Bien qu'efficace, il ne peut offrir une prévention absolue.
- Si vous recevez un spam à contenu illégal (négationnisme, pédophilie...) contactez immédiatement la chaîne d'alerte (cf Fiche «La chaîne d'alerte»)

En pratique

► Ne répondez jamais à un spam.

► Ne cliquez sur les liens de désabonnement à la «mailing list» de l'expéditeur que si vous êtes sûr qu'il permet un réel désabonnement (renseignez-vous sur le sérieux de la société expéditrice du courriel).

► Plus généralement, ne cliquez jamais sur les liens hypertextes insérés dans le corps du spam.

► Utilisez de préférence des logiciels de messagerie permettant de filtrer les messages (type Thunderbird).

► N'ouvrez jamais un fichier joint à un spam : ce pourrait être un virus ou un spyware.

► Ne diffusez jamais à des tiers des adresses de messagerie autres que la vôtre sans le consentement des intéressés.

► Si vous recevez de manière répétée des spams venant d'une même société, transférez ces messages à reseaux@ac-rouen.fr.

Les virus

Fiche 8

Comment se protéger efficacement ?

Présentation

Un virus est un petit programme qui, lorsqu'on l'exécute, se charge en mémoire et exécute à l'insu de l'utilisateur les instructions que son auteur a programmées. Les résultats de l'exécution peuvent être très divers tels que l'envoi de données confidentielles au pirate (mots de passe, numéro de carte bleue...), l'effacement de fichiers ... Qui plus est, la présence d'un virus est généralement indétectable pour l'utilisateur.
Ils possèdent en outre la faculté de créer des répliques d'eux-mêmes au sein d'autres ordinateurs du réseau, ou via la messagerie.

Les enjeux

Les virus informatiques représentent aujourd'hui la forme de criminalité informatique la plus développée. La nature même des risques qu'ils font courir et leurs conséquences nécessitent une lutte à tous les niveaux.

Le principal vecteur de diffusion étant la messagerie électronique, celle-ci doit faire l'objet d'une attention particulière. Cela se traduit par des mécanismes et une organisation adéquate de la messagerie académique, cela implique aussi des mesures et bons gestes côté utilisateur.

Un nouveau vecteur émergent est la contamination par programmes téléchargés sur Internet, en particulier sur les sites pirates («crack» de logiciels en particulier) et sur les sites de téléchargement de sharewares. Là aussi la réponse la plus efficace est un comportement responsable de la part des utilisateurs (ne pas utiliser de logiciels piratés, ne pas installer de logiciels dont l'éditeur n'est pas connu ...)

Les recommandations

Nous recommandons, pour se protéger des virus :

- d'avoir un anti-virus à jour. Un antivirus est diffusé chaque année par la Mission TICE sous forme de cédéroms envoyés aux établissements.
- la prudence la plus extrême lorsque vous recevez des pièces jointes, même s'il s'agit d'un utilisateur connu car l'adresse de l'expéditeur est falsifiable.
- de contrôler toutes les nouvelles applications à installer.

En pratique

► Installer l'antivirus sur l'ensemble des postes de l'établissement.
► Veiller à ce que son paramétrage soit correct, et assure sa mise à jour régulière.

► Etre prudent lorsque vous recevez des pièces jointes (en particulier des .exe) : en cas de doute, contacter l'expéditeur.

► N'installer aucun logiciel pirate, shareware, freeware inconnu sur une machine sensible.

► En cas de doute sur l'état d'une machine, contacter la plate-forme d'assistance au 02 32 08 88 88.

Lois et internet

Fiche 9

Que doit-on savoir ?

Présentation

L'observation des règles commence par le respect des lois que nul n'est censé ignorer. Tout utilisateur de l'établissement est tenu de respecter la législation en vigueur. Par exemple si, dans l'accomplissement de son travail, un utilisateur est amené à constituer des « fichiers nominatifs » relevant de la loi « Informatique et Libertés », il devra auparavant faire une demande d'autorisation auprès de la CNIL, sous couvert du chef d'établissement.

Les enjeux

Les lois et les règles, mêmes si elles peuvent par moment nous paraître contraignantes, sont faites pour nous protéger. Le respect de celles-ci trouve son fondement ici.

De plus, le non-respect peut entraîner des poursuites civiles ou pénales de leurs auteurs. Leur connaissance revêt donc ce double enjeu.

Les recommandations

D'une façon générale, les textes des lois qui traitent de la sécurité informatique sont disponibles sur Internet :

- la loi du 6/1/78 dite « informatique et libertés » (http://www.cnil.fr/) ;
- la loi du 5/1/88 relative à la fraude informatique, complétée par la loi du 22/7/92 dite « loi Godfrain» (http://www.legifrance.gouv.fr/citoyen/code.cgi) ;
- la législation relative à la propriété intellectuelle (http://www.legifrance.gouv.fr/citoyen/code.cgi) ;
- la législation applicable en matière de cryptologie (http://www.ssi.gouv.fr/)
- la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

En pratique

En matière de lois et d'Internet, vous devez être particulièrement attentifs :

► aux téléchargements effectués depuis Internet. En plus des virus, vers et autres logiciels espions qu'ils peuvent receler, vous risquez de contrevenir au droit de la propriété intellectuelle.

► à l'introduction de toute application informatique qui manipulerait des données nominatives. Vous risquez de tomber sous le coup de la loi informatique et libertés.

► à un usage des ressources informatiques de votre établissement non conforme aux missions de l'Éducation Nationale. Vous risqueriez de tomber sous le coup de la loi Godfrain en particulier.

Sur ces sujets, pour toute question d'ordre juridique, vous devez nous contacter à l'adresse suivante : dajec@ac-rouen.fr

Les pratiques à risques

Fiche 10

Que doit-on surveiller ?

Présentation

L'évolution rapide des réseaux et des usages donne le sentiment d'un foisonnement difficilement contrôlable. Au-delà des pratiques illégales, certaines peuvent s'avérer risquées. S'il est illusoire de vouloir tout contrôler, certaines pratiques à risques doivent être jugulées.

Les enjeux

Les pratiques à risques peuvent causer des dégats pour l'établissement ou des tiers. Elles peuvent également, sans qu'elles aient pour conséquences des dommages, entraîner des poursuites civiles ou pénales contre l'établissement. Elles peuvent aussi porter atteinte à l'intégrité de mineurs par la consultation de sites illicites.

Elles peuvent aussi conduire à faciliter des malveillances internes (vol de devoirs sur le réseau, tentative de modification de notes par les élèves...). Cela justifie la mise en place de bonnes pratiques et d'un contrôle qui peut s'exercer à la fois à priori et à postériori.

Les recommandations

► **D'une façon générale,**
nous vous recommandons :

- d'interdire le trafic «peer to peer» ;
- de ne pas autoriser «le chat» ;
- de contrôler la connexion d'ordinateurs extérieurs à l'établissement ;
- ne pas télécharger, ni exécuter des programmes inconnus sur les postes ;
- ne pas utiliser le poste de travail avec les droits administrateurs ;

► **Les solutions de type wifi**
Elles sont très complexes à déployer de manière sécurisée. Déployer du wifi sans prendre en compte la sécurité est s'exposer à de très gros problèmes de sécurité.

► **Le contrôle**
La mise en oeuvre de ces recommandations s'associe à des contrôles que vous pouvez effectuer sur le système d'information de votre établissement. Les traces enregistrées sur les passerelles AMON et SLIS sont conservées pour réaliser une analyse éventuelle de trafics illicites.

En pratique

Concernant les accès à Internet :
► Le raccordement d'un ordinateur « étranger » à l'établissement doit faire l'objet d'une autorisation préalable du chef d'établissement. Un tel raccordement est réalisé avec un objectif précis et pour une durée limitée ;
► Demander conseil à la division informatique avant tout déploiement d'une solution à base de Wifi. Les points d'accès wifi doivent faire l'objet d'une attention toute particulière tant au niveau de la configuration que des journaux de connexion.

Ouverture de services hébergés
► Les demandes d'ouvertures de services sur la passerelle AMON/SLIS ne doivent pas être traitées à la légère. Elles doivent faire l'objet d'une discussion préalable au sein de l'établissement et d'une demande de conseil auprès du Rectorat.

En cas de suspicion de trafic anormal :
► Les RSSI du Rectorat doivent être saisis (rssi@ac-rouen.fr).

Les aspects juridiques

Fiche FJ01

Les Blogs [1]

Qu'est-ce qu'un blog ?

Le terme « blog » est une abréviation de « weblog » qui signifie journal sur internet. Bien souvent, il s'agit d'une sorte de journal intime publié sur l'internet. On peut y trouver des textes, des photos, des vidéos... Sur chaque article du blog il y a la possibilité, pour les visiteurs du site, de laisser des commentaires qui peuvent être immédiatement publiés.
On peut créer un blog de manière très simple, sans aucune connaissance particulière, en utilisant les services de sites de blogs. Il en existe de nombreux, mais le plus utilisé par les jeunes est http://www.skyblog.com/

Les blogs : on a le droit ou pas ?

Bien sûr que les blogs sont autorisés !
Ils sont même recommandés : pour dialoguer avec ses copains, pour échanger des idées ou des informations, pour parler de ce (et de ceux) qu'on aime.
De nombreux sites pédagogiques utilisent ce nouveau média pour produire et diffuser des documents avec leurs élèves.
Cependant les blogs sont aussi très souvent utilisés en toute ignorance des lois et règlements.
Révéler sur un blog trop d'informations sur soi et ses habitudes peut être dangereux pour les mineurs. Par ailleurs, les mineurs peuvent être exposés à des contenus violents ou pornographiques présents sur certains blogs.

Comment fonctionne un blog ?

Exemple à partir de Skyblog

► La création d'un blog

Pour créer un blog sur le site de Skyblog, il suffit de créer un compte, avec des informations sur l'identité du propriétaire du blog. Mais la seule information vérifiable est l'adresse électronique, et de nombreux sites permettent de créer des adresses électroniques sans aucune vérification et donc de manière anonyme. Ainsi, en 10 minutes, on peut créer une adresse électronique avec des informations fictives et, avec cette adresse, créer un blog dans un total anonymat.

► La gestion d'un blog

Pour alimenter un blog sur le site de Skyblog, on crée des articles. Chaque article peut contenir du texte et une image. L'article est créé à partir d'un formulaire web et, une fois validé, il est instantanément publié.
A posteriori, le propriétaire du blog peut supprimer les commentaires qui ont été déposés.
Lorsqu'on dépose un commentaire sur le blog, un message prévient qu'une trace est gardée sur l'origine du commentaire : «N'oublie pas que les propos injurieux, racistes, etc. sont interdits par les conditions d'utilisation de Skyblog et que tu peux être identifié(e) par ton adresse internet (190.182.253.10 X:162.30.25.100, R:192.168.11.208) si quelqu'un porte plainte».

Comment trouver des blogs?

On peut effectuer une recherche avec un moteur de recherche (comme Google) en saisissant des mots-clés (par exemple : « blog » « nom-du-lycee », « prof », « ville », « nom-d'un-professeur »…) et en effectuant diverses combinaisons de ces mots-clés.
On peut aussi effectuer des recherches à l'intérieur des sites de blogs. Dans Skyblog, par exemple, on peut saisir les mêmes mots-clés.
La recherche de blogs est très difficile et le fait de ne pas en trouver ne signifie pas qu'il n'y en a pas. Lorsqu'on a trouvé un blog sur l'établissement, il peut être intéressant de regarder la rubrique « Mes skyblogs préférés » (toujours dans le cas exemple du site Skyblog). S'il y a d'autres blogs sur l'établissement, il est fort possible qu'ils y soient indiqués.
La consultation des statistiques du serveur de communication AMON/SLIS peut aussi être très utile, en effet, le site Skyblog est sur la liste noire des sites (sites interdits).

Comment identifier le propriétaire d'un blog ?

Le propriétaire d'un blog n'est pas facile à déterminer car il apparaît à travers un pseudonyme. Cependant, la plupart du temps, les propriétaires ne se cachent pas et en parcourant le site on découvre des éléments qui permettent de l'identifier (prénom, photos, classe…).

Les aspects juridiques

Fiche FJ01

Les Blogs [2]

En pratique

Comment réagir lorsqu'on découvre un blog problématique ?

► **Conserver une trace du blog**

● Pour garder une trace de l'ensemble du blog et des éléments problématiques qu'il contient, il faut capturer le site. N'importe quel aspirateur de (../..) (../..) site fera l'affaire (par exemple HTTrack, qui est téléchargeable gratuitement : http://www.httrack.com/).

● S'il y a seulement une page du blog qui pose problème, il est possible d'enregistrer la page à partir du navigateur. Dans ce cas, il faut veiller à bien enregistrer la page complète (avec les fichiers associés, comme les images). Attention, la capture d'une page ne permet pas de capturer les commentaires.

► **Effectuer les démarches pour faire cesser le problème**

Plusieurs types d'actions sont possibles :

● contact du propriétaire du blog. Sur chaque blog il y a une adresse de courriel qui permet de contacter le propriétaire du blog.

● contact de l'hébergeur du blog (Skyblog, dans les exemples précédents). Un message peut être envoyé au contact indiqué sur le site hébergeur pour lui signaler les problèmes constatés et, éventuellement, lui demander de fermer le blog.

● plainte déposée au commissariat.

► si le propriétaire du blog est un élève de l'établissement identifié, il est naturellement possible de le convoquer avec ses parents.

Quelles suites donner lorsque le propriétaire du blog est un élève ?

Si le propriétaire du blog problématique est un élève, on peut envisager diverses suites selon la gravité des faits, sous réserve que ces mesures soient prévues dans le règlement intérieur afin de sanctionner ces comportements :

- l'avertissement
- l'exclusion temporaire
- le conseil de discipline (exclusion définitive)

Il peut-être envisageable, pour le premier cas qui se présente, de réunir une représentation de la communauté éducative (commission permanente, comité de pilotage des TICE, représentants du CVL…) afin de débattre du problème de manière assez large avant de prendre les décisions.

Dans tous les cas, une plainte peut être déposée, en parallèle, par le chef d'établissement et/ou la victime (élève, professeur …). La plainte débouchera sur des sanctions pénales qui seront différentes selon la nature de l'infraction poursuivie.

► La plainte est le seul recours possible si le propriétaire du blog problématique n'est pas un élève de l'établissement.

Quelles suites donner lorsque le propriétaire du blog problématique est un personnel de l'Etat ?

- Informer l'autorité académique en vue, si nécessaire, d'une procédure disciplinaire
- Dépôt de plainte éventuel par le chef d'établissement ou par le ou les personnes visées dans le blog
- S'il s'agit d'un personnel contractuel de droit privé, la sanction est prise par le chef d'établissement. Le dépôt de plainte est également envisageable.

Quelles sont les bases légales des sanctions et les peines encourues?

Voir tableau synoptique en fiche FJ03

Comment prévenir ?

Il est souhaitable que des actions d'information soient mises en place pour prévenir les dérapages dans les blogs.

Exemples de mesures :

- Insertion dans le règlement intérieur de l'établissement de la charte utilisateurs (personnels, élèves).
- Réunion d'information des délégués de classe et des représentants au CVL
- Accent mis dans le B2I sur la pratique citoyenne des usages de l'informatique.
- Introduction d'un thème sur les blogs (et plus généralement, sur la publication numérique) en ECJS.
- Mise en place en début d'année de conférences d'information pour les élèves et les parents de l'établissement (par classes ou par groupe de classes).

Les aspects juridiques

Fiche FJ02

Les téléphones portables

L'utilisation des téléphones portables au sein des établissements et des modes de communication électronique appelle plusieurs observations.

Quel usage autorisé?

En premier lieu, il apparaît opportun de souligner dans les règlements intérieurs quel cadre l'EPLE souhaite voir respecté.
L'interdiction de l'usage du téléphone portable par les élèves à l'intérieur des locaux (salles de classe, couloirs, réfectoire…), est parfaitement envisageable. Non respectée, elle pourra amener le chef d'établissement à prononcer une sanction (conforme au principe de proportionnalité) inscrite dans le règlement intérieur.

En revanche, l'interdiction générale et absolue de la possession d'un téléphone portable ne doit pas être retenue.

Recommandations

En second lieu, il apparaît également utile de mentionner dans le règlement intérieur les incidences possibles d'un phénomène susceptible de se développer : la prise de photographies par les élèves, à l'aide de leur téléphone portable, des personnels de l'établissement, images parfois mises en ligne sur internet dans le cadre de blogs. Le code pénal fixe précisément les conditions d'atteinte à l'intimité de la vie privée d'autrui.

Il s'avère par conséquent indispensable d'informer tout propriétaire d'un téléphone portable de ce à quoi il s'expose en cas de dépôt de plainte par une personne s'estimant victime d'une atteinte à sa vie privée.

Quelles sont les bases légales des sanctions et les peines encourues?

- **L'article 226-1 du code pénal** prévoit qu' « est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui:

  En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

  En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.»

- **Par ailleurs, l'article 226-8 du même code** précise qu' « est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention (…)».

Les aspects juridiques

Fiche FJ03

Tableau synoptique des peines

Exemple	Infraction	Textes légaux de référence	Sanction légale
Photos d'élèves ou de professeurs sans autorisation de publication.	Droit à l'image	Article 1382 Code civil Article 1383 Code civil Article 9 du Code civil Article L226-1 Code pénal Article L226-2 Code pénal	1 an de prison 45.000 Euros d'amende
Caricature d'un professeur faite à partir d'une photo publiée sans autorisation.	Représentation des personnes	Article 1382 Code civil Article 1383 Code civil Article L226-8 Code pénal	1 an de prison 15.000 Euros d'amende
Mise en ligne d'images ou de textes trouvés par exemple sur Internet, sans demander l'autorisation, ou de morceaux de musique téléchargés sans paiement de droits.	Droit d'auteur (contrefaçon)	Article 1382 Code civil Article 1383 Code civil Article L335-2 Code la propriété Intellectuelle Article L335-3 Code la propriété Intellectuelle Article L335-4 Code la propriété Intellectuelle	Par une personne 3 ans de prison 300.000 Euros d'amende En bande organisée 5 ans de prison 500.000 Euros d'amende
Mise en ligne du logo (protégé) d'une entreprise trouvé par exemple sur Internet sans demander l'autorisation	Droit des marques (Dessins et modèles) (contrefaçon)	Article 1382 Code civil Article 1383 Code civil Article 716-10 Code la propriété Intellectuelle	3 ans de prison 300.000 Euros d'amende
Commentaires sur un camarade ou un professeur du style « c'est un voleur ».	Diffamation	Article 1382 Code civil Article 1383 Code civil Article 23 loi 29/07/1881 Article 31 loi 29/07/1881 Article 32 loi 29/07/1881	12.000 Euros
Commentaires sur un camarade du style « c'est un sale voleur de (nationalité)» (ou ethnie, religion, race).	Diffamation	Article 1382 Code civil Article 1383 Code civil Article 32 loi 29/07/1881	1 an de prison 45.000 Euros d'amende
Commentaires du style « la prof de (matière) est une g….v….. »	Injure	Article 1382 Code civil Article 1383 Code civil Article 30 loi 29/07/1881 Article 31 loi 29/07/1881 Article 34 loi 29/07/1881	12.000 Euros
Commentaires sur une camarade du style « c'est une p… de (nationalité) » (ou ethnie, religion, race).	Injure	Article 1382 Code civil Article 1383 Code civil Article 30 loi 29/07/1881 Article 31 loi 29/07/1881 Article 34 loi 29/07/1881	6 mois de prison 22.500 Euros d'amende
« N… ta mère ! ».	Message contraire à la décence	Article 1382 Code civil Article 1383 Code civil Article R624-2 Code pénal	750 Euros

Quizz sécurité en EPLE

11 points à vérifier en 22 questions

Lorsque vous n'êtes pas sûr de votre réponse, répondez NON

Etes-vous régulièrement informé de l'état de la sécurité informatique dans votre établissement ?	❒ OUI ❒ NON	Une personne a-t-elle été chargée de s'en tenir informée ?	❒ OUI ❒ NON
Votre système informatique est-il protégé contre les problèmes d'électricité, d'élévation de température, d'inondation et d'incendie ?	❒ OUI ❒ NON	Avez-vous un contrat de maintenance de ces systèmes ?	❒ OUI ❒ NON
L'accès aux locaux informatiques est-il protégé par des fermetures adaptées et une alarme ?	❒ OUI ❒ NON	Savez-vous précisément combien il existe de clés, qui les détient et qui a connaissance du code de l'alarme ?	❒ OUI ❒ NON
Existe-t-il des procédures de sauvegarde automatique des données, tests et restauration de sauvegardes ?	❒ OUI ❒ NON	Les sauvegardes sont-elles régulièrement contrôlées ?	❒ OUI ❒ NON
Existe-t-il des procédures de protection contre les virus ?	❒ OUI ❒ NON	Les mises à jour sont-elles régulièrement contrôlées ?	❒ OUI ❒ NON
Toutes les bases de données utilisées dans votre établissement sont-elles recensées ?	❒ OUI ❒ NON	Centralisez-vous les documents déclaratifs de ces bases à la CNIL ?	❒ OUI ❒ NON
Existe-t-il un document qui précise les règles de sécurité, les droits, les devoirs et les responsabilités des élèves utilisant votre informatique ?	❒ OUI ❒ NON	Est-ce une charte signée par chaque élève ?	❒ OUI ❒ NON
Existe-t-il un document qui précise les règles de sécurité, les droits, les devoirs et les responsabilités des membres du personnel ?	❒ OUI ❒ NON	Cette charte est-elle annexée au règlement intérieur ?	❒ OUI ❒ NON
Chaque utilisateur est-il identifié lorsqu'il utilise votre système informatique ?	❒ OUI ❒ NON	La gestion des comptes et mots de passe garantit-elle leur confidentialité ?	❒ OUI ❒ NON
Existe-t-il un filtrage des accès aux sites sur l'internet ?	❒ OUI ❒ NON	Les mises à jour de liste noire et le suivi des journaux sont-ils réguliers ?	❒ OUI ❒ NON
Le contenu de l'ensemble du site web de l'établissement est-il conforme aux textes en vigueur ?	❒ OUI ❒ NON	Un contrôle régulier du respect du droit à l'image, de la vie privée, de la conformité aux bonnes mœurs est-il effectué ?	❒ OUI ❒ NON

Comptez le nombre de **OUI** cochés

► **plus de 17 :**
Bravo ! Vous avez fait de réels efforts en matière de sécurité. Moins de 22, votre système reste encore exposé. Il faut étudier les quelques points qui restent.

► **de 12 à 16 :**
Vous pouvez faire face à certains problèmes mais votre dispositif est encore trop exposé. Il faut analyser la situation afin de déterminer les améliorations indispensables.

► **de 0 à 11 :**
La sécurité est désastreuse ! Vous êtes à la merci du moindre incident. Pour reprendre le dessus face à ces risques, un travail de fond doit être entrepris !

Académie de Rouen - 1er trimestre 2006