Internet a-t-il rendu nos ados fous ? Peut-on faire tout et n'importe quoi sur le réseau ?

Val Notre Dame – 21 janvier 2015

Madame Simon remercie les nombreux parents présents à la conférence, fait une courte introduction du sujet et présente les deux orateurs : Le Commissaire Bogaert de la Computer Crime Unit et Monsieur Wéry, avocat spécialisé en droit des médias, ainsi que l'équipe de « Devoir d'enquête » (RTBF) qui fait un reportage sur la problématique de l'usage d'internet chez les jeunes.

Mr Bogaert présente le plan de son intervention. Son exposé comporte 3 parties :

- Les mails
- Le surf sur le net
- Les réseaux sociaux

L'activité des jeunes sur le net ne se limite pas qu'à ces 3 aspects, elle se compose aussi de jeux, de Youtube, de la musique, des webcams,… tout ce que permet de faire un smartphone et est issu d'une très importante évolution technologique de ces dernières décennies.

Les Mails

Bien que le mail ne soit pas l'outil le plus utilisé des ados actuellement, il va rapidement le devenir car c'est via ce moyen que les professeurs d'université communiquent avec leurs élèves (que ce soit pour des travaux ou pour l'accès au serveur pour les syllabi) sans parler de l'usage du mail à titre professionnel.

En ce qui concerne les mails, la première sécurité passe par le mot de passe. Il est donc primordial d'avoir un mot de passe sérieux. Mr Bogaert présente la liste des 25 mots de passe les plus courant (parmi lesquels basketball, football, pasword, ..).
Il rappelle que du mot de passe dépend la défense de son ordinateur : un bon hacker craque un mot de passe simple en maximum 8 heures (voire quelques minutes).

Il rappelle les principales règles de sécurité en matière de mot de passe :

1) Combiner lettres minuscules et majuscules avec des chiffres et caractères spéciaux (= , ?) sur une longueur de 8 à 10 caractères minimum.
2) Créer le raccourci d'une phrase que vous retenez facilement mais qui ne veut rien dire afin de rendre le travail des pirates plus difficile (ils utilisent entre autre des logiciels spécialisés couplés à des dictionnaires)
   Ex : la phrase « Mon grand frère Max a 19 ans ! » donne le mot de passe « MgfMa19a! », mot de passe quasi introuvable par des hackers.
3) Ne jamais donner son mot de passe à quelqu'un sous quelque prétexte que ce soit (à l'exception des parents lorsque l'on est mineure…).Un ami, voire un petit copain, peut vite passer du stade du grand amour à pire ennemi et les vengeances informatiques sont légions.

4) Utiliser des mots de passe différenciés pour les différentes applications que l'on utilise, cela renforce la sécurité de votre ordinateur.
   Ex : Créer un mot de passe selon l'exemple 2 et pour chaque application, modifier 1 caractère en début ou fin de mot de passe. Il suffit alors de garder chez soi un index de la modification. Dans le cas de l'exemple repris en 2, on pourrait garder chez soi une liste reprenant les chiffres (sans le reste du mot de passe) qui dirait : 19 = Facebook, 20 = banque, …

Mr Bogaert renseigne le site « Beesecure » mis au point par des collègues luxembourgeois pour tester la résistance d'un mot de passe : https://www.bee-secure.lu/fr/themes/mots-de-passe.

Courriers Indésirables :

Pour s'identifier à tout site ou réseau social, il faut donner une adresse email qui sera couplée à des informations. Facebook, par exemple, va revendre ces informations à des agences marketing pour des campagnes de pub.

Mr Bogaert donne quelques règles de sécurité afin d'éviter les déconvenues sur internet en matière de courriers indésirables :

1) Ne pas diffuser son adresse mail sur internet à tout bout de champs (chaque inscription à quelque chose ou commande)
   Solution : créer une adresse mail « poubelle » pour toutes les commandes, cartes fidélités, sur laquelle on recevra toutes les publicités et garder son adresse mail « secrète ».
2) Ne pas répondre à des emails non sollicités.
3) Ne pas se désinscrire d'un envoi de mails. Ce faisant, on valide l'adresse mail (confirme qu'elle existe bien), elle sera alors récupérée dans des bases de données.
4) Utiliser un service mail avec filtre automatique type gmail dans lequel on peut signaler les mails indésirables afin qu'ils ne parviennent plus dans la boîte de réception mais également qu'ils soient bloqués en amont dans les banques de données « spam ».

Il recommande d'aller visiter le site « Spamsquad.be » qui reprend les sites et mails les plus utilisés par les sociétés marketing afin de pouvoir s'en préserver.

Il attire également l'attention sur les pratiques suivantes :

- Les Mails de « fishing » : qui fonctionne de 2 manières :
  - À l'ouverture d'un mail non sollicité, il lance un petit programme qui va récupérer toutes vos données au cours de vos utilisations ou
  - En vous demandant de vérifier vos identifiants par mail. Aucun site ou banque ne fait ce genre de démarche par mail, et ce, même si le site ressemble à l'original comme 2 gouttes d'eau.

  Truc : vérifier l'adresse IP
- Ne jamais diffuser d'HOAX (mails rumeurs) : il s'agit souvent d'informations fausses, périmées ou invérifiables qui parce qu'elles émeuvent ou scandalisent, sont propagées spontanément par les internautes. Grâce à ce Hoax, des personnes malintentionnées vont récupérer toutes vos données et adresses valides…
  Solution : signaler ces Hoax à l'adresse www.hoaxbuster.com.

Surfer sur internet

Mr Bogaert rappelle les règles élémentaires de sécurité sur internet :

1) Ne pas croire tout ce que vous lisez sur internet
2) Vérifier et recouper l'information
   Il illustre ces 2 premiers points par l'exemple de fausses informations diffusées pendant 3 mois sur Wikipédia avant d'être repérées et corrigées…
3) Attention aux téléchargements de vidéos « attirantes » (ex : regarde cette photo de toi sur Facebook) mais qui redirigent vers des sites qui ne sont plus Facebook et qui masquent des logiciels virus malveillants de type, par ex., « keylogger » (qui enregistre toute l'activité de votre clavier jusqu'à l'encodage d'une adresse mail - reconnaissable au « @ » - et mot de passe).

Messagerie instantanée :

1) Ne pas accueillir d'inconnus dans la liste d'amis et ce même s'il a un profil « jeune » attirant.
2) Ne jamais aller à un rendez-vous pour une rencontre « life » avec quelqu'un rencontré sur internet.
3) Ne pas croire tout ce qu'on y dit. La diffusion des Hoax passe souvent par là aussi.
4) Pas de webcam avec des inconnus

Réseaux sociaux

Principal moyen de communication et par lequel les ados rentrent en contact avec les autres.

Mr Bogaert présente les principaux réseaux sociaux utilisés par les jeunes :

- Netlog :
  Seul réseau belge, particulièrement attentif à la sécurité et la protection de la vie privée mais … pratiquement inconnu.

- Twitter :
  Permet d'interagir et donner les événements très rapidement.
  Comme il permet de faire des commentaires : ne jamais oublier qu'un twit peut être retwitté. Cela peut donc aller très vite et même parfois trop.
  Ex : Fadila Laanan –mauvais lien dans un twit

- My Space :
  Espace où un artiste peut tester l'accueil que le public fera à ses nouveautés dans le secteur de la musique, vidéo ou art.

- Google + :
  Si vous avez une adresse gmail, Google vous a créé de manière automatique un profil sur Google +.

- Youtube :
  Site musical qui appartient à Google, qui bien sûr vous enverra de la pub en fonction de vos centres d'intérêts (connu suite à votre navigation).

- Ask :
  Comptait 10 millions d'utilisateurs en 2012, en compte 64 millions en 2014
  Permet d'interpeller un profil anonymement… et lâchement ! Ce qui mène aux pires dérives d'internet aux conséquences parfois catastrophiques.

- Snapchat :
  Photo instantanée qui est censée disparaître après un temps déterminé … sauf qu'il existe maintenant des applications qui permettent de récupérer l'image, de faire croire qu'elle n'a jamais été vue alors qu'entre temps, elle a été captée et diffusée à bien d'autres destinataires que les destinataires initiaux…
  Mr Bogaert insiste sur ce dernier élément car, sous prétexte que cela s'efface, on a tendance à envoyer tout et n'importe quoi par Snapschat et on oublie que certaines personnes peuvent être mal intentionnées, même involontairement !

- Facebook :
  1 humain sur 7 est sur Facebook, on compte 6 milliards de « like » par jour. Grâce à ces likes, on connait vos centres d'intérêts.

  Il y a souvent une course au nombre d'amis… ce qui pousse souvent à des comportements dangereux.

  MrBogaert rappelle que Facebook est une société commerciale qui, par les informations que vous transmettez, vous adresse des publicités ciblées.

  Il développe donc ci-après Facebook plus en détail

<u>La problématique Facebook</u> :

Vu les éléments ci-dessus, Il est donc important :
- de limiter l'accès à votre profil à vos amis connus (pas de challenge au plus grand nombre d'amis…).
- être prudent sur les photos et les données de votre profil.
- respecter les autres (pas de photos de tiers sans leur accord, voir ci-après Mr Wéry).
- bien paramétrer la confidentialité par rapport au contenu.

<u>Paramètres de confidentialité</u> : (cadenas)

1) **Journal** (mur) :
   Si votre profil a été créé avant avril 2014, par défaut, votre journal (mur sur Facebook) est public. Il est donc nécessaire d'aller vérifier si le paramètre de confidentialité est activé.
2) **Evénement marquants** :
   Attention à ce que l'on poste sur le mur car Google dispose d'un logiciel « Gramsearch » qui analyse le contenu des données reprises sur le mur et n'hésite pas à les reprendre en événements marquants et qui vous permet de retrouver des groupes suivant certains critères même si on ne souhaite pas qu'ils y figurent. CQFD, tout contenu est analysé.

   Solution : aller vérifier les paramètres de confidentialité via
   - le cadenas (en haut à gauche),
   - puis sélectionner le dinosaure. Là, vous arrivez sur les menus de paramètres de confidentialité « de base ».

Mr Bogaert conseille aussi d'aller plus loin voir la notion *« Souhaitez-vous que d'autres moteurs de recherche puissent avoir accès à votre profil »* qui par défaut, si votre profil date d'avant avril 2014, est mis sur « oui ». Cela ouvre donc votre journal à tous les moteurs de recherche…

3) **Journal d'identification** :
   C'est là que votre image peut être associée à votre profil par quelqu'un d'autre. En activant ce paramètre, vous serez automatiquement avisé lorsque quelqu'un publie une photo en l'associant à votre profil. Cela permet de la supprimer de votre mur et/ou interagir avec la personne pour en obtenir la suppression si nécessaire.

4) **Les applications** :
   Si un de vos amis utilise une quelconque application et vous en informe, les développeurs de cette application ont mis au point des programmes qui leur permettent d'avoir accès à vos informations également … sauf si vous bloquez cette possibilité dans les paramètres de confidentialité.

Facebook sur smartphone :
Depuis la dernière mise à jour de juin 2014, Facebook lit vos sms sur votre smartphone, ce qui lui permet de mieux vous connaître pour mieux cibler les pubs à vous adresser.

Mr Bogaert rappelle aussi que les conditions d'utilisation (que tout utilisateur de Facebook accepte) comportent un droit d'utilisation des contenus ! Il rappelle également que tout élément mis sur Facebook ne peut jamais être totalement effacé. En effet, même si l'on demande soi-même d'effacer son profil Facebook, il ne sera effacé que du serveur où il est hébergé 60 jours après la demande. Mais ne sera effacé que le contenu de ce seul profil. Si quelqu'un a repris une quelconque information de votre profil, elle existera toujours tant que le profil de cette personne existera et Facebook peut garder une copie d'archive du contenu. Bref, tout ce que vous mettez sur Facebook ne vous appartient plus et peut avoir de lourdes conséquences plus tard lorsqu'un employeur ira consulter votre profil.
Ex : jeune activiste qui ne trouvait pas d'emploi.

Il rappelle également la rapidité à laquelle une information (vraie ou fausse) se propage sur internet.

Dérives : cyber harcèlement

Cela peut prendre plusieurs formes :

- création de faux profil où l'on publie de fausses informations sur des personnes pour s'amuser mais aux conséquences qui peuvent être dramatiques.
- Harcèlement direct sur votre profil par inondation de notifications par plusieurs personnes

Mr Bogaert, présente rapidement le site « stop cyberhate » : application qui permet de traiter du cyber harcèlement, illustrée de vidéos. Sur ce site figure aussi un questionnaire qui permet à toute personne qui se sent mal par rapport à une situation sur internet d'évaluer si elle est en situation critique ou non. Si c'est le cas, l'aide à l'enfance (n° de téléphone 103) peut être contactée automatiquement et vous mettre en lien avec une personne anonyme qui peut vous donner des conseils.

En cas de cyber harcèlement de quelque sorte que ce soit, il faut demander de l'aide ou en parler à une personne de confiance (parents, frère, ami, profs, éducatrice,…) et ne pas rester seul face à ce problème.

Mr Bogaert rappelle aussi aux parents présents que, sur le site de Child Focus, sont repris tout un tas de conseils, entre autres, en ce qui concerne les paramètres de sécurité à appliquer en fonction de la tranche d'âge des enfants.

Sur ces dernières informations se termine l'intervention de Mr Bogaert qui passe la parole à Mr Wéry.

Tout d'abord, Etienne Wéry dresse un rapide schéma du problème : les parents vivent au XXème siècle et les ados au XXIème. En clair, il y a eu une telle évolution technologique ces dernières années qu'il est normal que les adultes aient du mal à suivre alors que les ados, qui sont nés dedans, suivent cela sans problème. Dans l'histoire de l'humanité, il n'est jamais arrivé de devoir assimiler une telle différence intergénérationnelle en si peu de temps.

Internet c'est :

- la mobilité : partout et tout le temps.
- le partage : valeurs fondamentales d'internet et des jeunes d'aujourd'hui
- l'abondance : on peut trouver tout et n'importe quoi sur le net, il n'y pas de limite. Tout peut être mis en ligne pour autant que ce soit dématérialisable.
- l'instantanéité : aujourd'hui, on ne peut plus attendre : on veut communiquer tout et tout de suite. Que ce soit bien ou pas, c'est une valeur pour la jeunesse d'aujourd'hui.
- la standardisation : on a l'impression que le contenu est varié mais en réalité, Facebook vous guide pas à pas sur la mise en ligne de votre contenu et Google fait de même lorsque nous faisons une recherche. Ce qui a comme conséquence que lorsqu'un professeur demande une recherche, il reçoit quasi exactement le même travail de tous ses élèves.
- Paradoxe de la liberté : pour un ado, un gsm est synonyme de liberté. Avec un gsm il est libre de communiquer avec le monde entier à tout moment et le plus vite possible. Alors que cela n'a jamais été aussi risqué : lorsqu'on exerce cette liberté, on se met en danger (Facebook qui lit les sms).
- Paradoxe de la concurrence : le contenu est tellement standardisé que l'on est poussé à différencier son contenu. Le but est de trouver un élément qui vous différencie des autres.

Ces différents éléments peuvent également s'appliquer à l'image avec une remarque supplémentaire : l'image est universelle et peut être comprise de tous (de quelque pays que vous veniez). Mr Wéry rappelle aussi que le fait de mettre une image sur Facebook fait qu'elle ne vous appartient plus (voir conditions générales Facebook ou autre version fantaisiste).

L'image est aussi mon moi que je mets en concurrence. Pour exister sur son mur par rapport aux amis, on va être incité à aller un peu plus loin et c'est cela qui mène à des dérives.

!!! Internet a été fait par et pour l'image et l'image est faite pour internet ! Ce qui explique que nos ados « sont accros » à leur gsm parce que le monde dans lequel ils évoluent a été créé comme cela.

Le droit est-il efficace pour éduquer les jeunes ? : pas vraiment parce que le droit n'est pas très universel alors qu'internet est universel. Le droit est aussi lié à l'autorité et à la transmission de l'information verticale alors qu'actuellement, on travaille de plus en plus sur l'horizontalité : le savoir existe et est à disposition. Il est plus important de savoir le retrouver et le manipuler que de le connaître.

De plus, les notions de droit diffèrent très fort d'un endroit à un autre. Par ex., les notions de droit à l'image et protection de la vie privée n'existent pas aux Etats-Unis (ni dans la culture, ni en droit) alors que chez nous, elles sont très fortes.

La vie privée et le droit à l'image sont des notions qui ont été inventées pour se protéger des attaques extérieures. Malheureusement, dans 75% des cas, le problème n'est pas venu de l'extérieur. Il vient de l'attitude de la personne elle-même qui a fait une bêtise et le regrette par après. Et contre cela, le droit ne peut rien.

On a par rapport à la vie privée une incompréhension complète intergénérationnelle. Mais les enfants ne sont heureusement pas tous devenus fous et les parents ne sont pas tous des ringards.

Dès lors, il faut faire reposer le dialogue intergénérationnel sur autre chose que des notions juridiques. A la place, il faut le faire reposer sur des repères universels, neutres et non juridiques.
L.E CRITERE qui répond à cela est la notion de mise en danger de soi ou des autres et afin de repérer quand il y a mise en danger, Mr Wéry propose de se poser **6 questions** :

1) <u>En ligne un jour = en ligne toujours</u>
   Suis-je prêt à assumer mon comportement aujourd'hui, demain et tout au long de ma vie car le contenu que l'on met en ligne aujourd'hui, dans 10 ans, il sera toujours là, et ce quoi que l'on fasse. Il faut donc être prêt à le défendre 10 ans plus tard. Ex. : jeune activiste qui ne trouve pas de travail suite à son passé.

2) <u>Réflexe « Decaux »</u>
   Etes-vous prêt à assumer que ce que vous mettez en ligne soit affiché dans tous les abribus de Belgique ? En mettant un contenu sur Facebook, c'est ce que vous faites au niveau mondial… Mr Wéry rappelle que les paramètres de confidentialité peuvent être contournés, ne sont pas faciles à manipuler et peuvent être modifiés lors de mise à jour du site.

3) <u>Moi c'est toi et toi c'est moi</u>
   Est-ce que je suis prêt à accepter que l'on me fasse ce que je suis en train de faire à un autre ?

   Faire une blague, c'est pas bien méchant. Sauf qu'avant, lorsqu'on se bagarrait dans la cour de récré, les cours et le retour au domicile le soir permettaient de calmer le jeu. Sur internet, l'escalade ne s'arrête jamais. C'est souvent comme cela que commence le cyber harcèlement.

   Tous les ans en Belgique, plusieurs ados se suicident suite à du cyber harcèlement qui a toujours commencé par quelque chose qui se voulait amusant, qui pris individuellement n'était pas super grave, mais si tout le monde s'y met toute la journée, puis 24h sur 24, cela termine souvent mal. Même une seule fois, c'est une fois de trop.

4) Ami ou ennemi
   Suis-je prêt à offrir à mon ennemi ce que je m'apprête à mettre en ligne ?

   Ce qui vous est personnel vous est personnel : ne mettez pas en ligne quelque chose qui pourrait donner du grain à moudre à votre ennemi ou à quelqu'un qui pourrait le devenir. Un ami peut devenir du jour au lendemain un ennemi et faire un mauvais usage d'informations que je lui ai données (ex. : mot de passe pour pirater un compte Facebook ou prédiction voyant)

   CQFD Faites attention à ce que vous mettez sur Facebook, on peut facilement tout savoir de vous.

5) Personne n'est parfait
   Si cela se passe mal, quel est le risque ? :

   Ne pas faire n'importe quoi parce que même si on destine la photo ou autre contenu à un cercle limité, cela peut toujours partir ailleurs comme expliqué ci-avant.

6) Au secours
   En cas de catastrophe, puis-je appeler quelqu'un en qui j'ai confiance et me faire aider (parents, professeurs, éducatrices, famille, …)
   Ex : vidéo « dénudée » rançonnée sur internet.

Si je réponds NON à une de ces 6 questions, il ne faut pas faire ce que j'étais prêt à faire sur internet. Vous vous mettez en danger ou vous mettez quelqu'un en danger.

Que faire en cas d'harcèlement :

1) Ne pas répondre
   Cela casse la surenchère et même si la personne continue à vous harceler, sans réponse, elle se lassera après quelques jours. C'est très dur mais c'est la seule solution.

   Pour protéger un jeune dans cette situation, il faut lui retirer tous ses moyens de communication pendant 10 jours. Après 10 jours, c'est en grande majorité passé et plus personne ne parle du problème.

2) Aller en parler à quelqu'un de confiance qui en fonction de la gravité fera le nécessaire (s'adresser aux parents du harceleur, à la police, à un avocat, …)

3) Si pas de possibilité d'en parler à quelqu'un de confiance, appeler le 103, numéro gratuit, anonyme, ouvert de 9h00 à 24h00 d'Ecoute Enfants (professionnels à l'écoute qui en ont déjà tellement entendu que rien ne les étonnera).

Avant d'entamer les questions, Mr Wéry rappelle la présence de l'équipe de Devoir d'enquêtes et fait appel aux témoignages.

Questions :

Quelle attitude peut-on avoir pour protéger nos ados sans être trop intrusif ?

Mr Bogaert suggère le dialogue au travers du partage d'expérience. Il ne faut pas rester figé à l'outil numérique : l'adulte a de l'expérience, qui même si la situation n'est pas similaire, peut être apparentée. Parallèlement, il rappelle qu'il faut mettre des règles et/ou limites d'utilisation.

Où vont tous les snapschat ?

Mr Bogaert précise que même fugace, la photo restera sur un serveur quelque part. Le but de la fugacité est d'inciter la personne à utiliser l'application et il est déjà arrivé que des pirates entrent sur les serveurs Snapshat et diffusent des photos.

Mr Wéry rappelle que statistiquement, si on a envoyé une mauvaise photo sur Snapshat, on a plus de chances de gagner au lotto que de voir faire un mauvais usage de la photo par Snapshat.

Le danger vient plus de la personne à qui on adresse la photo. En effet, bien que censée être fugace, il existe maintenant des applications ou des possibilités de garder les Snapshats via capture d'écran.

Peut-on supprimer les Screanshot faits par d'autres :

Techniquement, non. Mais si tu sais qui a fait le Screanshot, il faut en parler avec tes parents qui via un avocat ou via la police feront le nécessaire pour que la photo soit supprimée.

Si on sait qui l'a fait, on peut aussi aller le/la voir en direct et lui expliquer qu'il n'a pas le droit de le faire. Il aura alors comme solution de l'effacer ou les autorités lui prendront son téléphone.

Que faire en cas de publication de quelque chose sur Facebook sans l'accord de la personne concernée :

Mr Bogaert rappelle qu'il est possible de signaler l'information à Facebook et qu'il existe une procédure de signalement d'une publication :

- Onglet « aide » (à côté du cadenas en haut à gauche)
- Se positionner sur le coin droit de la publication, une flèche inversée apparaît. En cliquant dessus, on arrive au menu de signalement (pourquoi on signale et qu'est-ce qu'on signale)

Le signalement est envoyé à Facebook qui analyse le signalement par rapport aux conditions d'utilisation et prendra le cas échéant contact avec vous par mail pour faire la preuve de votre signalement. Si Facebook est d'accord avec le signalement, il supprime automatiquement la publication. Si ce n'est pas le cas, il faudra passer par des procédures plus lourdes. Malheureusement, il faut savoir que Facebook est assez difficile à convaincre.

Un père souligne que Facebook est une immense machine commerciale et que chaque utilisateur de l'application rapporte 10 $ par an à Facebook. C'est donc une grande machine marketing qui vous adresse de la publicité ciblée en fonction de vos contenus. Mr Bogaert complète l'intervention en indiquant que Facebook a modifié ses conditions d'utilisation : depuis le 1er janvier 2015, Facebook s'autorise à vous géolocaliser en permanence (puce gsm ou borne wifi) afin de vous adresser de la pub ciblée géolocalisée (ex Centre commercial)!

Que peut-on faire en cas de photo inappropriée ?

1) Supprimer la photo (voir ci-avant)
2) Si Facebook s'en sert, je peux m'y opposer mais il faut passer par une procédure en justice (que l'on gagne facilement). Malheureusement, la photo n'est effacée que du serveur en question et pas toutes ses copies ou back up. Elle devient peu visible mais garantir qu'elle disparaisse à tout jamais est impossible.
3) Dans le pire des cas, il faut supprimer son compte Facebook : 60 jours après la demande, toutes les données seront effacées par Facebook à tout jamais

La plupart des plaintes passent par les sites de signalement. Il n'existe pas de statistiques officielles mais c'est comme cela que l'on règle la plupart des cas. Il faut savoir que lorsque cela part en justice, les sanctions peuvent être très lourdes. Heureusement, la plupart des plaintes sont gérées par les signalements : c'est gratuit et cela va relativement vite. Le site de la Computer Crime Unit est à votre disposition pour les signalements.

Comment se prémunir des mails de fishing :

Il existe des navigateurs qui en protègent plus ou moins bien.

Dans le monde du logiciel libre, Mr Bogaert recommande d'installer Firefox qui peut être couplé à des petits modules complémentaires qui signaleront les risques de fishing

Sinon, pour tous les navigateurs, il est possible de leur ajouter un petit module complémentaire « Adblock Plus » : application qui bloque les pubs en pop up. Cela ne plaît pas aux annonceurs mais cette application est soutenue par les états.

En ce qui concerne les mails, les signaler via les fonctions « courriers indésirables » ou « spam » ce qui fera remonter l'information aux opérateurs qui peuvent alors bloquer ces mails dans votre boîte mails;

*
* *

Mme Simon remercie les 2 conférenciers pour leurs exposés très intéressants et invite les nombreux parents à une collation pendant que les filles regagnent leurs dortoirs.

*
* *

Suite à la conférence, Mr Bogaert m'a adressé un mail reprenant quelques sites intéressants à connaître.

Outre ceux déjà repris dans le texte ci-dessus, il conseille d'aller visiter les sites pour :

- Scanner son ordinateur à partir d'une solution externe :
  http://stopransomware.fr/nettoyer-son-ordinateur
- Trouver un logiciel antivirus :
  Taper « comparatif antivirus » dans Google