2. Internet – Mise en relation des personnes et des idées

> « Finalement, tout est lié – les gens, les idées, les objets. La qualité du lien est la clé de la qualité en tant que telle ».
>
> *Charles Eames, designer du début du XXe siècle*

LISTE DE POINTS À VÉRIFIER :

6. COURRIER ÉLECTRONIQUE ET COMMUNICATION

Avez-vous créé plusieurs comptes de messagerie électronique et défini des mots de passe différents pour chacun d'entre eux ?

Votre mot de passe est-il assez fiable (plus de 8 caractères et associant lettres, chiffres et symboles) ?

Indiquez-vous clairement l'objet de vos courriers électroniques à l'aide de mots-clés pertinents dans la ligne prévue à cet effet ?

Avez-vous prévu une authentification à deux facteurs sur vos comptes de courrier électronique (question de sécurité subsidiaire et/ou numéro de téléphone portable) ?

7. SALONS DE DISCUSSION (DIALOGUE EN LIGNE OU CHAT) ET MESSAGERIE INSTANTANÉE

Vos coordonnées figurent-elles dans votre site web ou blog ?

Avez-vous pris des mesures pour protéger votre vie privée en ligne ?

Vous êtes-vous assuré que le contenu que vous utilisez pour votre site web/blog respecte la législation relative au droit d'auteur ?

8. RÉSEAUX SOCIAUX ET PARTAGE SOCIAL

Nous n'avons qu'une réputation : réfléchissez-vous systématiquement avant de publier quelque chose en ligne ?

Quand avez-vous mis à jour pour la dernière fois vos paramètres de confidentialité sur les sites que vous utilisez ?

La démocratie repose sur la participation du plus grand nombre possible de citoyens au débat public : avez-vous essayé de faire entendre votre voix par le biais des sites de réseautage social qui le permettent ?

9. PROTECTION DE LA VIE PRIVÉE ET PARAMÈTRES DE CONFIDENTIALITÉ

Avant de publier une photo sur les réseaux sociaux, vous demandez-vous s'il est vraiment nécessaire de le faire et d'identifier les personnes qui y apparaissent ?

Lisez-vous les conditions générales d'utilisation des applications mobiles pour comprendre ce qui est « à vous » et ce qui est « à eux » dans tout ce que vous partagez ?

Lorsque vous installez une application, êtes-vous sûrs de savoir exactement à quelles informations privées elles auront accès ? Cet accès est-il véritablement nécessaire au bon fonctionnement de l'application ?

Savez-vous quel est l'impact du Règlement général de l'Union européenne sur la protection de vos données ?

Fiche d'information 6

Courrier électronique et communication

Le courrier électronique[1], (e-mail) est un outil qui permet d'envoyer des messages entre plusieurs ordinateurs connectés à un réseau comme Internet. Ce terme désigne également le message lui-même (abrégé « courriel »). Il ne faut en général que quelques secondes pour transférer un courrier électronique. Le destinataire peut en prendre connaissance et y répondre quand il le souhaite. D'une utilisation souple et efficace, le courrier électronique a radicalement changé la manière dont nous travaillons et communiquons. Des milliards de messages sont envoyés chaque jour.

Une adresse de messagerie électronique se compose de deux parties : un nom local et un nom de domaine, séparés par le signe « @ ». Le nom local est souvent, mais pas toujours, le nom de l'utilisateur, tandis que le nom de domaine correspond à l'organisation, à la société ou au fournisseur d'accès Internet de celui-ci. Le nom de domaine peut également désigner le type d'organisation et/ou le pays. Par exemple, name@ox.ac.uk est l'adresse d'une personne qui travaille ou étudie à l'Université d'Oxford.

1. https://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique

Les comptes de courrier électronique restent au cœur de l'expérience utilisateur car ils sont souvent demandés pour pouvoir s'inscrire à des sites et participer en ligne. Par conséquent, bien qu'il existe aujourd'hui de nombreux autres moyens de communication dont certains peuvent être préférés aux emails (réseaux sociaux, messagerie instantanée, etc.), les adresses électroniques sont devenues un aspect essentiel de l'identité en ligne des Internautes et leur servent souvent d'identifiant pour se connecter à l'ensemble des services en ligne qu'ils utilisent.

INTÉRÊT PÉDAGOGIQUE

Les adresses de courrier électronique étant souvent demandées en ligne, apprendre à bien gérer un compte de courrier électronique a des vertus pédagogiques, comme apprendre à trier du courrier physique en séparant le contenu personnel du contenu administratif important pour pouvoir le retrouver facilement.

Le courrier électronique est également un outil précieux dans les projets interculturels entre élèves de pays différents. Il peut être utilisé pour l'amélioration de leurs connaissances en langues et le partage d'informations sur leurs cultures respectives.

Certains élèves plus réservés s'expriment mieux par le courrier électronique que dans une discussion en classe face à d'autres élèves

CONSIDÉRATIONS ÉTHIQUES ET RISQUES

- Votre adresse email étant la porte d'entrée à tous vos comptes en ligne, le piratage de votre compte de courrier électronique peut avoir des conséquences très graves.
- La plupart des clients de messagerie (programmes informatiques utilisés pour accéder au courrier électronique[2] d'un utilisateur et le gérer) que l'on trouve en ligne sont gratuits, mais nombre d'entre eux utilisent des algorithmes pour analyser le contenu de vos messages et afficher de la publicité ciblée sur la page d'accueil de votre messagerie web.
- Il est difficile d'exprimer des émotions dans un courrier électronique. C'est pourquoi il faut toujours veiller à rédiger vos messages avec soin pour vous assurer qu'ils ne seront pas mal compris. Les « émoticônes »[3], petites icônes expressives dont font partie les smileys, peuvent vous aider à préciser vos intentions, et en particulier à exprimer l'ironie ou l'humour. Utilisez-les toutefois avec parcimonie pour ne pas détourner l'attention du destinataire de votre message.
- Un pourcentage important des courriers électroniques reçus sont des messages non sollicités et sont en général des spams indésirables[4] (voir Fiche d'information 19 sur le spam, les logiciels malveillants, la fraude et la sécurité). Heureusement, les filtres antispam sont de plus en plus efficaces pour distinguer ce type de messages des courriers électroniques normaux.
- Veillez à ne pas contribuer vous-même à la diffusion de ces messages indésirables en transférant à tout va des courriers électroniques que vous trouvez « amusants » ou « intéressants » à l'ensemble de vos contacts. Si vous le faites trop souvent, les filtres antispam risquent d'identifier votre adresse de courrier électronique comme un proxy de spam et de la bloquer, empêchant ainsi tout contact avec quelqu'un d'autre.
- Certains courriers transférés sont faux ou frauduleux, par exemple, ceux qui prétendent qu'une société ou organisation s'est engagée à verser une somme d'argent donnée pour une cause humanitaire (souvent, un enfant malade ayant besoin d'une intervention chirurgicale) à chaque transfert du message.

2. https://fr.wikipedia.org/wiki/Client_de_messagerie
3. https://fr.wikipedia.org/wiki/%C3%89motic%C3%B4ne
4. https://en.wikipedia.org/wiki/Email_spam

- Il est très facile de masquer un nom pour tromper le destinataire. Il suffit par exemple de le modifier dans les paramètres ou de créer une adresse électronique anonyme de type *elvispresley@hotmail.com* dans une messagerie Internet. Même si vous reconnaissez l'adresse électronique comme étant celle d'un de vos contacts, vérifiez également la ligne « objet » du message car il est possible que l'ordinateur de l'expéditeur soit devenu une « machine zombie »[5] détournée par un pirate ou infectée par un virus.
- Un lien peut sembler vous rediriger vers un site web alors qu'il vous conduit en fait à un autre. Cette technique est particulièrement courante dans les attaques d'hameçonnage (*phishing*)[6].

BONNES PRATIQUES

- Créez plusieurs comptes de courrier électronique à des fins différentes (inscription sur des sites de réseaux sociaux, achat de produits en ligne, etc.). Conservez-en un que vous garderez aussi privé que possible en ne publiant pas son adresse sur le Web et en ne l'utilisant que pour les services importants que vous et vos amis utilisez. Réservez-en un autre pour vous inscrire à des services que vous pourriez n'utiliser qu'une fois, ou que vous n'utilisez que rarement.
- Veillez à rédiger des messages aussi concis que possible. Essayez d'éviter les paragraphes trop volumineux. Vérifiez l'orthographe.
- Pensez à bien indiquer le but de votre message à l'aide de mots-clés pertinents dans la ligne « objet ». Cela permet au destinataire d'une part, de voir qu'il s'agit d'un message authentique et d'autre part, de le retrouver plus facilement par la suite.
- Créez des mots de passe sécurisés pour vos comptes de courrier électronique (plus de 8 caractères, associant lettres, chiffres et symboles) et utilisez des mots de passe différents pour chaque compte.
- Restez raisonnable quant au volume de courrier électronique que vous envoyez et faites preuve d'intelligence et de stratégie dans le choix de vos outils de communication. Une conférence téléphonique ou une discussion sur un forum privé seront peut-être plus adaptées à des échanges privés avec un grand nombre de personnes qu'une masse de courriels.
- Abstenez-vous de vérifier votre messagerie électronique toutes les dix minutes. De nombreuses personnes se laissent interrompre en permanence par les courriels.
- De manière générale, ne transmettez jamais des informations sensibles comme vos coordonnées bancaires par courrier électronique. Vous n'aurez à le faire qu'en de rares occasions, par exemple pour réserver une chambre d'hôtel. En cas de doute, agissez avec précaution, vérifiez la réputation en ligne du service que vous souhaitez utiliser et la marche à suivre pour supprimer la carte ou annuler la transaction et préférez des services de paiement comme PayPal aux services moins sécurisés comme les services de transfert direct d'argent (par exemple Western Union). Cela dit, n'envoyez jamais par courriel des informations confidentielles telles que les identifiants et mots de passe de vos comptes en ligne. Les services en ligne ne vous les demanderont jamais. Si vous recevez un courrier électronique sollicitant ces données, il s'agit d'une tentative d'hameçonnage.
- Des stratégies de hameçonnage sont de plus en plus sournoises font leur apparition, dont certaines consistent à vous envoyer de faux courriels de notification qui imitent parfaitement les messages que vous recevez des services que vous utilisez (par exemple, les sites de réseautage social) et vous dirigent vers un faux site web vous demandant vos données de connexion. Pensez à vérifier systématiquement l'adresse de courrier électronique de l'expéditeur du message et l'adresse du site web donné en lien au cas où quelque chose vous paraîtrait suspect.

5. https://fr.wikipedia.org/wiki/Machine_zombie
6. https://fr.wikipedia.org/wiki/ Hame%C3%A7onnage

- Conservez une saine méfiance par rapport au courrier électronique que vous recevez. N'ouvrez pas un message dont la source ne vous semble pas fiable.
- Soyez particulièrement attentifs aux pièces jointes. Si vous n'attendiez pas une pièce jointe de l'expéditeur du message ou si elle ne vous semble pas fiable pour toute autre raison, supprimez-la sans l'ouvrir. Même les pièces jointes reçues d'expéditeurs connus et dignes de confiance devraient d'abord être enregistrées puis analysées au moyen d'un antivirus avant d'être ouvertes.
- Faites usage de toutes les fonctionnalités de sécurité proposées par votre client de messagerie. De manière générale, il vous propose de fournir une deuxième adresse de courrier électronique au cas où votre compte serait victime de piratage et de plus en plus, de donner également votre numéro de téléphone portable pour des vérifications de sécurité plus poussées dans des cas exceptionnels. Configurez correctement les paramètres de sécurité de votre compte de manière à ce que vous puissiez plus facilement le récupérer s'il venait à être piraté.
- Consultez la Fiche d'information 19 sur le spam, les logiciels malveillants, la fraude et la sécurité pour des conseils supplémentaires concernant le courrier électronique.

MODE D'EMPLOI

- Pour consulter vos courriers électroniques, vous pouvez utiliser l'application « officielle » de votre service de courrier électronique sur votre smartphone, votre tablette ou votre ordinateur fonctionnant sous Windows 8 ou version ultérieure (par exemple l'application Gmail, Outlook ou Yahoo!), aller directement sur son site web (en utilisant un service de messagerie web) ou utiliser un client de messagerie, application externe qui télécharge les courriers électroniques depuis votre service de courrier électronique et vous permet de les gérer et de les organiser. L'avantage de cette dernière solution est qu'elle permet de regrouper et de consulter en un même endroit tous vos courriels, téléchargés depuis plusieurs services différents. Les clients de messagerie les plus courants sont Thunderbird et Outlook. Le plus souvent, ils sont utilisés pour les courriels professionnels.
- Pour plus d'informations sur la mise en place d'un filtre antispam, voir la Fiche d'information 19 sur le spam, les logiciels malveillants, la fraude et la sécurité

SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Demandez à vos élèves les plus âgés qui disposent d'une adresse e-mail, de se connecter à leur service de courrier électronique et d'aller dans les paramètres de sécurité pour sécuriser leur compte en ajoutant une question de sécurité, une deuxième adresse email ou un numéro de téléphone portable.
- Voici les procédures à suivre pour sécuriser votre compte de courrier électronique sur Gmail, Yahoo! et Outlook.
  - ▶ *<https://support.google.com/accounts/answer/46526?hl=fr>*
  - ▶ *<https://support.microsoft.com/fr-fr/help/12410/microsoft-account-help-protect-account>*
  - ▶ *<https://fr.aide.yahoo.com/kb/account/Sécurisez-votre-compte-Yahoo-sln2080.html>*
- Pourquoi insister sur ces trois grands en particulier, alors qu'il existe de nombreux autres services de courrier électronique ? Pour la raison qu'ils sont, du moins pour Gmail et Outlook/Hotmail, liés à de nombreux autres services. Ainsi, un compte Google est quasiment indispensable lorsque l'on possède un smartphone fonctionnant sous Android et le compte Outlook est souvent relié au système d'exploitation Windows. Cela signifie qu'indépendamment de vos préférences, vous pourriez être « contraint » de créer un compte de courrier électronique

sur l'un de ces services. Vous êtes bien entendu libre d'utiliser des clients de messagerie proposant des paramètres de confidentialité plus stricts comme Web.de ou Protonmail.com. En général, les fournisseurs d'accès à Internet proposent eux aussi un service de courrier électronique. D'autres solutions peuvent également être trouvées en ligne.

- Invitez vos élèves à travailler par groupes de trois ou plus et demandez-leur d'imaginer des mots de passe fiables pour un compte de courrier électronique factice. Précisez bien qu'il s'agit d'en trouver de nouveaux et non de divulguer leurs mots de passe personnels ! Après 10 minutes de recherche d'idées, demandez aux équipes de présenter leur mot de passe en précisant pourquoi elles pensent qu'il est sécurisé. Aidez-les à définir les caractéristiques d'un mot de passe sûr (plus de 8 caractères, associant chiffres, lettres et symboles) et les défauts habituels des mots de passe peu robustes (mots se trouvant dans un dictionnaire, ayant un lien direct avec vous comme votre nom de famille, le nom de votre chien, etc.)

INFORMATIONS COMPLÉMENTAIRES

- Des exemples bien connus de clients de messagerie sont Microsoft Outlook *<https://products.office.com/en-us/outlook/email-and-calendar-software-microsoft-outlook>* et Mozilla Thunderbird *<http://www.mozilla.org/projects/thunderbird/>*.
- Truth or Fiction est un site web permettant aux Internautes de vérifier la véracité des courriers électroniques couramment transférés : *<http://www.truthorfiction.com/>*. Un autre site similaire : *<http://m.snopes.com/whats-new/>*.
- Trois des principaux sites de messagerie web sont Outlook *<https://office.live.com/start/Outlook.aspx>*, Yahoo! *<https://mail.yahoo.com>* et Gmail de Google*<http://www.gmail.com>*. Vous pouvez également chercher vous-mêmes d'autres prestataires de courrier électronique, dans votre pays.
- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :

  Article 13 – L'enfant a le droit de recevoir et de répandre des informations à condition qu'elles ne nuisent ni à lui-même, ni à autrui.

  Article 16 – L'enfant a le droit au respect de sa vie privée et à la protection de la loi contre toute atteinte ou immixtion dans son mode de vie, sa réputation, sa famille ou son domicile.