Protéger ses données et son ordinateur

Objectifs de cet atelier	*Pré requis*
Savoir protéger son ordinateur des menaces. Savoir nettoyer ses traces.	Les bases de l'utilisation d'un ordinateur.
Matériel nécessaire	*Durée*
Un ordinateur pouvant être connecté à internet. Un accès internet et si besoin des ordinateurs seront mis à disposition lors de l'atelier.	Une heure trente à renouveler selon les demandes et les besoins.

Déroulement de l'atelier

1) Logiciels
2) Le courrier électronique
3) Mots de passe
4) Payer sur Internet avec vos données bancaires
5).Communiquer sa position
6) Hameçonnage.
7) Sauvegarde et compte utilisateur
8) Les dangers d'internet pour les enfants et ado

Mise en pratique, questions réponses

Evaluation, votre avis sur la séance, vos questions, les points à revoir, à approfondir

1) Les logiciels.

1.1) Anti virus et autres :

Les logiciels malveillants sont appelés "malwares" en anglais.

Les plus importants malwares sont :

- Les **virus** se dupliquent sur d'autres ordinateurs.
- Les **vers** se répliquent sur un réseau et le saturent.
- Les **espions**/logiciels n'endommagent pas votre ordinateur, mais ils en récupèrent des données qu'ils envoient à leurs auteurs (votre numéro de carte de crédit par exemple).
- Les **chevaux de Troie** sont des logiciels qui s'installent sur une machine pour permettre à d'autres virus de s'introduire ou de se propager (exemple récent les ransongiciels…).
- Les **keyloggers** enregistrent tout ce que vous tapez au clavier.

Les solutions :

Mettez régulièrement à jour vos logiciels (navigateur, antivirus, pare-feu, Windows Update etc.). C'est l'assurance de profiter de la meilleure protection pour votre ordinateur.

Avast, Avira et Windows defender (antivirus gratuits)

Malwarebytes (complète l'antivirus pour les autres menaces) et Adwcleaner (pups…)

Ccleaner (optimisation du fonctionnement d'un ordinateur)

1.2) Firewall.

activez le **pare-feu** de son ordinateur, il permet de définir quel sont les **communications** autorisées sur le réseau.

1.3) Navigateur.

Utilisez de préférence un **navigateur alternatif** Open source (style Mozilla):

- Un **cookie** est un petit fichier envoyé par le site web visité, et installé sur le disque dur de l'internaute via le navigateur. Il permet de suivre à la trace votre navigation.
- **Le cache** conserve une trace des sites visités (fichiers, images, ...), ce qui permet ensuite un chargement accéléré des pages.
- L'**historique** donne une liste de l'ensemble des sites visités sur une période donnée.

La solution pour faire barrage à ces mouchards:

Paramétrez le navigateur afin que les cookies soient acceptés, mais effacés à chaque fois que vous quittez votre navigateur (dans « Préférences », puis « Vie privée ») et effacer le cache et l'historique régulièrement.

Ajoutez des extensions gratuites proposées par les navigateurs (dans « Préférences », puis « Extensions »), comme Ghostery qui permet d'afficher et de supprimer les cookies des régies publicitaires. Adblock qui bloque les bannières publicitaires.

Evitez les extensions de fonctionnalités non indispensables comme les plugins ou les barres d'outils.

1.4) Navigation privée avec protection contre le pistage.

Lorsque vous naviguez dans une fenêtre privée, votre navigateur ne conservera pas :

- Les pages visitées
- Les cookies
- Les recherches
- Les fichiers temporaires

La navigation privée ne vous rend pas anonyme sur Internet.

Votre fournisseur d'accès à Internet ou votre employeur peuvent toujours connaître les pages que vous visitez.

1.5) Changez de moteur de recherche

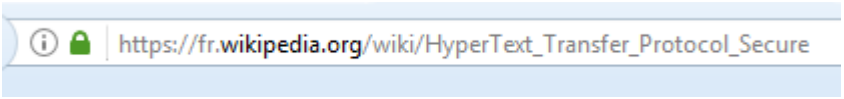
Google est le moteur de recherche le plus utilisé en Europe (80 % des internautes) il vit des pubs et des informations collectées à votre insu.

vous pouvez utiliser des moteurs de recherche ne conservant aucune information sur vos coordonnées ou vos requêtes comme DuckDuckGo (http://duckduckgo.com) ou Qwant (https://www.qwant.com/)

1.6) Vérifiez que le site est sécurisé.

L'HyperText Transfer Protocol Secure, plus connu sous l'abréviation HTTPS — littéralement « protocole de transfert hypertexte sécurisé » permet au visiteur de vérifier l'identité du site web auquel il accède.

Il est également utilisé pour les transactions financières en ligne.



2) Le courrier électronique :

Ne répondez pas aux mails qui demandent la saisie d'informations confidentielles ou personnelles (comme les mots de passe, numéros de comptes, cartes de crédits, etc).

Ne cliquez pas sur les liens ou pièces jointes contenus dans des e-mails si vous n'en connais pas la provenance de façon certaine.

Ayez un esprit critique et analysez chaque message avant d'agir, même si le message provient d'une connaissance :

- Son message est-il étrange ? Inattendu ?
- Utilise-t-il un langage inhabituel ?
- S'agit-il d'un message de détresse ?
- Propose-t-il de participer à un concours ? De profiter d'une aubaine ?
- Le message contient-il un lien ou une pièce jointe ?

Si vous répondez positivement à une de ces questions, soyez prudent et tentez de contacter votre interlocuteur par un autre canal.

Soyez conscient qu'une adresse e-mail peut très facilement être falsifiée.

Ne relayez pas de messages type chaîne de lettres (« Envoie ce message à 10 contacts et tu deviendras riche »)

2.1) Le spam :

Pour éviter le spam (courrier indésirable), utilisez 2 adresses e-mail :

- 1 adresse principale pour les relations de confiance ;
- 1 adresse secondaire (ou un alias) pour les contacts publics.

Pensez aussi aux services d'e-mails jetables pour les informations non-personnelles :

Ne communiquez pas votre adresse e-mail principale à tout le monde et évite de l'afficher ouvertement à des endroits publiquement accessibles (Blog, Facebook, flyer, etc.).

Ne répondez jamais aux spams.

2.2) Les hoax :

Evitez de faire circuler les canulars et fausses nouvelles ou désinformations :

Les virus ne sont pas annoncés par courrier électronique.

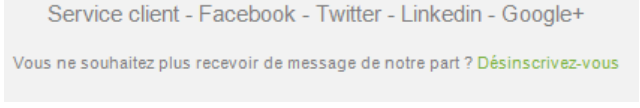
Les correctifs de sécurité ne sont pas distribués par e-mail.

Les e-mails qui vous invite à les diffuser à tous tes contacts (lettres en chaîne) sont presque toujours des canulars ou des arnaques.

En cas de doute, vérifiez les informations reçues sur www.hoaxbuster.com par exemple.

2.3) Les courriels de publicité:

Désinscrivez vous des sites marchands et autres qui vous envoi des pubs par courriels. En général, quelque part sur la page, on trouve (en tout petit) un lien hypertexte se désabonner ou se désinscrire.



3) Les mots de passes.

Près de 7 internautes sur 10 (1) utilisent le même mot de passe pour leurs différents comptes et espaces personnels en ligne. Si c'est votre cas, changez cette mauvaise habitude !,

Evitez a tout prix les mots de passe du style 0123456789.

3.1) Choisir ses mots de passe :

Les mots de passe représentent la fondation de votre sécurité numérique.

Utilisez des mots de passe assez longs (plus de 12 caractères) ou, mieux encore, des « phrases de passe », contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux.

Le mot de passe ne doit pas :

- Faire partie d'un dictionnaire ;
- Correspondre à des données personnelles (noms, date de naissance, etc) ;
- Etre une suite logique de chiffres ou de lettres (123456, abcdef…).
- Utilisez un mot de passe différent pour chaque service en ligne pour éviter que la divulgation accidentelle ou mal intentionnée d'un mot de passe ne donne accès à tous vos comptes d'un coup.

Ne pas oublier de se **déconnecter** à la fin d'une session et n'enregistrer pas votre mot de passe dans le navigateur.

Une technique parmi d'autres:

Choisissez une phrase facilement mémorisable, comme par exemple «Je suis ardéchois07 ».

Ajoutez le nom du service ou du site (par exemple leboncoin.fr)

Cela donne **Jesuisardéchois07leboncoin.fr**

Quasi impossible à deviner et à cracker.

3.2) Gérer ses mots de passe

Il existe des gestionnaires de mots de passe comme Password Safe, LastPass ou KeePass

Ces outils permettent de mémoriser autant de mots de passe que nécessaire, de générer des mots de passe solides et nous alertent sur les problèmes de sécurité qui affectent les différents services utilisés.

4) Payer sur Internet avec vos données bancaires

D'une manière générale, assurez-vous du sérieux du site marchand : la connexion est-elle bien sécurisée (vérifiable avec la mention « https »), y a-t-il un numéro de téléphone, une adresse de siège social, etc.).

N'achetez pas dans n'importe quelle boutique.

Lorsque vous effectuez un paiement sur Internet, le site marchand (ou celui de la banque du commerçant) peut légitimement vous demander :

- Le **n° de votre carte bancaire** : 16 chiffres répartis en 4 blocs de 4 chiffres, présents en relief sur la face avant de votre carte,
- La **date de validité** : en relief sur la face avant de votre carte, après la mention « EXPIRE FIN »,
- Le **cryptogramme** : 3 derniers chiffres imprimés au dos de votre carte à droite de la zone de signature,
- Le **nom** et éventuellement le **prénom** : en relief sur la face avant de votre carte.

Le code secret à 4 chiffres (PIN) qui vous permet d'utiliser les distributeurs de billets, de carburants ou de payer physiquement dans un commerce est **absolument inutile pour un paiement sur Internet**. Ne le donnez jamais sur un site Internet. Il ne vous est demandé que sur les sites frauduleux.

Pour lutter contre l'utilisation des numéros de cartes volés (en phishing par exemple), certains sites commerçants demandent à la banque du client de vérifier que la personne en train d'effectuer le paiement est bien le propriétaire de la carte.

Dans ce cas, lors de l'opération de paiement sur le site marchand (ou sur le site de la banque du commerçant), un **code secret complémentaire** peut vous être demandé. Il peut vous être envoyé par sms, par mail, par téléphone.

Les sites de vente en ligne proposent parfois des **moyens de paiements alternatifs** à la carte bancaire. Certains proposent par exemple le paiement via Paypal, ce qui vous évite de fournir systématiquement votre numéro de carte. Il faut toutefois ouvrir un compte Paypal en fournissant votre numéro de carte ou créditer le compte.

Il est possible d'acquérir une **carte de crédit prépayée**. Ces cartes que l'on peut également utiliser en boutique de rue sont créditées d'un certain montant avant utilisation.

Dans le même esprit que la carte prépayée, les **cartes virtuelles ou e-cartes** sont proposées par quasiment tous les établissements bancaires français.

5) Communiquer sa position

De plus en plus de sites Internet demandent votre position géographique : il s'agit d'une information précieuse pour vous vendre de la publicité ciblée. Mieux vaut refuser.

6) Hameçonnage.

L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc.

Ils envoient aux clients un e-mail « maquillé » qui invite les clients à donner leurs coordonnées.

Ne le faites jamais ! Jamais une entreprise, quelle qu'elle soit (FAI, banque, opérateur mobile, EDF, etc.), n'adresserait une telle demande à ses clients.

Ne répondez jamais à des courriels vous demandant de fournir des renseignements personnels.

Le **pourriel** désigne un message électronique commercial non sollicité que reçoivent des personnes, plus communément par courriel. Le pourriel a souvent la forme d'une publicité, mais il est aussi la source d'escroqueries, de virus informatiques et de contenu offensant.

7) Sauvegarde et compte utilisateur.

Afin de préserver ses données d'une perte irrémédiable, **sauvegardez régulièrement vos fichiers** sur un support externe, disque dur, DVD Rom, clef USB….

Dans l'idéal, il faudrait utiliser deux comptes :

Un **compte administrateur** pour installer les programmes et configurer son PC.

Un **compte de consultation** (avec des droits réduits) pour naviguer sur le net.

8) Les dangers d'internet pour les enfants et ado.

Les jeunes forment la population la plus exposée et la plus ciblée par les prédateurs de toutes sortes sur le Net.

Il est toujours recommandé aux parents et à toutes autres personnes ayant des enfants mineurs sous leur responsabilité de les **accompagner sur Internet** et de s'intéresser aux activités qui peuvent leur être proposées

Il faut sensibiliser les enfants sur les dangers d'internet.

Une session sera organisée a ce sujet