.

Internet: session 2017-2018

INTERNET@Les dangers du Net

Internet devrait être un espace sécurisé où vous et votre famille pouvez communiquer, apprendre, acheter et partager sans vous soucier de la sécurité de vos informations personnelles.

Les plus gros problèmes sur Internet

- LA SÉCURITÉ
- LE VOL D'IDENTITÉ
- LES RÉSEAUX SOCIAUX
- LA TELEPHONIE MOBILE
- LA DÉSINFORMATION

1) La Sécurité

- Utilisez une technologie de sécurité informatique réputée et maintenez-la à jour. Installez toujours des pare-feu et des logiciels de détection des intrusions.

- Effectuez toujours les mises à jour et la maintenance requises pour ces programmes.

- Utilisez un service d'évaluation de réputation de sites Web (pour vérifier rapidement la sécurité d'une URL).

Ce type de service indique les sites potentiellement dangereux pour votre ordinateur.

- Méfiez-vous des sites Web qui demandent l'installation d'un logiciel.

- Lisez toujours attentivement les accords de licence et annulez le processus d'installation si d'autres programmes sont installés en plus du logiciel que vous souhaitez installer.

- Fournissez des informations personnelles uniquement sur les sites Web qui affichent une icône de verrou au bas de votre navigateur.

-Pour protéger votre messagerie électronique, utilisez un programme anti-spam. La plupart des logiciels de sécurité informatique réputés disposent de ce type de fonction.

- Méfiez-vous des e-mails inattendus ou paraissant suspects. N'ouvrez jamais les fichiers joints et ne cliquez jamais sur les liens contenus dans ces e-mails.

- Soyez vigilant lorsque vous recevez des e-mails vous demandant vos coordonnées bancaires, et ne fournissez jamais vos informations personnelles en cas de demandes non sollicitées.

2) Le vol d’identité

Prévenir l’usurpation d’identité et les arnaques en ligne

- Utilisez un logiciel de sécurité réputé sur votre ordinateur. Il vous aidera à protéger votre ordinateur contre les virus,
les programmes espions, les spams et autres logiciels malveillants conçus pour dérober des données personnelles. Mettez-le régulièrement à jour, et veillez à ce que le pare-feu soit activé.
- Naviguez intelligemment sur Internet. Si vous devez saisir des informations personnelles, indiquez-en le moins possible.
Utilisez un mot de passe difficile à deviner et changez-le régulièrement
- Ne téléchargez aucun élément dont vous n’êtes pas sûr. Des logiciels malveillants peuvent parfois être téléchargés au sein d'installations de programmes légitimes. Téléchargez du contenu provenant uniquement de sites réputés et assurez-vous que le fichier que vous téléchargez est sûr en mettant à jour votre logiciel de sécurité.
Soyez très prudent lorsque vous téléchargez des fichiers exécutables (fichiers qui portent l’extension « .exe »).
- Soyez vigilant lors de vos achats en ligne. Consultez les politiques de confidentialité et de sécurité des sites que vous visitez afin de savoir quels types d’informations sont collectées, comment la sécurité de ces données est assurée et avec qui les informations sont partagées.
- Payez vos achats en ligne par carte de crédit. Il s'agit du meilleur moyen d’être couvert contre la fraude.

Vérifiez régulièrement votre relevé bancaire pour vous assurer que personne n’a utilisé votre carte à votre insu,
et signalez toute fraude immédiatement auprès de l’entreprise.

3) Les réseaux sociaux

- **Ne divulguez pas vos données personnelles**. Apprenez à utiliser les paramètres de confidentialité des sites de réseaux sociaux
et vérifiez leurs politiques de confidentialité et de sécurité.
Vérifiez les modalités du service pour vous assurer que vos enfants sont assez âgés pour utiliser le site.
- **Sécurisez votre ordinateur**. Utilisez un logiciel de sécurité informatique réputé et mettez-le régulièrement à jour.

Cela vous aidera à vous protéger contre les logiciels malveillants conçus pour infecter votre ordinateur
et voler vos informations personnelles.
- **Ne divulguez pas d'informations personnelles**. Assurez-vous que vos enfants savent qu'ils ne doivent jamais communiquer leur numéro de téléphone, leur adresse ou leur nom.
Certaines technologies de sécurité, peuvent même vous aider à les empêcher de publier des informations comme le numéro de téléphone de votre domicile.

- **Respectez les droits d'auteur** et évitez d'utiliser ou de divulguer abusivement du contenu protégé par des droits d'auteur sur votre profil.
- **Signalez les problèmes**. Informez le site de tout contact non sollicité ou de tout contenu inapproprié.
La plupart des grands sites de réseaux sociaux disposent d'une fonction spécifique

4) La téléphonie mobile

- **Ne divulguez aucune information** par téléphone que vous ne souhaitez pas publique.

Même s'il s'agit d'une communication privée, dès que les mots sont prononcés ou envoyés, il n'est plus possible de les effacer.

- **Utilisez la Localisation avec prudence**. Prenez soin de ne partager votre position GPS qu'avec des personnes que vous connaissez**.**

- **Téléchargez vos applications** sur les plates-formes reconnues comme sur les «Stores» de votre système d'exploitation

(Android, IOS, Windows...).

5) La désinformation

La désinformation y est courante sous de multiples aspects.

- Les sites haineux qui propagent des propos diffamatoires en diffusant ouvertement des points de vue extrémistes.
- Les sites commerciaux où les publicitaires créent des environnements à la fois informatifs et amusants dans le seul but de promouvoir leurs produits auprès d'un public cible.
- Les pages Web, généralement personnelles, où n'importe qui peut publier ce qu'il veut en prétendant que c'est vrai et présenter de simples opinions comme des faits.
- Les sites « pastiches » ou parodiques, qui induisent volontairement le visiteur en erreur, soit pour s'amuser, soit pour des raisons politiques, ou pour montrer aux jeunes combien il est facile de duper les gens en ligne.
- les canulars diffusés par email, qui diffusent fausses alertes aux virus informatiques, procédés bidon pour soi-disant faire fortune, légendes urbaines et alarmes sanitaires infondées.

A vos notes