Conseils pour éviter les spams et les emails de phishing

1. Protégez votre adresse électronique principale, qui est connectée, par exemple, aux services bancaires en ligne, aux demandes d'emploi ou aux communications professionnelles, et utilisez une deuxième ou une troisième adresse pour tout le reste.

2. Installez un filtre anti-spam associé à une protection anti-hameçonnage et anti-virus - votre fournisseur de messagerie gratuit vous en offre généralement gratuitement.

3. N'ouvrez jamais les pièces jointes d'e-mails provenant d'expéditeurs inconnus.

4. Évitez de permettre aux expéditeurs inconnus de recevoir une confirmation d'envoi d'e-mail ou l'ouverture d'un e-mail, par exemple via des notifications automatiques Out-of-Office.

5. Désactivez l'affichage des emails HTML dans votre programme de messagerie. Cela empêchera par exemple les cookies d'être téléchargés.

6. N'écrivez pas votre adresse électronique en texte brut sur Internet, par exemple dans des livres d'or, des commentaires de blog ou des forums en ligne.

7. S'il n'est pas entièrement nécessaire de fournir votre adresse électronique, ne le faites pas.

8. Ne répondez pas aux spams même s'il existe un lien de désinscription.

9. Ne cliquez pas sur les liens dans les e-mails, car cela permet de vérifier votre adresse e-mail et vous recevrez encore plus de spam à l'avenir.

10. Les adresses des expéditeurs sont faciles à manipuler - vérifiez si l'expéditeur correspond à l'adresse e-mail.

11. Les offres et produits sérieux ne sont pas annoncés par le biais d'envois massifs entachés d'erreurs de frappe.

LIVRE ET CULTURE

Cultivez vos loisirs en toute convivialité

Depuis plus de quinze ans l'association, « ***Livre et Culture*** » œuvre pour offrir aux Montois, et aux habitants des communes voisines, une gamme variée de loisirs et d'activités de divertissement culturel dans de nombreux domaines et elle cherche sans cesse à diversifier son action.
Une quarantaine de bénévoles animent l'ensemble des ateliers et des clubs ainsi que l'administration de l'association.
Les activités de l'Association se déclinent en cinq grands thèmes :

- **Arts Créatifs**
- **Informatique**
- **Photo-Vidéo**
- **Loisirs**
- **Culture**

La plupart de ces animations sont réalisées par des animateurs bénévoles.
Vous pouvez également faire partager votre passion en devenant animateur à votre tour.

2 rue du commerce
37260 MONTS
06 07 65 97 96
www.livreculture.fr

LIVRE ET CULTURE

Cultivez vos loisirs en toute convivialité

Les menaces sur Internet sont tout de même un peu différentes de celles que l'on peut trouver physiquement sur son ordinateur.

Elles concernent principalement tout ce qui touche à la vie privée des internautes.

Peu de risques donc de voir tous nos fichiers disparaitre suite à la visite d'un site.

Par contre les numéros de cartes bleues transitent, les mots de passe et en général toutes les données qu'on transmet depuis notre clavier.

Il est difficile et surtout naïf de vouloir présenter toutes les techniques de hacking possibles liées à la sécurité sur Internet.

Je recommande d'une manière générale de :

Maintenir son navigateur et ses plugins à jour

Changer régulièrement ses mots de passe

Rester vigilant quoi qu'il arrive

2 Navigateurs qui respectent la vie privée

Firefox de Mozilla & Brave *(le dernier né).*

Les plugins utiles : Ublock Origin , Adguard adblocker et Avira Safety Browser

Comment se protéger contre les virus et les chevaux de Troie.

1. Utilisez toujours un programme antivirus avec un filtre anti-spam et anti-phishing.

2. Gardez toujours tous vos programmes (navigateurs, plugins, systèmes d'exploitation, protection antivirus, etc.) à jour.

3. Assurez-vous d'installer toutes les mises à jour logicielles avant de vous connecter à Internet.

4. N'ouvrez jamais les pièces jointes d'e-mails provenant d'expéditeurs inconnus.

5. Téléchargez uniquement des logiciels et des applications depuis des sites officiels ou des magasins d'applications.

6. Faites des sauvegardes régulières et sécurisez-les en plus avec un mot de passe.

7. Les smartphones et les tablettes nécessitent également une protection antivirus, et les systèmes Mac et Linux ne sont pas non plus à l'abri des virus et des chevaux de Troie.

8. Ne vous contentez pas de cliquer par curiosité sur des titres accrocheurs et des articles sur des sites comme Facebook.

9. Activez le pare-feu sur votre ordinateur et votre routeur.

10. Utilisez des programmes supplémentaires tels que des bloqueurs de script, des bloqueurs de publicité .

11. Naviguez toujours et travaillez avec des droits d'utilisateur restreints, pas en mode administrateur.

Adresses utiles

https://cybermalveillance.gouv.fr
https://www.cnil.fr
https://www.arobase.org/

En savoir plus sur la sécurité
https://www.leblogduhacker.fr/

Conseils pour sécuriser les transactions bancaires en ligne

1. Votre banque ne vous demandera jamais, par courrier électronique ou par téléphone, de mettre à jour les détails de votre compte.

2. Pour les opérations bancaires en ligne, un programme antivirus doté d'une protection anti-phishing doit toujours être installé.

3. Gardez toujours tous vos programmes (navigateurs, plugins, systèmes d'exploitation, protection antivirus, etc.) à jour.

4. Installez toutes les mises à jour logicielles avant de vous connecter à votre compte bancaire en ligne.

5. Les règles de sécurité en vigueur pour les transactions bancaires en ligne via un smartphone ou une tablette sont les mêmes que pour un PC (mises à jour, protection AV, etc.).

6. Les opérations bancaires en ligne ne doivent être effectuées que sur vos propres appareils ou sur des appareils fiables.

7. Évitez les transactions bancaires en ligne via le Wi-Fi ouvert ou non sécurisé, par exemple dans les cafés ou les hôtels.

8. Pour les opérations bancaires, assurez-vous qu'il existe une connexion Internet sécurisée.

9. Lorsque vous accédez à votre compte bancaire, assurez-vous que personne ne regarde par-dessus votre épaule.

10. Concentrez-vous sur la minimisation des données et évitez de saisir vos coordonnées bancaires inutilement.

11. En cas de doute, contactez d'abord votre banque.

Astuces pour les mots de passe en béton.

1. Un mot de passe fort consiste en une combinaison de lettres minuscules et majuscules (az, AZ), de chiffres (0 à 9) et de caractères spéciaux (! @ # $% ^ * () _ + | ~ - = \ `{} []: "; '), et doit contenir au moins 10 caractères au total.

2. Évitez les mots de passe du dictionnaire - indépendamment de la langue, du dialecte ou du jargon.

3. Évitez les mots de passe contenant des informations personnelles (nom des membres de la famille / animaux de compagnie / date de naissance / etc.).

4. N'utilisez jamais un mot de passe que vous avez déjà utilisé par le passé.

5. Utilisez un mot de passe différent pour chaque site Web / application.

6. Évitez d'utiliser les fonctions «Mémoriser le mot de passe» dans le navigateur ou dans les applications.

7. Ne jamais enregistrer ou noter vos mots de passe en texte brut, que ce soit numériquement ou sur papier.

8. Choisissez des services utilisant une authentification à deux facteurs.

9. Les mots de passe sont faciles à retenir s'ils reposent par exemple sur un titre de chanson ou un dicton. Exemple: "**C**ela **p**eut **ê**tre **une f**açon **d**e **s**e **s**ouvenir" et le mot de passe pourrait être: "**CpE1fDsS** »

10. Utilisez un gestionnaire de mot de passe. Ceux-ci génèrent automatiquement des mots de passe forts, les enregistrent dans un trousseau et leur permettent d'être utilisés simultanément sur plusieurs appareils.

11. Même le mot de passe le plus fort reste incertain si vous répondez honnêtement à la question de récupération du mot de passe «Quel est le nom de votre animal favori».

Gestionnaires de mots de passe

Keepass, BitWarden, Dashlane