Quelques bonnes pratiques de sécurité sur le numérique

Si le numérique est un outil qui nous permet de réaliser de très nombreuses choses, il reste important de surveiller sa pratique au quotidien. En effet, même si les choses sont plus sécurisés qu'avant, la faille principale de sécurité reste la même: l'être humain. Et cela, les fraudeurs, pirates etc... le savent très bien.

Voici donc quelques conseils et bonne pratiques de sécurité.

Pour éviter les mails ou SMS frauduleux:

- **Ne pas agir dans l'urgence !** Les messages frauduleux **exploitent les faiblesses humaines.** Menace de perdre des droits, de risque de prison, de paiements en cas de non-réponse etc... Le premier instinct est d'essayer de résoudre le problème stressant qui nous est donné. Au contraire, **on va d'abord prendre du recul face à ce type de message.**
- **Réfléchir à la logique/le contexte du message**. Est-ce bien l'organisme qui prétend vous contacter qui le fait? Leur demande est-elle réaliste? L'organisme ferait-il ce genre de demande par mail/SMS ?
- En cas de doute: **N'appelez pas le numéro dans le message/ne cliquer pas sur le lien du message!** Contactez l'organisme/allez sur le site officiel selon les méthodes de contact / de connexion habituelles en cas de doute.
- **On ne télécharge/n'ouvre pas de pièces jointes d'un mail douteux!**

Pour sécuriser ses comptes:

- On évite de créer des comptes sur des sites où l'on n'a pas confiance envers le site.
- **Dans la mesure du possible, 1 compte = 1 mot de passe** (différent des autres).
- Si le compte n'est pas pour une démarche administrative, vous pouvez même mentir sur certaines informations qui ne vous semblent pas utiles au site de connaître (par exemple, la date d'anniversaire pour un compte sur MYTF1).
- **Pour être encore plus sécurisé, on peut changer certains mots de passe de temps à autre.**

Pour sécuriser ses données:

- On peut refuser les cookies.
- On peut utiliser la navigation privée.
- **On évite d'enregistrer ses identifiants dans le navigateur Internet.**
- **On pense bien à enregistrer ses données importantes sur différents supports** (sur une clé usb, un disque dur externe, un espace de stockage en ligne...).
- On peut aussi **synchroniser ses données avec certains services**, ou faire des sauvegardes complète si nécessaire.

SIEA CONSEILLER NUMÉRIQUE France services
Financé par GOUVERNEMENT Liberté Égalité Fraternité FRANCE RELANCE
Financé par l'Union européenne NextGenerationEU

Pour naviguer sur Internet en sécurité:

- J**e privilégie les connexions privées** (en wifi chez moi notamment) pour des actes plus sensibles (démarches administratives, bancaires...)
- Je n'utilise les wifis publics que pour des actions plus basiques, et j'évite d'entrer des identifiants sur le wifi public.
- **J'évite les sites qui ne sont pas en https (avec un cadenas)**.
- Les sites gouvernementaux ont majoritairement **".gouv.fr"** dans l'adresse du site
- Sur les réseaux sociaux, je n'écris pas n'importe quoi/**je fais attention à ce que je partage en ligne.**
- **Je fais attention à ce que je lis sur internet.** On se retrouve très vite dans des bulles d'informations qui ne vont que dans notre sens / on peut très vite prendre des actualités comme des faits en ne lisant que les titres des infos.
- Pour des achats en ligne, surtout entre particuliers, je préfère les méthodes proposées par les sites de ventes. Si je le souhaite, je peux mettre en place d'autres mesures de sécurité avec ma banque. **Attention aussi aux offres trop alléchantes !**
- Pour des achats avec des marques, **on s'assure d'être sur le site officiel de la marque pour plus de sécurité.**
- **Attention à ce que l'on télécharge sur son ordinateur !** Ne pas télécharger des fichiers dont on ne sais rien.

Que faire en cas de piratage ou actions malveillantes:

- **Si vous avez un antivirus, lancez une analyse de l'ordinateur.**
- Si vous pensez que quelqu'un pirate votre ordinateur, **pensez à la fois à prendre des photos, conservez des preuves, et en parallèle à vous déconnecter d'internet.**
- Vous pouvez signaler le piratage du compte au site sur lequel votre compte se trouve.
- **Vérifiez que l'adresse mail/le numéro de récupération sont bien les vôtres,** si vous avez encore accès au compte.
- **Si un compte a été piraté, on change bien sûr le mot de passe de tout les comptes avec le même mot de passe.**
- **Prévenir la banque / les proches si nécessaire**, si vous souhaitez éviter les risques de transactions à votre insu / que les pirates utilisent vos comptes pour essayer d'obtenir des informations de la part de vos connaissances.
- **Selon les situations, vous pouvez également porter plainte à la police/gendarmerie.**
- **En cas de besoin, amenez le matériel à un informaticien.**
- **Ne payez pas de rançon ! Cela ne débloquera rien.**
- Je peux me rendre sur le site "**cybermalveillance.gouv.fr**" pour plus d'infos selon le type de problème rencontré.

SIEA
CONSEILLER NUMÉRIQUE France services
Financé par
GOUVERNEMENT Liberté Égalité Fraternité
FRANCE RELANCE
Financé par l'Union européenne NextGenerationEU