Comment assurer votre sécurité numérique
Sur PC, smartphone et tablette

7 conseils de cybersécurité

- Wi-fi : changez toujours le mot de passe par défaut de votre routeur/modem
- Installez un logiciel antivirus sur l'ensemble de vos objets connectés à internet
- Vérifiez les permissions données aux applications et supprimez celles que vous n'utilisez pas
- Choisissez des mots de passe renforcés et différents pour vos comptes sur les réseaux sociaux
- Faites des copies de sauvegardes et mettez à jour régulièrement vos logiciels
- Sécurisez votre équipement avec des mots de passe, codes PIN, schémas ou informations biométriques
- Vérifiez les paramètres de confidentialité de vos comptes sur les réseaux sociaux

6 règles de sécurité pour les achats sur internet

- Achetez seulement auprès de vendeurs fiables et vérifiez les notations des clients
- Il est vivement recommandé de faire vos achats sur un site web disposant d'une sécurité « https » : en effet, il existe 2 types de sites internet. Ceux dont l'adresse commence par « http:// » et ceux dont l'adresse commence par « https:// ».
- Évitez de faire vos achats sur les sites en « http:// » et ne créez pas un compte sur un site lorsque L'Url commence par « http:// » car les informations (mot de passe, informations personnelles, informations bancaires ...) peuvent être interceptées par des tiers (attention, cette condition est nécessaire, mais pas suffisante).
- Réfléchissez à deux fois si une offre a l'air trop belle pour être vraie
- Utilisez vos cartes de crédit pour acheter sur internet pour une meilleure protection du consommateur
- Vérifiez vos comptes en banque régulièrement pour détecter toute opération suspecte

Soyez vigilants et évitez...

- D'ouvrir des liens et pièces jointes issus d'e-mails et Sms d'expéditeurs inconnus
- De transmettre vos numéros de compte ou de cartes bancaires
- D'acheter en ligne des produits qui semblent en rupture de stock partout ailleurs
- D'envoyer de l'argent directement à des personnes que vous ne connaissez pas
- De partager des informations qui ne proviennent pas de sources officielles
- De faire des donations à des associations caritatives sans vérifier auparavant leur authenticité

4 conseils pour la cybersécurité avec des enfants

- Vérifiez les paramètres de sécurité et de confidentialité des jeux connectés
- Changez le mot de passe par défaut et assurez-vous de la mise à jour des logiciels
- Utiliser le contrôle parental pour protéger l'activité connectée de vos enfants
- Parlez avec votre enfant de Cyber sécurité. Écoutez leurs expériences de connectés et expliquez leur l'importance d'être aussi en sécurité sur internet

Cypiée 20 route Napoléon 38119 Pierre-Châtel
Tel : 04 76 30 15 78 – 06 95 35 03 58
animateurcypiee@gmail.com www:cypiee.fr

Utilisez votre messagerie de façon sécurisée

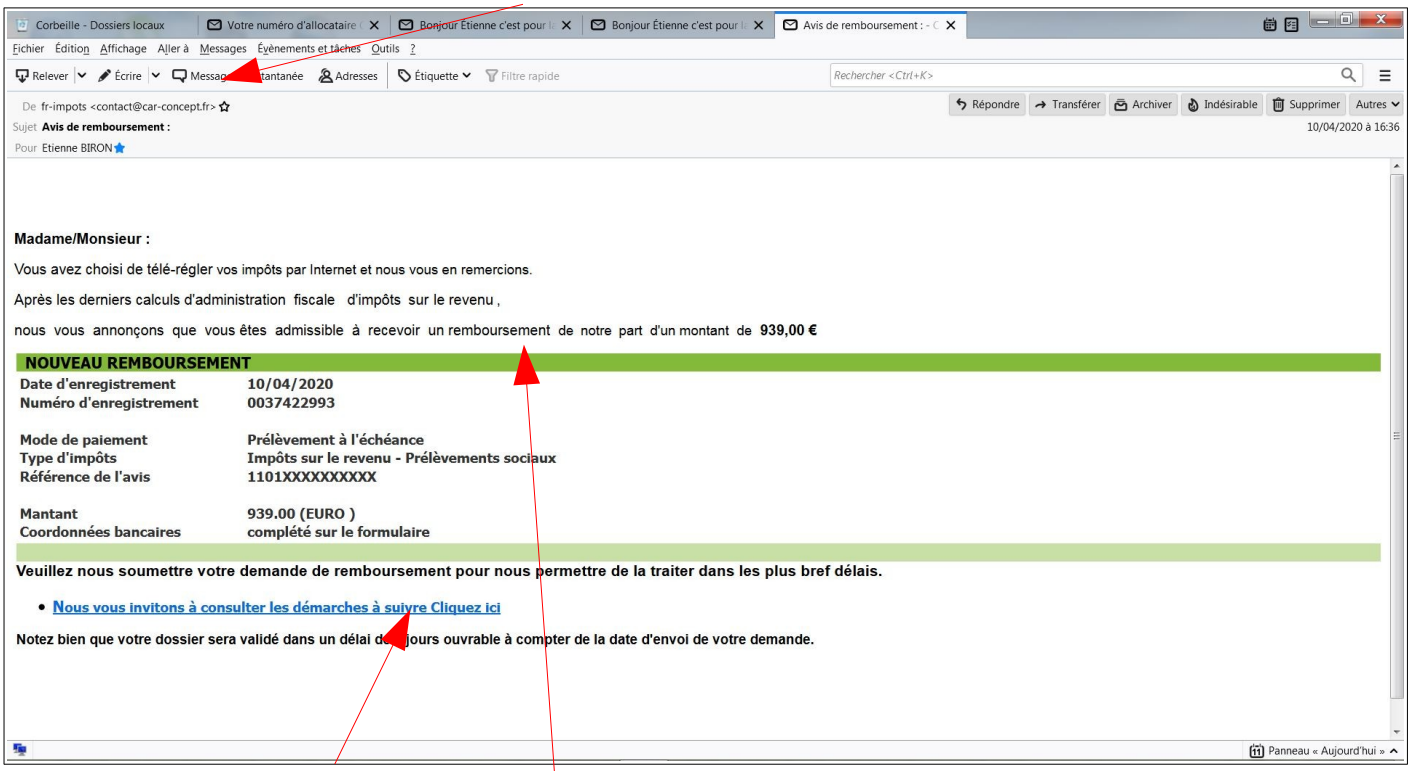
La messagerie électronique permet de communiquer facilement entre particuliers ou avec différents organismes. L'adresse électronique peut être utilisée pour créer un compte auprès d'un site marchand et recevoir des factures et des messages promotionnels. Mais, c'est également par le biais des courriers électroniques que des personnes malveillantes peuvent récupérer des informations confidentielles (codes d'accès, informations bancaires, etc). Un courriel n'est pas anodin !

Nos conseils :

- Lisez attentivement les informations contenues dans les courriels : interrogez-vous sur la pertinence et la crédibilité du contenu, sur l'identité de l'expéditeur et son langage, etc.
- Si un courriel vous semble douteux, ne cliquez pas sur les pièces jointes ou sur les liens qu'il contient : dans tous les cas méfiez vous des extensions de pièces jointes qui paraissent douteuses (exemples : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk…), et qui peuvent contenir des codes malveillants. N'ouvrez jamais un fichier se terminant par .exe
- Ne vous fiez pas aux éléments graphiques des courriels : en effet de nombreux courriels frauduleux utilisent les logos et chartes graphiques des administrations ou entreprises les plus connues. Voir figurer des logos qui paraissent officiels ne veut pas nécessairement dire qu'il s'agit d'un courriel officiel.

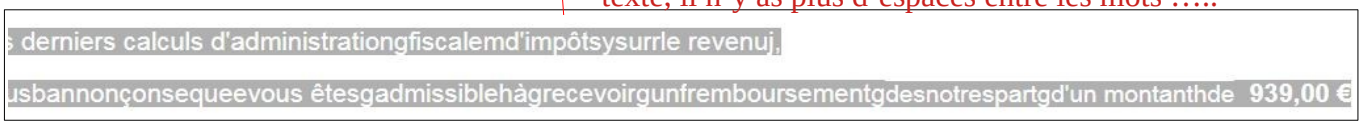
<u>Voici l'exemple d'un mail frauduleux :</u>

Adresse mail de l'expéditeur : contact@car-concept.fr ne ressemble pas à une adresse des impots



L'URL de ce lien est bizzare !
Surtout ne pas cliquer sur ce lien !

Voici ce qui apparaît lorsqu'on sélectionne une partie du texte, il n'y as plus d'espaces entre les mots …..



Méfiez-vous des faux sites administratifs

Méfiez-vous des faux sites administratifs. En effet de nombreuses arnaques font tout pour tromper le consommateur et prendre l'apparence d'un site officiel. Généralement ces sites sont souvent des sites commerciaux qui proposent de réaliser pour vous des démarches administratives (demande d'extrait d'acte de naissance, consultation de points sur le permis de conduire, etc.) moyennant rémunération alors que les sites officiels de l'administration proposent les mêmes prestations gratuitement. Si ces types de services peuvent être légaux, soyez vigilant sur les services qu'ils proposent.

Nos conseils :

- Sachez reconnaître les faux sites : les sites officiels de l'administration française se terminent par « .gouv.fr » ou « .fr » et jamais par « .gouv.org » ou « .gouv.com ».
- Consultez le site service-public.fr : pour être redirigé vers le site adéquat en fonction de la demande.
- Ne vous fiez pas aux premiers résultats des moteurs de recherche : car ils ne correspondent pas toujours aux sites officiels.
- Vérifiez l'identité du site et ses mentions légales avant de réaliser le moindre paiement.

En cas d'incident, contactez cybermalveillance.gouv.fr

Nos conseils :

- Si vous êtes victime d'un incident de cybersécurité, connectez-vous sur le site cybermalveillance.gouv.fr qui permet d'établir un diagnostic précis de votre situation ainsi qu'une mise en relation avec des spécialistes et organismes compétents proches de chez vous. Le site propose aussi des outils et des publications dispensant de nombreux conseils pratiques.

- Il est possible également de signaler un contenu illicite sur le site internet-signalement.gouv.fr.