LIENS UTILES

Vous pensez être victime d'une escroquerie ?
Signalez votre cas sur internet-signalement.gouv.fr

Vous avez donné votre numéro de carte prépayée ?
Appelez le service client PCS Card : 01 80 96 19 61

Vous avez envoyé un colis au fraudeur ?
Bloquez le colis à la Poste en appelant le 36 31

En cas de doute sur un email Paypal
Transférez-le à spoof@paypal.fr

Vous avez repéré un site de phishing ?
Signalez-le sur www.phishing-initiative.com

Vous avez reçu une tentative d'escroquerie par mail ?
Appelez Info Escroqueries au 0811 02 02 17

Pour toute question,
la Gendarmerie Nationale reste à votre écoute.

Gendarmerie nationale
Une force humaine

CONSEILS POUR UNE UTILISATION D'INTERNET SANS DANGER

Une utilisation maîtrisée est une utilisation sans danger

1) Avant de surfer sur internet, vérifiez la mise à jour du système d'exploitation et de l'antivirus de votre ordinateur, ainsi que l'activation du pare-feu.

2) Vous pouvez effectuer des achats via internet en utilisant des sites sécurisés
Votre banque peut vous proposer un service d'ecard, qui vous permet d'effectuer un achat unique sur le net.

3) Pensez à changer régulièrement vos mots de passe, n'ayez pas le même pour toutes vos connections. N'hésitez pas à utiliser les lettres, les chiffres et les symboles, ainsi qu'alterner les majuscules et les minuscules.
Exemple : 7éTjeVàPariS6 (cet été je vais à Paris 6)

4) Concernant les arnaques aux petites annonces :

- Méfiez-vous des offres trop alléchantes et des propositions de paiement par Paypal ou Western Union
- N'envoyez jamais vos coordonnées bancaires, ni le code des tickets PCS
- N'expédiez jamais un colis avant que le paiement ne soit validé (chèque, virement, …)
- Soyez vigilants avec les demandes provenant de l'étranger surtout lorsque la personne ne vous contacte que par email
- Recherchez l'email de votre interlocuteur ou son identité sur un moteur de recherche pour vérifier s'il est référencé sur des sites anti-arnaques
- Si vous publiez une annonce, masquez les informations qui pourraient être utilisées pour usurper votre identité.

5) Concernant les emails :

- N'ouvrez pas de pièce jointe si l'expéditeur vous est inconnu
- Si vous recevez un email d'un organisme connu (CAF, Impôts, EDF, …) pour vous rendre de l'argent, ne cliquez pas sur le lien, il vous sera demandé de rentrer votre identité complète ainsi que vos coordonnées bancaires.
- Si vous êtes victime de rançongiciel : ne payez pas, déconnectez-vous d'internet et faire une restauration du système.

6) N'envoyez pas de photos ou de vidéos intimes. Faites très attention au cybersexe et aux chantage de conversation Skype.

7) Les enfants et les adolescents constituent une cible privilégiée, protégez-les :

- Des messages intrusifs et dangereux
- Des sites internet pour adultes ou illégaux, voire payants
- Des conversations dangereuses
- Des risques harcèlement en ligne

Pensez également à votre e-réputation : toutes vos publications sur les réseaux sociaux ne vous appartiennent plus.

8) Faites régulièrement des sauvegardes des données importantes sur votre ordinateur.