



Lutte contre la cybercriminalité



Les utilisateurs d'ordinateurs sont de plus en plus nombreux et ces ordinateurs sont généralement connectés à des réseaux, en particulier à l'Internet. Si ces utilisateurs ne prennent pas un minimum de précautions, leurs ordinateurs peuvent être facilement attaqués. Avec le développement des nouvelles technologies, la délinquance s'adapte et la cybercriminalité ne cesse de croître. Aujourd'hui de plus en plus de particuliers internautes font des achats en ligne et certains participent à des ventes aux enchères entre particuliers. Conseils et astuces pour éviter de vous faire spolier.

Récupération frauduleuse de données bancaires

Exemple : Vous recevez un mail de votre banque vous demandant votre identifiant de connexion et votre mot de passe de consultation de votre compte en ligne ou votre numéro de carte bancaire avec votre code confidentiel. Le mail vous explique que votre banque a besoin de mettre à jour vos données de connexion.

VOTRE BANQUE NE VOUS DEMANDERA JAMAIS VOS COORDONNÉES BANCAIRES

Achat d'un bien sur internet

Risques : L'objet payé risque de ne pas être livré.

Solutions : Choisir un mode de paiement par PAY PAL ou l'utilisation d'une carte bancaire à usage unique. Privilégier les achats sur des sites français connus.

Attention aux trop bonnes affaires. Éviter les mandats en espèces via les organismes tel que western union ou mandat cash. Pour les objets de valeur il faut privilégier une transaction en face à face, rencontrer le vendeur et voir le bien.

Escroquerie

Exemple : Vous recevez un mail intitulé

« urgent et confidentiel », il émane d'une veuve d'officier, d'un médecin, d'un avocat... Il vous demande de l'aide pour sortir une très grosse somme illégalement de son pays. En échange vous toucherez une commission sur cette somme. Il vous suffit de donner votre numéro de compte en banque afin que l'argent y soit versé.

NE JAMAIS RÉPONDRE À CE TYPE DE PROPOSITION

9 idées pour se protéger

- 1- Utiliser un antivirus et un pare-feu à jour.
- 2- Se méfier des trop belles affaires. Il s'agit de faux sites de vente.
- 3- Ne conclure aucun achat important sans rencontrer le vendeur et avoir vu et essayer le bien.
- 4- Se renseigner sur le vendeur avant d'acheter, grâce aux moteurs de recherche.
- 5- vérifier le panier qu'il ne contienne pas d'autres articles avant de valider la commande.
- 6- Faire une copie d'écran et garder une trace de toutes mes opérations en ligne
- 7- Refuser d'effectuer un transfert de fond ou un virement bancaire à l'étranger qui n'offre absolument aucune garantie.
- 8- Porter plainte à la Gendarmerie en cas d'escroquerie, piratage de comptes de messagerie, extorsion d'argent pour débloquer un ordinateur etc..... Vous pouvez également utiliser la plateforme de signalement et de dépôt de plainte en ligne grâce au dispositif THESEE.
- 9- Consulter les conseils pratiques à retenir sur le portail de la sécurité informatique.

<https://cyber.gouv.fr/> (site de l'ANSSI)