

CONSEILS POUR LUTTER CONTRE LA CYBERCRIMINALITE

Conseils et astuces pour éviter de vous faire spolier

Avec le développement des nouvelles technologies, la délinquance s'adapte elle aussi et la cybercriminalité ne cesse de croître. Aujourd'hui, 52% des particuliers internautes font des achats en ligne et 35% participent à des ventes aux enchères entre particuliers.

RÉCUPÉRATION FRAUDULEUSE DE DONNÉES BANCAIRES

Définition : Récupération d'informations bancaires

Solutions : Ne jamais donner les informations bancaires ni par téléphone ni par internet lorsque vous n'êtes pas à l'origine de la démarche.

Saisir l'adresse URL d'accès au service pour être sûr de ne pas être sur une copie de la page d'un site.

Vérifier que le navigateur est en mode sécurisé (HTTPS).

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 COORDONNEES BANCAIRES

ESCROQUERIE A LA NIGERIANNE

Définition : Envoi par email d'une demande d'aide en utilisant la sensibilité ou la cupidité des gens.

Solution : Ne pas répondre ... Si vous voulez aider une œuvre caritative il faut toujours passer par un organisme officiel.

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 REPONDRE A CE TYPE DE PROPOSITION

LES MULES

Définition : Accepter que de l'argent transite sur votre compte en échange d'une commission.

Conséquences : Passible de 5 ans de prison

Exemple : Vous recevez un email qui vous demande le plus souvent pour des raisons humanitaires d'accepter sur votre compte, dont vous devez fournir les références, le virement d'une somme d'argent généralement faible, que vous devrez ensuite reverser sur un autre compte. L'escroc a obtenu ce qu'il désirait en utilisant vos comptes pour blanchir son argent.

NE JAMAIS REPONDRE A CE TYPE DE PROPOSITION

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.

Essayer de contacter par téléphone le vendeur et recouper les infos afin de les vérifier.

Se méfier des e-mails attractifs.

Eviter les mandats en espèce via les organismes tel que Western Union

Pour les objets de valeur, il faut privilégier une transaction en face à face, rencontrer le vendeur et voir le bien.

VENTE D'UN OBJET PAR INTERNET

Risques : Ne pas recevoir le paiement

Solutions : Attendre d'avoir encaissé le règlement et d'être sûr que l'argent est bien sur le compte, pour les transactions avec la Western Union, attendre au minimum une semaine avant de livrer le bien vendu.

Exemple : Vous avez déposé une annonce sur un site internet pour vendre un objet de valeur. Une personne domiciliée à l'étranger vous contacte par mail et se dit intéressée pour acquérir le bien. L'acheteur vous envoie alors un chèque. Vous déposez le chèque à votre banque, laquelle crédite la somme sur votre compte. Rassuré, vous faites parvenir le bien à l'acheteur. Quelques jours plus tard, votre banque vous informe que le chèque est faux.

LES SOCIETES EN LIQUIDATION OU 100% FICTIVES

Risques : Un cybermarchand en liquidation judiciaire peut maintenir son site ouvert et ainsi encaisser l'argent sans jamais vous envoyer vos achats.

Solutions : Avant tout achat, taper dans un moteur de recherche « le nom de la société + arnaque » de nombreux résultats apparaissent.

8 IDEES POUR SE PROTEGER

1. utiliser un antivirus et un pare-feu à jour
2. se méfier des trop belles affaires
3. ne conclure aucun achat important sans rencontrer le vendeur et avoir vu et essayé 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 ses opérations en ligne
7. refuser d'effectuer un transfert de fonds ou un virement bancaire à l'étranger qui n'offre aucune garantie
8. porter plainte à la gendarmerie en cas d'escroquerie

RIEN NE REMPLACERA LA VIGILANCE ET LA PRUDENCE. VOUS ETES HONNETE MAIS RIEN NE PROUVE QUE VOTRE INTERLOCUTEUR L'EST.