9 décembre 2019

Prévention contre la cybercriminalité

Lieutenant CASSAING, commandant la Communauté de Brigades de Thiers

Gendarmerie nationale

Introduction

Le numérique n'est pas une évolution ni une révolution mais une métamorphose.

Avec le développement des nouvelles technologies, la délinquance s'adapte elle aussi et la cybercriminalité ne cesse de croître. Aujourd'hui 80% des internautes effectuent des achats en ligne.

Vol de données

Objectif : *Récupération frauduleuse de données (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 directement l'adresse URL *d'accès au service pour être sur de ne pas être sur une copie de la page d'un site*

→ ne pas cliquer sur les liens ni ouvrir les pièces jointes

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

VOTRE BANQUE NE VOUS DEMANDERA JAMAIS VOS COORDONNÉES BANCAIRES

Gendarmerie nationale

Escroqueries

La fraude 419

Définition : Envoi par **e-mail** 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 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 A CE TYPE DE PROPOSITION

Gendarmerie nationale

Blanchiment d'argent

Les mules

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

Conséquences : Passible de **5 ans d'emprisonnement**

Exemple : Vous recevez un e-mail 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 à obtenu ce qu'il désirait en utilisant vos comptes pour blanchir son argent.

NE JAMAIS RÉPONDRE A CE TYPE DE PROPOSITION

Escroqueries

Achat d'un bien sur Internet

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

Solutions :

- Choisir un **mode de paiement sécurisé** (ex : PAY PAL ou 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**
- **Éviter** les mandats en espèce via les organismes tel que **western union** ou les cartes prépayées **PCS**
- Pour les objets de valeur il faut **privilégier** une transaction en **face à face**, rencontrer le vendeur et voir le bien.

Gendarmerie nationale

Escroqueries

Vente d’un bien sur Internet

Risques : Ne pas recevoir le paiement

Solutions : Attendre d'avoir **encaisser le règlement** et d'être sur que l'argent est bien sur le compte.

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 ce 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 faite parvenir le bien à l'acheteur. Quelques jours plus tard, votre banque vous informe que le chèque est faux.

Escroqueries

Les sociétés en liquidation ou 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 »** afin de vérifier si de nombreux résultats apparaissent.

Les bonnes pratiques

1/ Complexifier son **mot de passe** (majuscules, minuscules, caractères spéciaux)

2/ Effectuer les **mises à jour** sans attendre

3/ Utiliser un **compte utilisateur** et **non administrateur**

4/ Effectuer des **sauvegardes régulières** de vos données

5/ Ne **pas utiliser** de clés **USB** ou de réseau **Wi-Fi** d'origine **inconnue**

6/ Appliquer les **mêmes règles** sur un **ordinateur**, un **smartphone** ou une **tablette**

7/ Faire preuve de **discrétion en déplacement**

8/ Se **méfier** des **e-mails**, **pièces jointes** et **liens**

9/ Rester **prudent** lors de **téléchargements** de logiciels

10/ Faire ses achats sur un site HTTP**S**

11/ **Séparer** vos **usages** professionnels et personnels

12/ **Limiter** la **communication** de ses **données** personnelles

Merci de votre attention

Avez-vous des question ?