AIDE-MEMOIRE ANTI-ARNAQUES - *www.eponaclic.fr - 03-2024*

LES ARNAQUES SUR INTERNET

Faites vos achats sur des sites de confiance, dont l'adresse commence par **https**. Au moment du paiement les icônes du navigateur (cadenas, clé) sont un gage de sécurité

Ne répondez pas au mail d'un établissement bancaire vous demandant vos identifiants de connexion à votre compte ou vos coordonnées bancaires

Si un mail vous paraît douteux, ne l'ouvrez pas et supprimez-le, ce pourrait être un virus

Si vous êtes victime d'une escroquerie sur Internet, contactez votre banque et déposez plainte sur **THESEE** ou auprès de la Gendarmerie

LE VOL A LA FAUSSE QUALITÉ

Si une personne se présente à votre porte, n'ouvrez-pas, utilisez l'entrebâilleur ou le judas

Si vous ne connaissez pas la personne, demandez lui de décliner son identité

Des démarcheurs peuvent être déguisés en faux agents, demandez-leur de présenter leur carte professionnelle. En cas de doute, ne laissez pas entrer et appelez le **17**

Accompagnez la personne dans ses déplacements, elle pourrait vous dérober des objets

Ne divulguez pas où sont placés votre argent, bijoux ou autres objets de valeur

LE DEMARCHAGE A DOMICILE

Ne signez aucun document qui ne vous semble pas clair et faites vous assister d'un proche, ne restez pas seul

Pour tout démarchage à domicile, vous disposez d'un délai de rétractation de **14 jours**. Ne payez rien immédiatement et surtout pas en espèces

Si vous faites entrer une personne chez vous, essayez de solliciter la présence d'un voisin

Ne rappelez pas un numéro que vous ne connaissez pas il pourrait s'agir d'un numéro surtaxé destiné à vous faire payer des communications abusives

AIDE-MEMOIRE ANTI-ARNAQUES - *www.eponaclic.fr - 03-2024*

1 - DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE

Un mot de passe c'est comme une clé propre à chaque porte, elle protège de l'intrusion.
Si on se fait voler un mot de passe utilisé pour différents sites web ou applications, ils pourront tous être piratés !

BONNES PRATIQUES

Utiliser des mots de passe longs, complexes et surtout différents pour chaque compte.
Changer le mot de passe sur le site ou le compte concerné au moindre doute.
Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

2 - FAIRE LES MISES A JOUR DES APPAREILS SANS TARDER

Les failles de sécurité des logiciels, applications et matériels sont comme des portes laissées ouvertes pour les pirates.
Ils peuvent les utiliser pour accéder aux données personnelles et les voler.

BONNES PRATIQUES

Faire les mises à jour des logiciels, applications et appareils, dès qu'elles sont proposées pour corriger leurs failles de sécurité.
Activer les options de mises à jour automatiques chaque fois que c'est possible.

CYBER REFLEXES
SE PROTEGER SUR INTERNET

3 - EN DIRE LE MOINS POSSIBLE SUR SON IDENTITÉ EN LIGNE

Publier et partager ses données personnelles sur Internet (nom, prénom, adresse mail, photos, vidéos, ...) peut les exposer à une utilisation malveillante.

BONNES PRATIQUES

Éviter de divulguer des données personnelles et celles de ses connaissances.
Vérifier les paramètres de confidentialité de ses comptes pour définir ce qui peut être visible par les autres.

4 - FAIRE UNE COPIE DE SES DONNÉES EN LIEU SÛR

Copier ses données (documents, images, carnets d'adresse, ...), c'est les sauvegarder pour éviter de les perdre en cas de piratage, de vol, de panne ou de casse de ses appareils.

BONNES PRATIQUES

Penser à faire régulièrement des sauvegardes de ses données sur un autre support (clé USB, disque externe, stockage en ligne, ...) pour pouvoir les retrouver en cas de problème.

5 - SE MÉFIER DES MESSAGES INATTENDUS ET ALARMANTS

L'hameçonnage ou phishing, ce sont des messages (mails, SMS, réseaux sociaux) ou appels d'escrocs qui se font passer pour un organisme familier (administration, banque...). Ces arnaques visent à voler des informations personnelles et à escroquer.

BONNES PRATIQUES

Toujours se méfier et ne pas se précipiter pour cliquer ou répondre.
Ne pas communiquer d'information sensible ou personnelle suite à un message ou un appel téléphonique.
Vérifier toujours l'information par soi-même, en se connectant à son compte sur le service concerné.

6 - ÉVITER LES CONTENUS PIRATES ET NON-OFFICIELS

Des virus qui peuvent pirater ses appareils ou ses comptes sont souvent présents dans les logiciels piratés, les sites de téléchargement, ...

BONNES PRATIQUES

Ne pas télécharger des contenus illégaux ni des solutions non officielles.
Installer uniquement des applications depuis les sites officiels des éditeurs.