♦ Conduite de prévention à tenir et arnaques sur le net

Le constat est clair, les personnes âgées sont les premières cibles des vols par ruse. Pour éviter toute déconvenues, il faut savoir être prudent. Vous trouverez ci-après quelques conseils que nous vous conseillons de suivre scrupuleusement.

Visite impromptue

Une personne vient frapper à votre porte, elle vous indique qu'elle est salariée d'un service sociale, de la mairie de votre commune et qu'elle souhaite faire le point avec vous, par rapport aux aides qui vous sont accordées.

Que faire ?
Si vous ne connaissez pas cette personne, laissez votre porte entrouverte avec l'aide d'une chaine ou d'un entrebâilleur de porte. Demandez-lui qu'elle justifie de son identité et qu'elle vous présente sa carte professionnelle. Le mieux est de contacter par téléphone, l'organisme qu'elle est censée représenter, ne lui demandez pas un numéro de téléphone de contact, elle pourrait vous fournir le numéro d'un complice !!

Conseil
Vous avez un voisin ou une voisine en qui vous avez confiance, un enfant ou un ami qui habite à proximité. Contactez un de ces proches car il est préférable de ne pas la recevoir seule.

Une personne travaillant pour un organisme social, ne verra aucun inconvénient à ce qu'un proche soit présent, bien au contraire !!

Les faux plombiers…
Le risque est accrue pour les personnes vivants en appartement. Effectivement, si vous avez un problème de plomberie ou d'électricité dans une maison, vous êtes la seule personne à demander une intervention. En appartement, ils peuvent inventer un stratagème comme une fuite d'eau chez le voisin du dessous. A savoir, que si votre voisin a effectivement une fuite d'eau, vous seriez la première personne informée car en général, il se serait déplacé en personne pour vous demander si vous n'aviez rien remarqué à votre domicile.

Dans le cas de travaux prévus par la copropriété ou le bailleur social, une affiche est installée dans le hall de l'immeuble.

Conseil
Si un plombier intervient chez votre voisin, c'est que celui-ci est présent. Avant d'ouvrir votre porte, téléphonez à votre voisin pour lui demander confirmation de cette intervention.

Retrait d'argent

En début de mois, vous allez à la banque effectuer un retrait d'espèces pour vos achats courants. Soyez discrets en indiquant le montant que vous souhaitez au guichetier. Si c'est un retrait au distributeur, assurez vous que personne ne vous observe et surtout **faites-vous accompagner**.

♦ Les arnaques sur le net

Le phishing

Le phishing (hameçonage en français) est une technique par laquelle des cybercriminels se font passer pour des organismes financiers ou de grandes sociétés en envoyant des courriels frauduleux. Ils récupèrent des mots de passe de comptes bancaires ou des numéros de carte de crédit pour détourner des fonds.

Quels sont les types d'organismes les plus copiés ?
Les banques, les sites de paiement en ligne (type Paypal), les assurances, les fournisseurs internet ou mobile, les sites de vente par correspondance (eBay), les réseaux sociaux, les organismes comme la CPAM ou la CAF… En fait, presque tous les sites où pourraient être enregistrés des codes confidentiels, des numéros de compte…

Votre banque, votre fournisseur d'accès ou les services publics ne vous demanderont JAMAIS votre numéro de compte, votre mot de passe par courriel.

Que faire ?
Vous avez un doute sur le contenu d'un courriel ? Ayez les bons réflexes : Ne répondez pas à ce courriel, ne cliquez sur aucun des liens proposés, supprimez-le.

Dans le doute, contactez l'expéditeur officiel du message en vous déplaçant en agence, en appelant votre conseiller ou en passant par le site officiel, pour déterminer s'il est bien l'expéditeur du message et s'il est nécessaire de réactiver un compte ou de procéder à une modification de données.

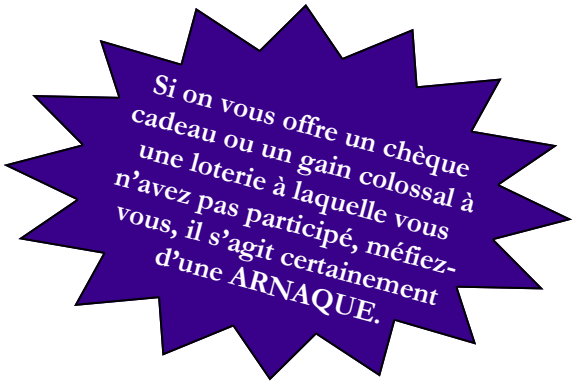
Le SCAM

Le SCAM est une escroquerie répandue sur Internet. Cette fraude abuse de la crédulité des victimes en utilisant les messageries électroniques pour leur soutirer de l'argent.

La version la plus connue se présente généralement sous la forme d'un spam (courrier indésirable) dans lequel une personne affirme posséder une importante somme d'argent et fait part de son besoin d'utiliser

un compte existant pour transférer rapidement cet argent…

Le scameur peut vous demander de lui envoyer l'argent par chèque ou, le plus souvent, par transfert (type Western Union). Il peut même vous demander vos informations bancaires… Ne donnez rien !



Autres exemples
Vous recevez un courriel d'un riche héritier dont les fonds ont été bloqués et qui vous promet 50% de la somme totale, si vous lui versez plusieurs centaines d'euros de suite…
Il existe aussi des variantes sur les sites de rencontres ou la messagerie instantanée (Windows Live ou Skype) où une personne, entame une discussion qui peut durer plusieurs semaines. De fil en aiguille, cette personne vous avoue tomber amoureuse, mais elle a des problèmes financiers, est malade ou vous demande de l'aide pour venir s'installer.

Que faire ?
Comme pour le phishing, ne répondez pas au courriel, ne le transférez pas et supprimez-le immédiatement. Internet est une source inépuisable d'informations, malheureusement certains y voient une façon rapide, et malhonnête, de s'enrichir.

Dénoncer ces pratiques est un acte citoyen

www.internet-signalement.gouv.fr a été mis en place par l'état et vous permet de signaler ces actions frauduleuses. Votre signalement sera traité par un service de police judiciaire spécialisé dans ces questions : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

www.phishing.fr est un site d'information sur le phinshing

www.phishing-initiative.com, créée par l'éditeur de logiciels Microsoft, le site de paiement en ligne Paypal et la société informatique française Cert-Lexci, permet de lutter contre les sites frauduleux. Les internautes peuvent ainsi signaler en quelques clics les sites francophones de phishing.

Vous avez répondu à un courriel frauduleux

Le premier réflexe est de porter plainte auprès du commissariat ou de la gendarmerie la plus proche. **Vous ne devez ni avoir honte, ni avoir peur !**

Cessez toute communication avec le fraudeur. Vous recevrez peut-être des messages de menace, voire des faux courriels de la police, de la gendarmerie. N'en tenez pas compte, ceci est une pratique courante des cybercriminels pour accentuer leur emprise sur leur victime.

La police, ou tout autre organisme judiciaire ne vous contactera JAMAIS par courriel.

Les Virus

Les chevaux de Troie :
Le cheval de Troie a pour objectif de récolter les informations sensibles ou de laisser « une porte ouverte » sur l'ordinateur. Ainsi, le pirate peut en prendre le contrôle. Il est transmis par les virus.

Le virus « Gendarmerie » :
Vous allumez votre ordinateur et hop… une page « officielle » apparait… un message provenant apparemment de la Gendarmerie Nationale, voir d'Interpol, pour certaines variantes, évoquent plusieurs infractions dont :
- Le téléchargement illégal de contenus

- Le partage de fichiers protégés par le droit d'auteur
- Le spam
- La diffusion de matériel pornographique impliquant des mineurs

Celui-ci vous invite à payer une amende pour débloquer votre ordinateur.

Apparu en 2011, ce message est un virus bloquant le démarrage de votre système d'exploitation (Windows) et vise à vous faire payer cette « amende » allant jusqu'à plusieurs centaines d'euros. **Bien entendu, votre ordinateur ne sera pas débloqué pour autant…**

Que faire ?

Ne paniquez pas ! Ne payez pas !

Malheureusement, sans connaissances techniques, il vous sera difficile, voir impossible, de retirer ce virus. Nous ne pouvons que vous conseiller de vous rapprocher d'une personne, un ami, de la famille...ayant suffisamment de bases en informatique, ou d'apporter votre ordinateur dans un magasin spécialisé. Cette solution vous coûtera une trentaine d'euros, certainement moins que la fausse amende demandée.

Acheter sur Internet

Avec Internet, l'achat n'a jamais semblé aussi simple et rapide… Malheureusement, il est plus facile pour les cybercriminels de voler des informations confidentielles.
De manière générale, on peut constater qu'un site est sécurisé en observant la barre d'adresse (en haut). Si celle-ci commence par https (s pour secure), le site est sécurisé. Un petit cadenas peut aussi être observé.

Un site doit toujours vous proposer ses CGV (Conditions Générales de Vente). Elles doivent mentionner sa raison sociale, son numéro d'identification (SIREN), les moyens de contact et de paiement…
Ne transmettez pas de données bancaires à des sites qui vous inspirent pas confiance ou qui ne donnent aucune indication sur la société.
Ne donnez jamais en ligne votre code confidentiel à quatre chiffres, celui-ci sert exclusivement pour les paiements en magasin.