Lorsque vous lisez un courrier électronique ou surfez sur Internet, vous devez vous préoccuper des arnaques qui essayent de voler vos informations personnelles, votre argent, ou les deux. La plupart de ces manœuvres frauduleuses sont connues sous le nom de « **arnaques par hameçonnage** »

Comment reconnaître ces arnaques ?

De nouvelles escroqueries apparaissent tous les jours. Vous pouvez apprendre à les reconnaître avec certains signes révélateurs.

Ainsi, méfiez-vous des mails pouvant contenir :

►**Des messages alarmistes et des menaces de fermeture de comptes, voir blocage de votre ordinateur** → on vous fait peur en vous demandant de régler rapidement un impayé ou de payer une amende...

►**Des demande de vérifications de vos coordonnées bancaires** → on vous demande de confirmer vos coordonnées bancaires (chose que les banques et les organismes officiels ne le font jamais !)

►**Des promesses d'argent avec peu ou sans effort** → on vous demande vos coordonnées bancaires pour le virement d'un salaire ou d'une indemnité (parfois en vous faisant parvenir de faux contrats de travail) ou pour toucher un gain de loterie...

►**Des affaires qui semblent trop belles pour être vraies** → on vous demande de verser une avance ou la totalité du prix d'un objet pas cher afin d'en profiter avant les autres, ou de verser des fonds pour aider à récupérer un héritage moyennant un pourcentage...

►**Des demandes de donation à une œuvre caritative après une catastrophe qui a été annoncée dans les médias** → là aussi on vous demande de faire un virement alors que le don est volontaire et non sollicité par mail...

►**Une mauvaise grammaire et des fautes d'orthographe** → souvent les faux mails ou les sites dit « miroirs » (copie d'un site bancaire ou autre) sont établis depuis certains pays africains de manières grossières...

►**Un lien qui ne correspond pas à l'adresse cachée** → le fait de rester (mais sans cliquez) avec le pointeur de la souris sur le lien proposé révèle l'adresse Internet réelle, comme l'info-bulle montrée ci-dessous (selon votre navigateur, elle peut aussi apparaître sur la partie inférieure de la fenêtre). Si la chaîne de numéros secrets ne ressemble en rien à l'adresse Internet de l'entreprise : c'est un signe suspect.

*Depuis 2002, la gendarmerie bénéficie d'enquêteurs spécialisés , dénommés **N-TECH**, affectés en unités de recherches. Ces « cybergendarmes" peuvent apporter leur concours et leur expertise aux unités territoriales.*

*La communauté de brigades de SAINT-MARTN D'AUXIGNY dispose d'un **correspondant N-TECH** qui est à même de répondre aux premières sollicitations des autres gendarmes sur le terrain.*

Conseils pour prévenir les actes de délinquance

Fiche d'informations

Arnaques par courriel ou site Web : Comment se protéger ?

Ce qu'il faut faire si vous pensez avoir été victime d'une escroquerie :

Si vous pensez avoir répondu à une arnaque par hameçonnage avec des informations personnelles ou financières, prenez ces mesures pour minimiser les dommages :

►Changez les mots de passe ou les PIN de tous vos comptes en ligne dont vous pensez qu'ils peuvent être affectés.

►Placez une alerte de fraude sur vos rapports de crédit. Vérifiez auprès de votre banque ou de votre conseiller financier si vous n'êtes pas sûr de la marche à suivre pour faire cela.

►Contactez la banque ou le commerçant en ligne directement. Ne suivez pas le lien dans le courrier électronique frauduleux.

►Si vous savez qu'un compte quelconque a été visité ou ouvert frauduleusement, fermez-le.

►Vérifiez régulièrement vos relevés bancaires ou de cartes de crédit pour traquer tout débit inexpliqué ou toute opération que vous n'avez pas formulée.

En cas de dépôt de plainte :

Ne pas effacer les mails frauduleux car l'exploitation des codes sources peut permettre aux enquêteurs de remonter jusqu'à ordinateur à l'origine de l'arnaque.

Comment protéger son ordinateur ?

►N'installez que les logiciels indispensables à vos activités : Internet est plein de logiciels pratiques ou amusants, à télécharger gratuitement : mini-jeux, utilitaires, etc. Il s'agit parfois de véritables virus ou logiciels espions.

►Téléchargez à partir de sites connus : méfiez-vous des sites inconnus qui proposent de télécharger des logiciels et des patchs. Parfois, ils cachent des programmes malveillants en leur donnant le nom des applications que vous recherchez.

►Installez un antivirus, un pare-feu et un anti-espiogiciels : l'antivirus analyse les contenus de votre ordinateur et ce que vous recevez pour détecter les programmes malveillants. **Le pare-feu** ou « firewall » vous protège en temps réel des tentatives d'intrusion car certains pirates de l'Internet passent leur temps à chercher des ordinateurs vulnérables, non protégés contre les intrusions, comparables à une maison dont la porte d'entrée serait grande ouverte. **L'anti-espiogiciel** ou « anti-spyware » analyse les contenus de votre ordinateur pour détecter les programmes espions.

►Mettez régulièrement à jour votre système d'exploitation : les plus connus sont Linux et Windows. Faites des mises à jour manuelles ou automatiques, en les téléchargeant depuis le site de l'éditeur de votre système d'exploitation. Les navigateurs Internet comme Internet Explorer, Netscape, Firefox, etc... doivent être également mis à jour afin d'être plus résistants face aux nouvelles menaces.

►Ne répondez jamais à un spam : vous seriez dès lors identifié comme une adresse valide.

►Méfiez-vous des pièces jointes : n'ouvrez jamais les pièces jointes des messages provenant d'expéditeurs inconnus ou celles des messages provenant d'expéditeurs connus, quand vous trouvez le message trop impersonnel (certains virus utilisent le carnet d'adresse de vos amis). Vous pouvez installer un **logiciel anti-spam** sur votre ordinateur. Signalez les spams que vous recevez à http://www.signal-spam.fr .

►Qu'est-ce qu'un botnet ?

Ce sont des réseaux d'ordinateurs reliés entre eux après leur infection par un logiciel malveillant. Si votre ordinateur fait partie d'un botnet, il peut réagir à votre insu et de manière transparente, aux ordres donnés par des criminels. Par exemple, l'ordre pourra être d'envoyer du spam, véhicule de multiples infractions, telles que les escroqueries, ou d'attaquer un site internet pour le rendre par exemple inaccessible aux internautes. Le site https://www.botfrei.de/fr/ met gratuitement à votre disposition des outils de protection et de nettoyage de votre ordinateur.

(*) Votre Gendarmerie :

Communauté de brigades de
SAINT-MARTIN D'AUXIGNY
22, avenue de la République
18110 SAINT-MARTIN D'AUXIGNY
02.48.66.69.00

Brigades à ST-MARTIN D'AUXIGNY,
D'HENRICHEMONT et LES AIX D'ANGILLON