LES NOUVEAUX MODES D'ESCROQUERIES SUR INTERNET

L'arrivée d'internet a fait place à une nouvelle criminalité, on parle alors de cybercriminalité. L'escroquerie n'a pas échappé à cette nouvelle technologie, et de plus en plus des internautes subissent des escroqueries. Mais alors comment s'en prémunir, et surtout comment la réprimer ?

L'article L 313-1 du code pénal prévoit quel « l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. »

Ce délit est puni de cinq ans d'emprisonnement et de 375000 euros d'amende.

L'infraction, depuis longtemps édictée, doit faire face à de nouveaux modes d'escroquerie, rendus possibles par le développement d'Internet.

En effet l'utilisation quasi universelle d'Internet par les utilisateurs du monde entier a poussé certains internautes peu scrupuleux à profiter de la crédulité et du manque de connaissance des autres utilisateurs.

II/ Internet en tant que nouveau moyen d'escroquerie

A/ Une prise de conscience politique

Selon les spécialistes de la délinquance sur internet la période actuelle de crise économique joue un grand rôle dans l'augmentation du nombre de ces infractions.

En effet a pour conséquence que les victimes potentielles sont plus nombreuses, car plus de monde est à la recherche de bonnes affaires.

Pour aider à la lutte contre ces pratiques le gouvernement a créé en 2009, dans le cadre de son plan de lutte contre la cybercriminalité, un nouveau site internet www.internet.signalement.gouv.fr.

Ce site constitue le portail officiel de signalement des contenus illicites de l'Internet.

Il permet aux internautes d'alerter les pouvoirs publics en cas d'escroquerie en ligne ou de comportement répréhensible.

Le gouvernement avait déjà ouvert des sites permettant le signalement de contenus pédopornographiques et le dépôt de plainte en ligne.

L'objectif est de permettre facilement à tout citoyen de dénoncer tout contenu illicite, qu'il s'agisse d'escroquerie, de diffamation, d'incitation à la haine raciale, etc.

Ce site s'inscrit dans le plan « anti-arnaque » dévoilé par le ministère de l'Intérieur qui comprend également une campagne de sensibilisation du public à l'escroquerie sur Internet ainsi que la mise en place d'un service téléphonique pour répondre aux interrogations des internautes souhaitant éviter de se faire « arnaquer » ou déjà victime d'escroquerie.

B/ Des moyens de se prémunir

Les deux cas les plus fréquents d'escroqueries sur Internet sont l' « hameçonnage » et l'escroquerie dite « à la nigériane ».

L'hameçonnage est une technique utilisée par les fraudeurs dans le but d'obtenir des renseignements personnels sur un internaute afin d'usurper son identité.

Ce délit consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance, comme par exemple une banque, afin de lui soutirer des renseignements personnels.

Les cibles les plus courantes sont les services bancaires en ligne, les fournisseurs d'accès Internet et les sites de ventes aux enchères tels qu'eBay et les services tels que Paypal.

Les escrocs passent le plus souvent par le biais de courriels à un grand nombre de victimes potentielles.

Les messages ainsi envoyés semblent émaner d'une société digne de confiance et sont formulés de manière à alarmer le destinataire afin qu'il effectue une action en conséquence.

Une approche souvent utilisée est d'indiquer à la victime que son compte a été désactivé à cause d'un problème et que la réactivation ne sera possible qu'en cas d'action de sa part.Le message fournit alors un hyperlien qui dirige l'utilisateur vers une page Web qui ressemble au vrai site de la société digne de confiance.

Arrivé sur cette page falsifiée, l'utilisateur est invité à saisir des informations confidentielles qui sont alors enregistrées par ledit escroc.

Face à ce type de sollicitation la vérification de l'adresse web dans la barre d'adresse du navigateur web est la première parade.

En effet une attaque consiste le plus souvent à utiliser un nom de domaine mal orthographié contrefaisant un nom de domaine réputé, dans le but d'induire la victime en erreur.

Par ailleurs il est prudent de ne pas répondre à un courriel vous demandant de transmettre vos coordonnées bancaires.

En effet votre banque ou toute autre institution de confiance ne vous demandera jamais vos coordonnées bancaires par courriel.

Enfin, en cas de doute, il est recommandé de prendre contact avec votre banque, qui pourra infirmer ou confirmer la requête en cause.

Dans le cas où vous constater une utilisation frauduleuse de votre carte bancaire vous devez en premier lieu le signaler à votre banque.

Puis, portez plainte au commissariat de police ou à la gendarmerie le plus proche de votre domicile.

Il faudra alors vous munir d'une pièce d'identité, de votre relevé bancaire sur lequel figurent les paiements contestés, et les coordonnées de votre banque et des références de votre carte bancaire.

Suite à ce dépôt de plainte, une enquête sera ouverte et transmise au procureur de la République.

La seconde escroquerie la plus fréquente est celle dite « à la nigériane ».

Ce type d'escroquerie repose sur la communication à la victime d'un scénario, ayant pour conséquence le plus souvent le versement d'une somme d'argent.

Cette arnaque fonctionne grâce à des mises en scène personnalisées à l'appui desquelles de faux professionnels, tels que de faux notaires, remettent de faux documents officiels, tels que de faux chèques bancaires.

Pour crédibiliser le scénario, les fraudeurs utilisent aussi de faux sites bancaires, des coordonnées usurpées d'avocats, etc.

Ces messages réclamant une somme d'argent proviennent de l'étranger.

Les conseils sont ici les même que concernant l' « hameçonnage ».

Si vous êtes toutefois victime d'une escroquerie sur Internet, il vous faudra déposez plainte au commissariat ou à la gendarmerie la plus proche.

Il vous faudra alors vous munir de tous les renseignements utiles tels que les références des transferts d'argent effectués, les références des personnes contactées.

Tous les renseignements que pourrez apporter seront utiles dans la mesure où ils peuvent aider à l'identification de l'escroc.

Sachez que ces personnes font appel à votre incrédulité et « plus que le scénario est gros..plus qu'il est efficace….) donc en cas de doute, prenez contact avec la Gendarmerie ou l'organisme déclaré.

Cordialement

Le major CUIGNET Pascal, commandant la BTA VEXIN SUR EPTE