GROUPEMENT DE GENDARMERIE DE L'ALLIER

LES ESCROQUERIES VIA LES RESEAUX DE TELECOMMUNICATION

DOSSIER DE PRESSE

MARS 2013

L'arrivée de l'Internet a fait place à une nouvelle forme de criminalité : la cybercriminalité. L'escroquerie n'a pas échappé à cette nouvelle technologie, et de plus en plus d'internautes la subissent. Cette infraction, prévue et réprimée par l'article 313-1 du Code Pénal, doit faire face à de nouveaux modes d'action, rendus possibles par le développement de l'Internet.

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

Voici donc un panel, non exhaustif, des escroqueries les plus fréquemment rencontrées sur les réseaux de télécommunication. L'escroc va ainsi utiliser tous les moyens mis à sa disposition par l'Internet pour piéger sa victime : les mails, les réseaux de sites de petites annonces, les sites de rencontre et les virus.

Les mails

L'escroquerie dite « **à la nigériane** » va abuser de la crédulité des victimes. En effet, celles-ci devront aider un individu, généralement d'origine africaine, à placer une forte somme d'argent en France moyennant une rémunération. Après les avoir mises en confiance, l'escroc leur demandera des petites sommes d'argent afin de régler des frais imaginaires.

L'escroquerie dite « **à la fausse loterie** » va permettre à la victime de croire dans le gain d'une forte somme d'argent dans une loterie internationale. Mais, la procédure pour récupérer cet argent nécessite le paiement de divers frais de gestion.

L'escroquerie dite « **à l'hameçonnage** » ou « **phishing** » va permettre à l'escroc de récupérer les coordonnées bancaires complètes (numéro de compte, numéro de carte de crédit) par l'intermédiaire de faux mails d'une administration (EDF, CAF …) ou d'une société de services (fournisseur d'accès Internet …). Il s'agira, souvent, d'une erreur comptable en votre faveur et pour recevoir la somme, vous serez redirigé vers une copie parfaite du site de la société en question afin de renseigner vos coordonnées bancaires.

L'escroquerie dite « **au piratage de webmail** » va faire croire aux victimes qu'un de leurs amis est en difficulté dans un pays étranger. Elles vont recevoir de nombreux appels à l'aide de ce faux ami qui leur demandera de l'argent pour régler des frais d'hospitalisation, des frais de justice … Dans ces cas, votre ami réel a vu son compte webmail se faire pirater et tout son carnet d'adresse abreuver de mails frauduleux.

Comment se prémunir contre ce type d'escroquerie :

- En général, les mails sont truffés de fautes d'orthographe et écrits dans un français approximatif.
- Les escrocs ont souvent un lien avec le continent africain (voyage, travail, famille …).
- **Jamais aucun organisme ou société ne vous demandera, par mail, vos coordonnées bancaires.**
- Essayez de contacter votre ami soit disant en détresse par un autre moyen (visite, appel téléphonique …).

Les petites annonces

L'escroquerie dite « **à la petite annonce** » va faire croire à la victime qu'elle a trouvé une bonne affaire en achetant un bien mobilier (voiture, téléphone, ordinateur …). Mais très rapidement, l'escroc demandera une petite somme d'argent pour régler les frais de port ou les frais de douane, par exemple.

L'escroquerie dite « **à Paypal** » va permettre à l'escroc, acheteur potentiel, d'acquérir des biens mobiliers via les sites de petites annonces ou de ventes aux enchères. Il proposera à la victime de payer le bien par Paypal. Celle-ci recevra très vite un faux mail de Paypal mentionnant que le paiement a été effectué. Il enverra donc, sans toutefois vérifier la présence des fonds sur son compte, son bien mis en vente.

L'escroquerie dite « **au faux chèque** » va toucher les personnes qui proposent des services (location de gîte, traduction …). Pour payer ces services, l'escroc enverra un faux chèque d'un montant supérieur à la facture. Il demandera à la victime d'encaisser le chèque et de lui renvoyer, soit par virement Western Union ou par virement bancaire à l'étranger, la différence. Malheureusement, quelques jours plus tard, la banque rejettera le chèque de l'escroc.

Comment se prémunir contre ce type d'escroquerie :

- Attention aux annonces alléchantes (prix d'un véhicule divisé par deux) qui cachent souvent une arnaque ou portent sur un objet volé.
- Lors d'une transaction par Paypal, vérifiez votre compte rapidement. Ne donnez jamais votre mot de passe Paypal à quiconque même à votre meilleur ami.
- Lors d'un règlement par chèque, attendez toujours son encaissement par votre banque avant d'envoyer des fonds.

Les sites de rencontre

L'escroquerie dite « **au site de rencontre** » va toucher aussi bien les femmes que les hommes. L'escroc contactera sa future victime via les sites de rencontre. Après plusieurs semaines de relations virtuelles et de mise en confiance, il demandera à la victime de l'argent pour différentes raisons : une hospitalisation, des frais d'avocat, achat d'un billet pour venir en France …

L'escroquerie dite « **à l'amour** » est une variante de la précédente. Cette fois, l'escroc va demander à la victime, en général un homme, de se dénuder et de se masturber devant la webcam. Plus tard, cet homme recevra un mail émanant d'un service de police africain ou français lui intimant le paiement d'une amende sous peine de poursuites pénales.

Comment se prémunir contre ce type d'escroquerie :

- Dans ces cas, les escrocs touchent à l'intimité ou à la sensibilité de leur victime. Par contre, toute demande réitérée d'argent devra vous paraître louche. De plus, un service de police ne communique jamais de la sorte pour le paiement d'une amende.

Les virus

L'escroquerie dite « **au rançongiciel** » ou « **ransomware** » va permettre à l'escroc, via un logiciel malveillant, de bloquer l'accès de tout utilisateur à une machine ou à un système d'exploitation. Pour cela, le virus prendra la forme d'une page émanant d'un service de police nationale ou internationale et demandera à la victime de payer une certaine somme afin de débloquer sa machine. Hélas, ce paiement sera sans effet sur le déblocage du système.

Comment se prémunir contre ce type d'escroquerie :
Les règles pour se protéger contre les rançongiciels comme pour toutes les contaminations par virus informatiques aujourd'hui sont les suivantes (sources site http://stopransomware.fr) :

- **Tenir à jour son ordinateur**:
  - Le système d'exploitation (autoriser les mises à jour automatiques)
  - Tous vos logiciels et en particulier les logiciels de navigation sur Internet ou de consultation de courrier électronique
  - Les logiciels additionnels ou plugins et en particulier ceux qui permettent d'afficher des animations Java, Flash ou encore des fichiers PDF
- Installer un logiciel **antivirus** et le tenir à jour: il existe des solutions payantes, comme gratuites. Vérifiez avec un antivirus tout support amovible (clé USB notamment) d'origine inconnue.
- **Ne pas cliquer sur les liens provenant de sources inconnues** (notamment des courriers électroniques non sollicités ou des messages sur les réseaux sociaux provenant de contacts inconnus ou ne correspondant à leur façon habituelle de s'adresser à vous).
- **Attention aux publicités sur les sites de streaming :** elles sont souvent porteuses de ce fameux virus qui va s'installer immédiatement sur votre système.
- **Réaliser des sauvegardes de vos fichiers les plus importants**: sur un disque dur amovible, sur des cédéroms ou encore sur des disques de partage sur Internet.

Pour finir, n'oubliez pas de signaler toute escroquerie ou tentative d'escroquerie sur le site gouvernemental https://internet-signalement.gouv.fr