QUE FAIRE QUAND ON EST VICTIME D'UN ACTE CYBERCRIMINEL

En cas d'acte cybercriminel, la victime doit utiliser le moyen classique de denonciation qui est la plainte aux fins d'enquête auprès des services de Police conformément aux dispositions du Code de procédure pénale et de l'article 52 Al. (1) de la Loi sur la Cybersécurité et la Cybercriminalité du 21 Décembre 2010. Elle doit collaborer de façon entière avec les Officiers de Police Judicaire pour la bonne marche de l'enquête.

QUELQUES CONSEILS PRATIQUES POUR EVITER D'ETRE VICTIME DES ACTES CYBERCRIMINELS

- éviter d'accepter les gains des loteries dont vous n'avez jamais participer;
- vérifier toujours que les messages reçus de l'opérateur de téléphonie proviennent d'un numéro court à quatre (04) chiffres ou d'un numéro du centre de messagerie de ladite structure;
- éviter d'exposer en ligne sa nudité aux individus dont vous ne maitrisez pas la moralité;
- éviter d'accepter les demandes d'amitié de personnes sur les réseaux sociaux que vous ne connaissez pas;
- éviter de faire enregistrer votre mot de passe dans le navigateur de votre téléphone portable ou de votre orcdinateur;
- éviter de faire dépanner son telephone chez un maintenancier dont on ignore la moralité;
- éviter de laisser son téléphone entre les mains d'un inconnu, même pour un court instant;
- éviter que les inconnus passent de coups de fil à partir de votre téléphone portable;
- éviter d'acheter des téléphones portables hors des boutiques de ventes d'appareils électroniques;
- éviter de vous précipiter de venir en aide à un proche via une tierce personne sans avoir la confirmation de celui que vous voulez aider.

QUELQUES ADRESSES UTILES

- Direction de la Police Judiciaire (DPJ) : **222 23 24 11**
- Groupement Spécial d'Opérations (GSO) : **222 30 32 71**
- Equipes Spéciales d'Interventions Rapides (ESIR) : **117/17**
- Compagnie de Sécurisation des Diplomates (CSD) : **120**

Ville de Yaoundé :

- Commissariat Central N°1 : **222 22 29 32**
- Commissariat Central N°2 : **222 22 72 72**
- Commissariat Central N°3 : **222 31 52 92**
- Commissariat Central N°4 : **222 23 13 34**

Ville de Douala :

- Commissariat Central N°1 : **233 42 79 89**
- Commissariat Central N°2 : **233 39 67 00**
- Commissariat Central N°3 : **655 97 65 67**
- Commissariat Central N°4 : **656 97 00 63**

Les services déconcentres

- DRSN/ADAMAOUA : **222 25 14 83**
- DRSN/EST : **222 24 15 36**
- DRSN/EXTREME-NORD : **222 29 15 01**
- DRSN/NORD : **222 27 22 05**
- DRSN/NORD-OUEST : **233 36 11 86**
- DRSN/OUEST : **233 44 14 19**
- DRSN/SUD : **222 28 33 92**
- DRSN/SUD-OUEST : **233 32 33 17**

PRÉSIDENCE DE LA RÉPUBLIQUE

DÉLÉGATION GÉNÉRALE À LA SÛRETÉ NATIONALE

47ème ANNIVERSAIRE DE L'ÉTAT UNITAIRE

JOURNÉE PORTES OUVERTES

POLICE CAMEROUNAISE

LOYALISME ET DEVOUEMENT

THÈME

« UNITÉ DANS LA DIVERSITÉ, ATOUT MAJEUR DU PEUPLE CAMEROUNAIS, DANS SA MARCHE RESOLUE VERS L'ÉMERGENCE »

LUTTE CONTRE LA CYBERCRIMINALITÉ

UNITE SPECIALE DE LUTTE CONTRE LA CYBERCRIMINALITE

Dans un contexte généralisé d'expansion des nouvelles technologies de l'information, les cybercriminels disposent de matière pour améliorer leurs techniques. De plus en plus, les pays du monde s'organisent afin d'apporter la riposte adéquate et le Cameroun n'est pas en reste. C'est dans ce contexte que le Délégué Général à la Sûreté Nationale, par Note de Service N° 47/DGSN/SG/ DPJ du 23 Mars 2018, a créé au sein de la Direction de la Police Judiciaire, l'Unité Spéciale de Lutte contre la Cybercriminalité (USLUCC). Cette Unité a été rendue opérationnelle dès sa création compte tenu de l'urgence en la matière.

Son personnel est constitué des fonctionnaires de Police hautement qualifiés et aguerris.

Ses missions sont celles de l'Investigation Numérique, du Renseignements Numériques, et de la lutte contre la Cybercriminalité et le Cyber terrorisme.

En ce qui concerne l'investigation numérique, cette Unité est présente sur les scènes de cyber crime pour rechercher, collecter, préserver, analyser et mettre sous une forme exploitable par la justice les traces ou preuves numériques. Elle écoute et surveille également les reseaux sociaux. Dans la lutte contre la cybercriminanilité et de cyber terrorismeme, elle effectue des enquêtes judiciaires portant sur les infractions visant ou utilisant des systèmes informatiques ou téléphoniques.

CYBERCRIMINALITE, PARLONS-EN!

Définie comme l'ensemble des infractions commises au moyen des TIC, la cybercriminalité est un fléau prenant de l'ampleur avec l'expansion de l'internet. Elle se manifeste sous plusieurs formes dans notre pays dont quelques unes sont relevées ici.

LA FRAUDE AUX ANIMAUX, PIERRES PRECIEUSES ET OBJETS D'ART (ESCROQUERIE BAMOUN)

Un animal, une pierre precieuse ou un objet d'art est mis en vente sur un site d'annonces. Le pseudo vendeur est soi -disant un expert et s'engage à faire livrer l'animal ou l'objet par societe de transport de colis (DHL). Pour ce faire, il demande un versement sous forme de mandat Western Union qu'il va retirer en bénéficiant d'une complicité local dans l'établissement.

LA FRAUDE AMOUREUSE – ARNACOEUR .

L'escroc rencontre sa victime sur des sites de rencontres et présente le profil de l'homme ou de la femme idéale. Plus tard, cette personne est victime d'une aggression ou est gravement malade et demande donc à la victime de l'argent pour payer les frais d'hôpital. Il existe de nombreuses variantes de cette fraude mais le but poursuivi est toujours le meme, Spolier la victime.

LA FRAUDE SUR SITES DE VENTES FANTÔMES

Un site internet fait commerce d'un bien qui intéresse les clients (ex : vente de chaussures de sport) et cumule un nombre important de fausses ventes avant de disparaître avec les versements des clients. Le client n'est jamais livré.

LA FRAUDE AUX LOTERIES (LE BAGNARD)

La victime reçoit un appel ou un SMS sur son portable qui lui annonce qu'elle a gagné à une loterie ou que grâce à sa fidélité à l'opérateur de télé phonie, elle a gagné un prix et qu'elle doit entrer en possession sous certaines conditions. L'escroc lui demande alors de saisir une suite de codes à travers lesquels la victime transfère en toute ignorance le contenu de son porte-monnaie électronique vers celui de l'escroc.

LA FRAUDE AU COMPTE FACEBOOK PIRATÉ

Le pirate prend le contrôle du profil Facebook de la victime (variante avec le compte Email et WhatsApp de la victime). Se faisant passer pour elle, il adresse à tous les contacts de la victime un message mentionnant qu'il est en difficulté et souhaite avoir une aide financière qu'il compte rembourser par la suite. Il communique alors le moyen de lui faire parvenir les fonds. (Orange Money, Mobile Money, express union etc..)

LA FRAUDE AU CHANSIM

Une variante de la fraude au compte Facebook piraté, l'escroc se rend chez l'opérateur de téléphonie et fait changer la SIM de la victime avec une complicité d'un agent. Il va vider son porte-monnaie électronique ou se faire passer pour elle pour escroquer ses contacts.

LE CHANTAGE À LA WEBCAM – SEXYCAM

L'escroc croise sa victime sur un site de rencontres ou sur Facebook et se fait passer pour une personne de l'autre sexe. Il demande à sa victime de s'exhiber ou de se masturber devant la webcam. Pendant ce temps, il met en œuvre un logiciel qui permet de capturer ce qui est diffusé sur la caméra. Il menace ensuite la victime de diffuser les images sur internet si une somme d'argent ne lui est pas versée.

N.B. : La liste des fraudes commises sur internet et à la téléphonie n'est pas exhaustive. Les cas relevés ici peuvent avoir plusieurs variantes.

LES SANCTIONS ENCOURUES PAR LES CYBERCRIMINELS

Ces sanctions sont consignées dans la Loi N° 2012/012 du 21 Décembre 2010 sur la Cybersécurité et la Cybercriminalité et la Loi N°2010/013 du 21 Décembre 2010 regissant les communications électroniques au Cameroun. Elles sont reparties comme suit:

* les atteintes aux personnes (les atteintes aux libetés indi viduelles et à la vie privée Art 75, et les atteintes spécifiques aux droits de la personne au regard du traitement des données à caractère personnel Art 75 et 84);
* les atteintes aux biens relatives aux moyens de paiement électronique Art 73;
* les atteintes sexuelles aux mineurs (la pornographie infantile ou à caractère pedophile Art 76 , 80 et 81, Outrage à la pudeur Art 79 et 82);
* les xénophobies et le racisme en ligne Art 77.