Déclaration de la communauté Africaine d'ICANN participant à la réunion conjointe AFRALO-AfrICANN à Dakar le 26 Octobre 2011

Les membres de la communauté Africaine d'ICANN participant à la réunion conjointe AFRALO – AfrICANN tenu le Mercredi 26 Octobre 2011 à Dakar, lors de la 42ème réunion publique internationale d'ICANN, après avoir débattu des dangers encourus par les utilisateurs finaux de l'Internet en Afrique du fait de la cybercriminalité sous toutes ses formes :

1. Exhortent les opérateurs des ccTLD Africains d'adopter l'implantation du DNSSEC qui est une mesure cruciale pour la sécurisation du DNS

2. Encouragent les pays Africains à mettre en place des autorités opérationnelles de certification à clé publique (signature électronique).

3. Recommandent aux Internautes Africains d'utiliser les clés ou signatures électroniques pour crypter ou signer les messages électroniques contenant des informations confidentielles ou critiques.

4. Encouragent les pays Africains qui ne disposent pas encore de CERT de procéder à la création d'une telle équipe pour répondre à temps aux requêtes des internautes et leur fournir le conseil nécessaire basé sur les informations de sécurité mises à jour.

5. Recommandent le lancement d'une initiative de Partenariat Public-Privé pour élaborer des directives de protection des enfants contre le contenu abusif des enfants sur Internet. L'initiative devrait adapter le projet global de directives de protection des enfants sur Internet publié par l'IUT à l'environnement national de chaque pays Africain, et pousser pour l'adoption d'une politique et de textes juridiques permettant la mise en œuvre de ces directives, qui devraient porter du reste sur les responsabilités des parties prenantes à savoir l'industrie des TIC, les pouvoir politiques, les organismes juridiques, les parents, les enseignants et tuteurs, et puis les enfants et les jeunes.

6. Conseillent aux parents Africains de se doter des logiciels de contrôle parental, tout en encadrant leurs enfants et les sensibilisant aux dangers présents sur le net.

7. Invitent tous les utilisateurs de l'Internet en Afrique à prendre contact avec l'équipe d'urgence en sécurité informatique (CERT) de leur pays (s'il y en a un) pour s'informer des dernières alertes en termes de virus informatique, et de suivre son conseil éclairé pour éviter les éventuels dommages à leurs systèmes.

8. Encourage la réactualisation des différentes déclarations et positions africaines sur la cybercriminalité en impliquant les utilisateurs finaux et la société civile dans le processus.

9. Invitent les pays Africains à coopérer pour une harmonisation et une mise à jour du cadre légal régissant le Cyberespace dans les différents pays Africains

10. Encouragent la mise en place des cycles de formation de formateurs sur les questions de Sécurité de l'Internet et de cybercriminalité

11. Recommandent aux usagers Africains de la toile de suivre de très près les règles minimales de sécurité listées ci-dessous :
    - **Utiliser des mots de passe de qualité.** c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés, et difficiles à deviner par une tierce personne.
    - **Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc. car** La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels).
    - **Effectuer des sauvegardes régulières** afin de pouvoir réagir à une attaque ou un dysfonctionnement.
    - **Désactiver par défaut les composants ActiveX et JavaScript**, car bien qu'ils permettent des fonctionnalités intéressantes, ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable.
    - **Ne pas cliquer trop vite sur des liens mais** saisir soi-même l'adresse du site dans la barre d'adresse du navigateur **car** Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message.
    - **Contrôler la diffusion d'informations personnelles :** une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises.
    - **Ne jamais relayer des canulars ;** des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc.
    - cultiver la prudence **: l'internet est une rue peuplée d'inconnus et** d'une façon générale, il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.
    - **Vigilance avant d'ouvrir des pièces jointes à un courriel :** elles colportent souvent des codes malveillants