MINISTÈRE DES POSTES & TÉLÉCOMMUNICATIONS | www.minpostel.gov.cm

CAMPAGNE NATIONALE POUR LA PROMOTION DE LA CULTURE DE LA CYBERSÉCURITÉ ET SENSIBILISATION À L'UTILISATION RESPONSABLE DES RÉSEAUX SOCIAUX

NATIONAL CAMPAIGN TO PROMOTE THE CULTURE OF CYBERSECURITY AND RAISE AWARENESS ON THE RESPONSIBLE USE OF SOCIAL MEDIA

"Tous mobilisés pour la cybersécurité au Cameroun"

"let all mobilized for cybersecurity in Cameroon"

LE JOURNAL DE L'ETUDIANT

LPE Le Petit Ecrivain

« De ma position de Chef de l'Etat, j'aperçois les signes d'un frémissement qui prouvent que vous vous intéressez de plus en plus aux affaires publiques.

Les réseaux sociaux vous offrent à cet égard un champ d'expression de prédilection. Chaque fois qu'en un clic, vous empruntez ces autoroutes de la communication qui vous donnent une visibilité planétaire, il vous faut vous souvenir que vous n'êtes pas pour autant dispensés des obligations civiques et morales, telles que le respect de l'autre et des institutions de votre pays. Soyez des internautes patriotes qui œuvrent au développement et au rayonnement du Cameroun, non des followers passifs ou des relais naïfs des pourfendeurs de la République.

Le Cameroun de demain, qui se construit sous nos yeux, n'aura plus grand-chose à voir avec celui d'hier. Vous en serez les premiers bénéficiaires. Il faudra vous en montrer dignes. »

Message du Chef de l'Etat à la jeunesse le 10 février 2018.

« From my position as Head of State, I perceive signs of your growing interest in public affairs.

In this regard, your favourite platform of expression is the social media. Whenever at a click, you access these communication highways that give you global visibility, you must bear in mind that you are not exempted from fulfilling civic and moral obligations, such as respect for others and your country's institutions. Be patriotic Internet users working for Cameroon's development and influence, and not passive followers or naive relays for staunch critics of the Republic.

The Cameroon of tomorrow, which is being forged before our very own eyes, will differ almost entirely from that of yesteryear. You will be its key beneficiaries. You will need to prove yourselves worthy of it. »

Head of State's message to the youth, 10 february 2018

« *Sous l'autorité et la coordination du Premier Ministre Chef du Gouvernement les pouvoirs publics élaborent des stratégies pour adresser la problématique de la cybercriminalité* »

Joseph DION NGUTE, Premier Ministre Chef du Gouvernement

« *Under the coordination and authority of the Prime Minister Head of Government the public authorities have been developping strategies to address the problem of cybercrime* »

Joseph DION NGUTE, Prime Minister Head of Government

L'interview,

Madame le Ministre des Postes & Télécommunications

1/ Aujourd'hui, le citoyen détenteur d'un téléphone portable approprié, se retrouve très souvent au départ ou dans la chaîne de dissémination d'une image ou d'une nouvelle, peu importe que ces images ou ces nouvelles soient vraies ou fausses. Dans les médias ou les réseaux sociaux, la persistance des «fake-news» a contribué à entretenir des contre-vérités, éloignant ainsi nombre de nos conci-toyens de la bonne information sur des sujets d'importance capitale. Pouvez-vous nous dire ce que c'est qu'un «fake news» ?

Le terme ***«fake news»*** est composé de deux mots anglais ***«fake»*** et ***«news»*** qui signifient ***«fausses informations»***. Les ***«fakes news»*** sont donc, des informations bénéficiant le plus souvent d'une large diffusion dans les médias, notamment sur internet et les réseaux sociaux, volontairement truquées pour tromper délibérément l'opinion en essayant d'attirer l'attention avec quelque chose de soi-disant ***«au-thentique»***, de choquer ou d'influencer l'opinion des autres. Ils sont écrits par des individus ou des groupes agissants dans leur propre intérêt ou au nom d'autres personnes. La création et la diffusion des fake news sont principalement dues à des motifs personnels, politiques ou économiques.

2/ Quel est l'impact social que pourrait avoir la propagation d'un fake news ?

Un fake news a pour but de manipuler l'opinion publique et de l'orienter dans la direction souhaitée par le manipulateur. Sur internet, les fausses informations, les rumeurs peuvent s'exprimer partout, et cibler à tout moment n'importe qui. Les réseaux sociaux sont d'ailleurs devenus le terrain propice à la diffusion et à la propagation des fake news en tout genre. La propagation des fake news peut être à l'origine de la mauvaise éducation des populations, de la dépravation des mœurs, des troubles sociaux, des soulèvements populaires et de l'instabilité d'un pays.

3/ Comment un fake news peut ternir l'image d'un individu et même d'une institution ?

« Tous mobilisés pour la cybersécurité au Cameroun »

Les fake news portent d'énormément préjudices sur l'image des individus et des institutions. Ils peuvent conduire à les discréditer ou les décrédibiliser auprès de l'opinion publique engendrant ainsi une perte de confiance. Un individu victime d'un fake news peut passer à côté d'un emploi où il aurait postulé ou perdre un poste de responsabilité qu'il occupait dans une structure, voire rater une promotion qui lui était promise. Il peut également devenir la risée d'une société. Des fake news, ont contribué à ternir l'image de plusieurs hautes personnalités dans notre pays. Une institution peut perdre des moyens humains et financiers à cause d'une fausse information qui aurait entachée son image.

4/ « Nous avons assisté ces derniers temps à la multiplication de comportements antipatrioti-ques, à la prolifération de discours haineux, à la publication de vidéogrammes violents, obscè-nes et déshonorants, qui ont choqué la cons-cience collective nationale. Le Chef de l'État Camerounais s'est adressé à ses compatriotes dans son discours traditionnel de fin d'année en décembre 2021, en quoi et comment un étudiant peut-il s'y identifier ?

Les étudiants et les jeunes en particulier, dans leur quasi majorité, sinon tous, utilisent les smartphones, et sont connectés tous les jours sur internet en général et, sur les réseaux sociaux en particulier. Ils sont forcément au contact des informations qui y sont véhiculées, y compris les fake news. Il y a beaucoup d'échanges d'information à l'intérieur du milieu estu-diantin et entre le milieu estudiantin et le monde extérieur. Ce qui explique le terme ***«génération androïde»***, utilisé par le Chef de l'Etat.
Les étudiants et les jeunes, constituent de ce fait la tranche de la population la plus exposée.

5/ « J'en appelle donc à votre responsabilité individuelle et exhorte chacun de vous à pro-mouvoir la culture de la paix. Je demande au Gouvernement d'intensifier la sensibilisation de toutes les couches sociales à un usage citoyen des réseaux sociaux ». Comment comprendre cette interpellation du Chef de l'État ?

Généralement, en matière de sécurité, le risque zéro n'existe pas et l'homme constitue le maillon le plus faible de la chaîne. Il est donc important de maintenir sa conscience éveillée face aux dérives constatées sur internet et dans les réseaux sociaux. Pour maintenir cette conscience éveillée, une sensibilisation perma-nente sur les meilleures pratiques et usages citoyens d'internet et des réseaux sociaux est d'un apport capital. Cette interpellation du Chef de l'Etat montre

qu'il est conscient de l'ampleur du phénomène des fake news et des risques que cela peut engendrer pour le Cameroun. Le Chef de l'État nous fait comprendre à cet effet que la sécurité est une affaire de tous et de chacun. En effet, l'utilisation malveillante des réseaux sociaux et de l'Internet d'une manière générale, est source de divers types de conflits entre les individus. Elle est surtout source de troubles sociaux et de déstabilisation des Etats. Il est donc indispensable, pour chaque citoyen, de contribuer à maintenir la paix, à travers un usage responsable des réseaux sociaux.

6/ Quel est le risque pour un étudiant de publier/partager des vidéogrammes violets, obscènes et déshonorants ?

Le premier risque est celui des sanctions prévues par la réglementation. En effet, au Cameroun, l'arsenal juridique n'est pas complètement démuni. Qu'il s'agisse de n'importe quelle personne, auteure d'une infraction cybernétique, ***la loi N°2010/012 du 21 décembre 2010*** relative à la cybersécurité et à la cybercriminalité au Cameroun a prévu des sanctions contre les partages ou publications de messages ou vidéo malveillants. En voici quelques-unes :

- Article 77 : (1) Est puni d'un emprisonnement de 2 à 5 ans et d'une amende de 2.000.000 à 5.000.000 ou de l'une des 2 peines seulement, celui, qui par la voie de communications électroniques ou d'un système d'information, commet un outrage à l'encontre d'une race ou d'une religion.

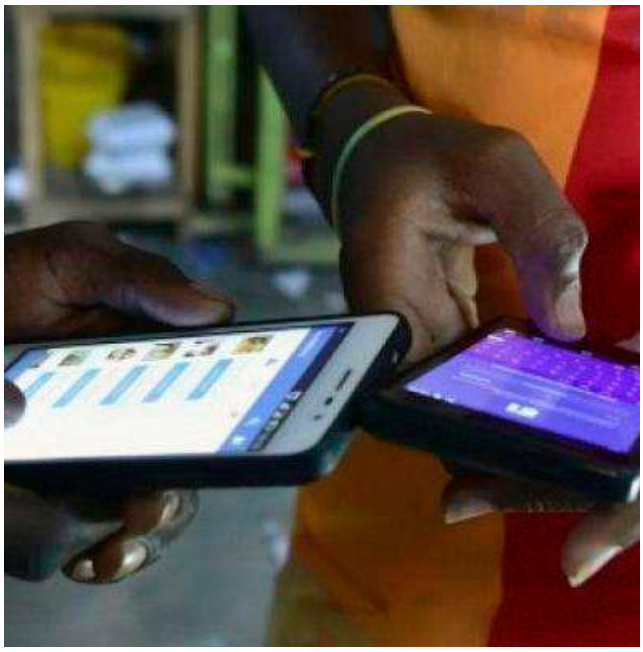
(2) Les peines prévues à l'alinéa 1 ci-dessus sont doublées lorsque l'infraction est commise dans le but de susciter la haine ou le mépris entre les citoyens.

- Article 78 : (1) Est puni d'un emprisonnement de 6 mois à 2 ans et d'une amende de 5.000.000 à 10.000.000 ou de l'une de ces 2 peines seulement celui qui publie ou propage par voie de communications électroniques ou d'un système d'information, une nouvelle sans pouvoir en apporter la preuve de véracité ou justifier qu'il avait de bonnes raisons de croire à la vérité de ladite nouvelle.

(2) Les peines prévues à l'alinéa 1 ci-dessus sont doublées lorsque l'infraction est commise dans le but de porter atteinte à la paix publique.

- Article 80 : (1) Est puni d'un emprisonnement de 3 à 6 ans et d'une amende de 5.000.000 à 10.000.000 ou de l'une de ces 2 peines seulement celui qui diffuse, fixe, enregistre ou transmet à titre onéreux ou gratuit l'image présentant les actes de pédophilie sur un mineur par voie de communications électroniques ou d'un système d'information.

(2) Est puni des mêmes peines prévues à l'alinéa 1 ci-dessus, quiconque offre, rend disponible ou diffuse, importe ou exporte, par quelque moyen électronique que ce soit, une image ou une représentation à carac-



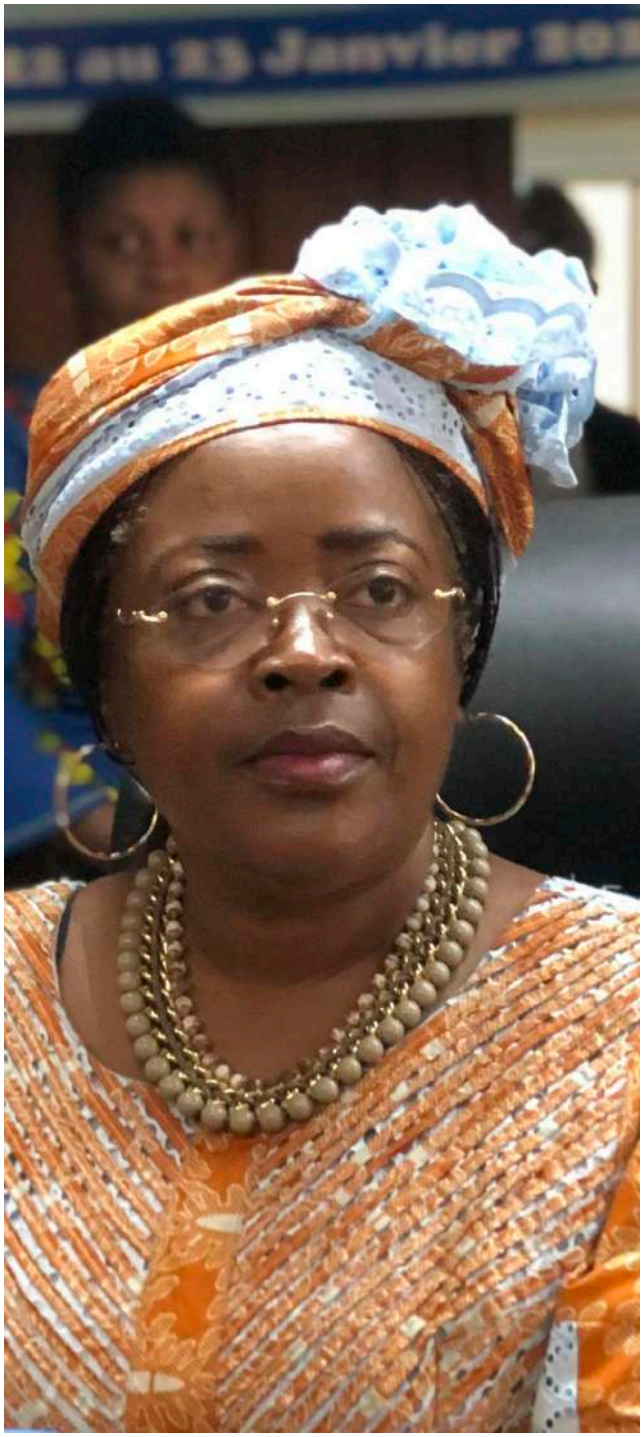
tère pédophile.
(3) Est puni d'un emprisonnement d'1 à 5 ans et d'une amende de 5.000.000 à 10.000.000 ou de l'une de ces 2 peines seulement, celui qui détient dans un réseau de communications électroniques ou dans un système d'information, une image ou une représenta-tion à caractère pédophile.
(4) Les peines prévues à l'alinéa 3 ci-dessus sont doublées, lorsqu'il a été utilisé un réseau de communications électroniques pour la diffusion de l'image ou la représentation du mineur à destination du public.
(5) Les dispositions du présent article sont également applicables aux images pornographiques mettant en scène des mineurs.
Au-delà de ces sanctions et bien d'autres prévues par la réglementation de notre pays, notamment le code pénal et la loi citée plus haut, il y a lieu de prévenir nos jeunes, que tout ce qui est posté sur Internet ne s'efface pas. Par conséquent, ils peuvent voir leur vie basculer du jour au lendemain, parce que les informations, photos ou vidéo refont surface quelques années plus tard, au moment où l'on s'y attend le moins, mettant un terme à certaines ambitions (politique, emploi, et autres).

7/ Quelle est la stratégie gouvernementale mise en place pour combattre le phénomène fake news ?

Le Cameroun dispose d'une stratégie gouvernementale de lutte contre la cybercriminalité dont l'objectif est de bâtir un cyber espace sûr et résilient. Et dans ce cadre, nous ne citerons que trois axes stratégiques majeurs qui sont : Le renforcement du dispositif légal et réglementaire, que nous avons mentionné plus haut. Cette loi déjà très dissuasive, est en cours d'actualisation, afin de permettre au Gouvernement de disposer d'un instrument juridique plus sévère contre les cybercrimes, y compris la désinformation, et adapté à l'évolution du numérique. Dans le domaine de la régulation, l'Etat dispose d'un Régulateur en matière d'internet : l'ANTIC, dont la principale mission est la lutte contre la cybercriminalité. Plusieurs autres structures de l'Etat sont également à l'œuvre : le SED, la DGSN et la DGRE. La deuxième orientation majeure de cette politique est le développement des infrastructures de cybersécurité en vue de la prévention, la

En cas de problème ou pour dénoncer les dérives, utilisez le numéro vert de l'ANTIC : 8202

détection et la neutralisation des menaces qui pèsent sur les réseaux et les systèmes d'information. Nous citerons notamment le centre d'alerte et de réponse de l'ANTIC, les laboratoires d'investigation numérique de la Direction de la Police Judiciaire. Et enfin, le dernier volet important, concerne la sensibilisation, le renforcement des capacités et la gestion du changement, qui visent à accroître les aptitudes des usagers à une meilleure utilisation du cyberespace. Réagissant aux Très Hautes Interpellations du Chef de l'Etat, le Ministère des Postes et Télécommunications a engagé depuis 2020 une vaste campagne de promotion de la culture de cybersécurité et sensibilisation à l'usage responsable des réseaux sociaux.
Organisée sous le thème : Organisée sous le thème : ***«Tous mobilisés pour la cybersécurité au Cameroun»***, cette campagne vise à mobiliser toutes les couches sociétales dans la lutte contre la cybercriminalité et le dévoiement des réseaux sociaux et mettre ainsi en place, une véritable coalition nationale pour la promotion de l'utilisation citoyenne des réseaux sociaux, cette campagne vise à mobiliser toutes les couches sociétales dans la lutte contre la cybercriminalité et le dévoiement des réseaux sociaux et mettre ainsi en place, une véritable coalition nationale pour la promotion de l'utilisation citoyenne des réseaux sociaux. La campagne qui s'est tour à tour déployée dans les régions du Centre, du Littoral, du Sud-ouest, de l'Est et du Sud est appelée à s'intensifier, suivant les récentes Très Hautes Prescriptions du Chef de l'Etat. C'est dans ce cadre que se situent les opérations de sensibilisation par voie de médias (TV, radio, réseaux sociaux, presse écrite) et par SMS; les campagnes d'affichage dans les institutions et établissements d'enseignement publics. Le MINPOSTEL dispose également d'Ambassadeurs de bonne volonté



pour la culture de la cybersécurité et l'utilisation responsable des réseaux sociaux, qui font également le relais de cette sensibilisation dans leurs activités.

8/ Comment la jeunesse peut-elle participer ?

Les jeunes doivent être des partenaires dans la lutte contre les fausses informations sur internet. Ce d'autant qu'ils ont tendance à mieux comprendre le fonctionnement d'internet et des réseaux sociaux. Nous nous réjouissons de l'action des Ambassadeurs de bonne volonté et des autres Partenaires (Hommes de Presse, Influenceurs, Professionnels ...), qui nous accompagnent déjà dans cette lutte, et qui sont très bien outillés pour sensibiliser d'autres jeunes. En somme, les jeunes doivent être éduqués et sensibilisés. Il y a lieu de les impliquer davantage dans les campagnes de sensibilisation car Ils connaissent aussi mieux les contenus, les tendances et le vocabulaire susceptibles d'accrocher les jeunes, et peuvent aider à créer des contenus capables d'intéresser un public plus large et de l'encourager à changer de comportement. Il y a lieu également lieu de les former sur les outils permettant de détecter les fake news.

9/ Est-ce que la création ou la promotion des réseaux sociaux camerounais palliera à ces comportements déviants ?

La création des réseaux sociaux peut réduire les comportements déviants, pas forcément les éradiquer. La difficulté actuelle réside dans le fait que les plateformes numériques qui véhiculent les fake news sont généralement hébergées aux USA et par conséquent échappent au contrôle des autorités camerounaises. La création ou la promotion des réseaux sociaux locaux ont ceci d'avantageux qu'ils seront mieux contrôlés au niveau national mais l'éducation, la sensibilisation de la population ainsi que la promotion et la vulgarisation des outils de détection des fake news semblent être les solutions les plus efficaces pour l'instant.

10/ À l'ère du numérique, quels conseils pouvez-vous donner à la jeunesse dite génération dite Android ?

La jeunesse dite génération androïde doit adopter un comportement citoyen dans les réseaux sociaux. Elle doit savoir qu'il y est interdit de propager des informations fausses, des informations à caractère haineux, tribal et raciste. La jeunesse doit développer un esprit critique et refuser d'accepter tout ce qui est publié sur internet et les réseaux sociaux, sans vérification préalable. Elle ne doit pas propager, ni diffuser des contenus à caractère pornographique, ni exposer la vie privée des individus ainsi que la sienne dans les réseaux sociaux ou internet. Chaque jeune aujourd'hui doit toujours se demander, avant de propager une information qui lui a été transférée : «pourquoi me l'a-t-on envoyée, sa véracité est-elle prouvée ? et quelles sont les conséquences si je la transfère ?». Leur avenir en dépend, l'avenir de notre pays en dépend.

Cybersécurité et lutte contre la Cybercriminalité
ARNAQUE NUMERIQUE

L'expert/Formateur Franck Arnold BAMA-SI
Ing., Doctorant en Télécommunications

I- CAS DES FAUSSES OFFRES D'EMPLOI

Certaines offres d'emplois diffusées sur Internet peuvent être frauduleuses. Des cybercriminels se font passer pour de vrais recruteurs pour soutirer aux victimes de l'argent ou des informations personnelles.

1. En quoi consiste l'arnaque à la fausse annonce d'emploi ?

Certaines offres d'emplois diffusées sur Internet n'amènent pas à de vrais recrutements. Elles sont en apparence identiques à de véritables offres, le plus souvent très attractives pour les candidats, et respectent les réglementations légales en matière de droit du travail (durée du travail, rémunération, etc.). Ces fausses offres d'emploi sont créées par des fraudeurs qui se font passer pour de vrais recruteurs en usurpant le nom d'une entreprise, son adresse, l'identité d'un salarié ou d'un responsable de l'entreprise, ou son numéro de contribuable. Les fraudeurs font miroiter un poste sans jamais avoir rencontré le demandeur d'emploi et envoient, pour renforcer leur crédibilité, des documents d'apparence officielle (contrat de travail, formulaire de candidature, etc.).

But recherché

Soutirer de l'argent ou dérober des informations personnelles (données bancaires, numéro de sécurité sociale) pour en faire un usage frauduleux.

2. Comment s'en protéger ?

a. ***Méfiez-vous d'une offre trop attractive***, voire hors norme. N'hésitez pas à en parler à votre entourage ou un professionnel de l'emploi (FNE...).

b. ***Méfiez-vous des propositions d'emploi non sollicitées.*** Ces propositions sont souvent adressées à de nombreuses personnes et votre adresse de messagerie ne figure pas toujours dans le champ «destinataire» où plusieurs autres noms s'y trouvent.

c. ***Méfiez-vous des annonces contenant des fautes d'orthographe ou qui demandent de répondre à une adresse de messagerie «publique»***. Une grande entreprise vous adressera ainsi toujours un message émis depuis son nom de domaine (exemple : ***XX@minpostel.gov.cm*** et non pas ***erick258@XY.com***).

d. ***Ne transmettez jamais à un recruteur vos données personnelles*** (RIB, numéro de sécurité sociale, de compte ou de carte bancaire) tant que vous ne l'avez pas rencontré.

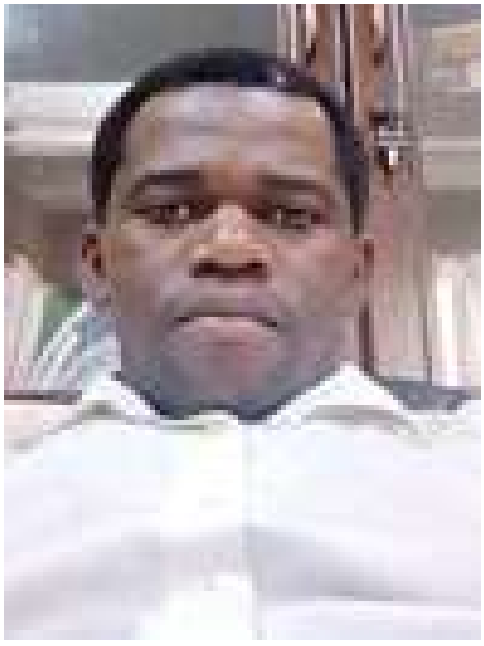
e. ***Ne versez aucune somme d'argent à un employeur potentie***l quel que soit le motif évoqué (contrat de travail potentiel ou suivi d'une formation préalable à l'embauche) et le mode de transfert (achat de cartes ou de coupons prépayés, virement express à l'international).

f. ***N'achetez jamais du matériel pour le compte de l'entreprise et n'acceptez jamais de recevoir un chèque*** ou un virement bancaire pour effectuer des achats nécessaires à votre prise de poste.

g. ***N'acceptez aucune rétribution de votre futur employeur*** tant que vous n'avez pas signé le contrat de travail.

h. ***Assurez-vous de l'existence juridique*** (Registre de commerce, N° contribuable) de l'entreprise à l'origine de l'offre d'emploi.

i. ***Soyez vigilant lorsqu'un recruteur vous contacte à un horaire atypique*** ou s'il ne peut vous rencontrer sous prétexte qu'il est à l'étranger.



j. ***Soyez attentif aux propos du recruteur*** en particulier lorsque par exemple, en cours d'entretien, il vous propose un poste différent de celui mentionné dans l'annonce.

k. ***Ne poursuivez pas la communication si vous doutez de l'honnêteté de votre interlocuteur***.

l. ***Prenez le temps de lire avec attention tous les documents qui vous sont communiqués*** et n'apposez jamais votre signature sur un document sans savoir précisément ce à quoi vous vous engagez.

m. ***N'encaissez jamais de chèques qui ne seraient pas de votre employeur***. Même si le montant d'un chèque déposé à votre banque apparaît en crédit sur votre compte, la banque, une fois les vérifications réalisées (chèque volé...), a plusieurs semaines pour valider l'opération ou l'annuler en débitant votre compte du même montant.

n. ***Tenez à jour votre antivirus et votre système d'exploitation.***

3. Victimes d'une arnaque à l'emploi, que faire ?

a) Interrompez immédiatement toutes relations avec le pseudo recruteur même si ce dernier se montre menaçant par message ou par téléphone.

b) Informez l'organisme dont vous avez transmis des données personnelles : si vous avez transmis des données personnelles (numéro de sécurité sociale...), informez-en l'organisme concerné (CNPS, FNE, ...).

c) Informez votre banque et surveillez régulière-

ment les opérations sur vos comptes : si vous avez transmis des informations bancaires, informez-en votre banque et surveillez régulièrement les opérations sur votre compte bancaire.

d) Conservez les preuves, notamment les numéros de téléphones, les messages que vous avez reçus ou toutes autres informations qui pourront vous servir pour signaler l'arnaque aux autorités. Si vous avez reçu le message par courriels (mails), conservez-les précieusement.

e) Informez l'organisme dont l'identité a été usurpée et/ou le site d'emploi qui a diffusé l'annonce en fournissant, si possible, l'ensemble des informations que vous avez pu collecter pour attester de la fraude à l'emploi (référence de l'annonce, nom de l'entreprise, nom du pseudo recruteur, coordonnées, etc.).

f) Signalez les faits à l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) en appelant le 8202.

g) Déposez plainte : que vous soyez victime d'une tentative d'escroquerie, d'un vol de données personnelles ou d'une escroquerie financière, déposez plainte au commissariat de police ou à la brigade de gendarmerie. Ce dépôt de plainte vous aidera dans vos futures démarches en cas d'usurpation de votre identité.

II- CAS D'ARNAQUES DANS LE SECTEUR DE LA TELEPHONIE MOBILE

Le téléphone mobile est l'un des terrains de jeu privilégiés des malfaiteurs. Les arnaques prennent différentes formes et répondent à des objectifs variés : vol d'argent, usurpation d'identité, espionnage de vos données...

1.Quelles sont les escroqueries par téléphone ?

De nos jours, les téléphones portables font partie de nos biens les plus précieux, et les cybercriminels en sont conscients. Nous les emmenons toujours avec nous, et nous les utilisons pour accéder à certaines des informations les plus privées de notre vie. Nous avons associé les données bancaires, les messageries électroniques et d'autres données sensibles à nos téléphones, ce qui en fait une cible parfaitement centralisée pour le vol d'identité et la fraude. Les types d'escroqueries par appareil mobile les plus courants sont les suivants :

Signalez les faits à l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) en appelant le 8202.

** Escroqueries de virus par appareil mobile*

Les escroqueries de virus par appareil mobile diffusent de fausses alertes prétendant qu'un virus a été détecté sur votre téléphone. En naviguant sur le Web avec votre téléphone, vous avez peut-être vu apparaître une page présentant ce type d'alerte. La page vous informera qu'une analyse de votre téléphone a révélé une infection virale et vous invitera à prendre des mesures immédiates. Ensuite, l'escroquerie vous pousse à télécharger une application «antivirus», qui est en fait un logiciel malveillant ou un logiciel espion. Une fois que le code malveillant est sur votre smartphone, les escrocs peuvent infecter d'autres appareils ou détourner les vôtres. Le moyen le plus simple de se protéger contre ce genre d'attaques est de s'assurer que votre téléphone est équipé d'un système de cybersécurité, comme ***Android Antivirus.***

** Phishing par SMS (smishing)*

Le phishing par SMS, ou le « smishing », fait référence à une escroquerie qui vous pousse à agir par SMS. Des liens malveillants peuvent vous être envoyés par SMS, et si vous ouvrez le lien, votre appareil peut être infecté par un logiciel malveillant ou un logiciel espion. Il peut aussi arriver que le criminel vous pousse à agir d'une certaine façon. Parmi les autres actions, on peut citer l'appel à un numéro de téléphone payant à la minute, le fait de vous faire souscrire un abonnement ou de vous contraindre à fournir des informations personnelles.

** Escroqueries par messagerie vocale (vishing)*

Le vishing, ou le « phishing vocal », fait référence à des escroqueries par téléphone cellulaire qui vous incitent à agir d'une manière ou d'une autre. Les escrocs se font passer pour une personne ou une organisation authentique afin de gagner votre confiance. Ils peuvent se faire passer pour des membres d'une entreprise officielle ou d'un service gouvernemental et vous convaincre que vous devez fournir des informations personnelles ou de l'argent. Ces escroqueries visent à vous faire agir pendant l'appel téléphonique. Les escrocs comptent sur l'urgence et espèrent que vous allez réagir dans la «panique» pour leur donner ce qu'ils veulent. C'est pourquoi les escrocs feront pression sur vous pour que vous effectuiez un paiement ou pour que vous partagiez des informations pendant l'appel même, plutôt que de vous demander

de les rappeler (une fois qu'ils auront raccroché).

* Escroqueries à l'appel en absence

Les escroqueries à l'appel en absence sont des appels provenant d'un numéro inconnu qui ne font sonner votre appareil qu'une fois, avec l'intention de vous faire rappeler. Cette escroquerie fonctionne, car les escrocs misent généralement sur le fait que la curiosité l'emportera sur votre jugement critique. Cependant, voici l'escroquerie : vous devez payer des frais lorsque vous passez l'appel, et les escrocs en profitent. Ces appels proviennent généralement d'un indicatif international, ce qui explique en partie pourquoi ils entraînent des frais. Parfois, un message vocal sera laissé, pour augmenter les chances que vous agissiez. Soyez donc vigilant si vous recevez un appel ou un message vocal d'un numéro que vous ne reconnaissez pas ou dont vous n'attendez aucun appel.

2. Comment éviter les escroqueries par appareil mobile

Chaque escroquerie a ses propres caractéristiques, mais celles-ci se résument généralement à quelques méthodes et objectifs communs. Comme de nouveaux types d'escroqueries apparaissent constamment, vous devez être prêt à faire face à l'inattendu. Pour éviter de tomber dans le piège de ces escroqueries par appareil mobile, vous devez être attentif à ce que l'on vous demande. En outre, vous pouvez mettre en place une meilleure protection tout au long de votre vie numérique pour assurer votre sécurité. Les escroqueries de toutes sortes consistent généralement à jouer sur vos émotions et à essayer d'établir une relation de confiance. Voici certaines des motivations émotionnelles qui sous-tendent les escroqueries :

- L'urgence ou les menaces peuvent vous inciter à agir plus rapidement. Si vous avez peur ou craignez de subir des conséquences si vous n'agissez pas, arrêtez-vous et posez des questions. Toute personne digne de confiance répondra à vos questions et vous permettra de vérifier que ses affirmations sont bien réelles. Les escrocs feront monter la pression. Les sujets les plus courants qui imposent l'urgence sont les dettes, les remboursements d'impôts ou les allégations de crimes fédéraux.

N'hésitez pas à vous rendre chez votre opérateur de téléphonie mobile pour des mesures concernant une proposition qui vous est faite par une tierce personne.

- L'empathie résulte d'une demande d'aide à d'autres personnes dans le besoin, ce qui vous empêche de refuser. Si vous vous sentez coupable de refuser ou de vous demander s'il s'agit d'une cause réelle, il s'agit peut-être d'un avertissement. Les escrocs peuvent prétendre faire partie d'une organisation caritative ou d'une autre cause sociale. Ils peuvent chercher à vous tromper en citant une catastrophe naturelle récente ou un autre sujet d'actualité dans le cadre de leur histoire.

- Les grandes promesses vous incitent à faire ce que l'escroc demande en échange d'une récompense. Soyez prudents si vous êtes excité à propos de l'offre ou si celle-ci fait naître un espoir. Par exemple, on peut vous annoncer que vous avez gagné un cadeau ou qu'on vous a offert une réduction importante sur un forfait de vacances. Dans le cadre de chaque escroquerie, on vous incite à donner suite à une demande.

Voici les demandes d'escroquerie les plus courantes auxquelles il faut faire attention :

- Effectuer un paiement, notamment en espèces ou parfois au moyen d'une carte cadeau. Il est difficile de se faire rembourser pour les achats effectués au moyen de ces modes de paiement.
- Communiquer des informations, comme un numéro de compte bancaire, un numéro de sécurité sociale ou un identifiant en ligne.
- Visiter un site Web via un lien pour vous connecter à un compte ou pour recevoir plus d'informations.
- Télécharger une application ou un fichier, par exemple une application antivirus.

Philippe MENGUE
22 ans, Étudiante en Communication et Marketing à l'Institut Supérieur de Technologie Appliquée et de Gestion, ISTAG, nous partage son experience.

-Fausses offres d'emploi

A l'ère du digital, beaucoup d'entreprises recourent au numérique pour déposer des offres d'emploi et ça se retrouvent vite fait dans facebook, whatsApp, et de fil en aiguille ça pullule dans les RS. À partir du téléphone on peut facilement répondre à une offre, le seul bémol, c'est qu'on ne sait plus qui est vrai dans ça. Des gens publient de fausses offres d'emploi pour des entreprises fictives et réussissent même à usurper le nom des boîtes sérieuses. J'ai été victime d'un faussaire et merci je ne suis pas aller plus loin dans la démarche. Il m'a demandé de l'argent pour analyser mon dossier ! *Pour ma part, dès qu'on demande de l'argent pour quoique ce soit, c'est du faux.*

-Publication des contenus obscènes

Prenons l'exemple de la jeune Cynthia F, ces vidéos ont fait le tour de la toile et conséquence directe : dépravation des mœurs, atteinte à la pudeur, incivisme... *A mon niveau moi je supprime et bloque l'expéditeur, ce n'est pas tout le monde qui veut avoir ces trucs dans son téléphone.*

-Arnaque dans le secteur téléphonique

J'ai été victime et maintenant je me méfie non seulement des numéros inconnus, mais aussi de donner mes pièces personnelles (CNI) à n'importe qui pour soi-disant faire une photocopie. De mon expérience, je pense qu'il est facile d'identifier le vrai du faux : les numéros des opérateurs sont courts (genre 9500, 8917, 8706...) et ceux des arnaqueurs sont des numéros ordinaires. Et plutôt que de t'embrouiller au téléphone, l'opérateur te renverra toujours au point le plus proche pour contact physique ! *Je ne reste même plus 5 secondes au téléphone avec un inconnu qui n'a rien de concret à me dire surtout s'il se passe pour un agent MTN ou ORANGE.*

FAKE NEWS DETECTOR

Préselectionné la à 3e édition de la Semaine de l'Innovation

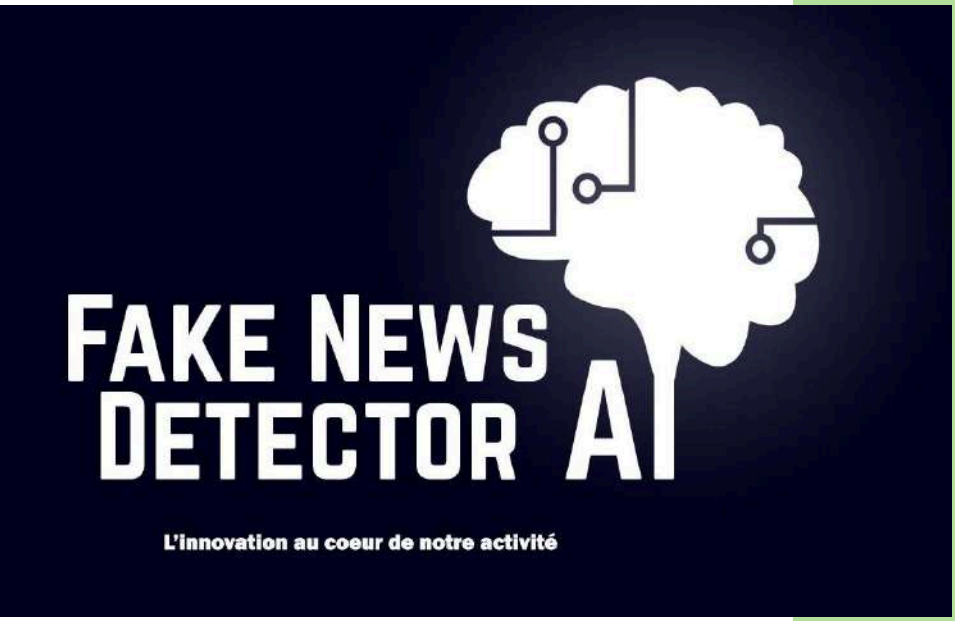
C'est quoi l'outil Fake news Detector ?

À l'heure du web, les réseaux sociaux prennent une place de plus en plus importante dans notre activité sur Internet. Ayant pour but initial de favoriser les relations avec des personnes qui se connaissent déjà, ils tendent à devenir des outils universels permettant de répondre au plus grand nombre possible de demandes : discuter et rester en contact avec ses proches, se divertir, se tenir informé... C'est dans ce dernier point que de fausses informations sont susceptibles d'apparaître. En effet, le terme «***Fake news***» désigne une fausse information, c'est-à-dire une information dont l'une ou toutes ses composantes sont erronées.

C'est dans l'optique de pouvoir prouver la véracité d'une information (ou sa ou ses composantes) que ***Bernadette ABODO*** et son équipe ont décidé de mettre sur pieds un logiciel basé sur l'intelligence artificielle et qui permet de détecter, comme le nom l'indique, si une information est vraie ou fausse.

Comment ça marche ?

Nous mettons sur pieds un système qui fonctionne automatiquement, instantanément, et basé sur de l'intelligence artificielle. Il permet d'alerter les utilisateurs du web et des réseaux sociaux si une information est vraie ou fausse. Cette application peut être installée sur téléphone et sur ordinateur et se synchronise aux comptes des uti-



Préselectionné à la 3e édition de la Semaine de l'Innovation Numérique

15e de la cuvée 2022,

a bénéficié de plusieurs formations et bootcamps organisés par le MINPOSTEL au CDIC

- Cinq Cent Milles (500.000) FCFA
- Don en matériel informatique

lisateurs tout en leur garantissant une protection de leurs données et une véracité des informations.

Pour vérifier une information ?

Notre logiciel sera capable :

- D'identifier la source de l'information afin de savoir si elle est fiable ou pas.
- De vérifier s'il y a eu une retouche d'une composante de l'information (d'image ou de vidéo).
- Nous utilisons aussi l'intervention de l'homme.

Quel a été l'apport ou l'approche du gouvernement dans le cadre de sa politique de soutien aux startups prometteuses de pareil projet ?

"Nous sommes aujourd'hui au règne des Fake news et Deep fakes. Ce qui n'est pas normal", regrette ***Madame la Ministre Minette LiBOM LIKENG*** sur son compte Twitter.
Il va s'en dire que les réseaux sociaux et le web en général bien qu'ils contribuent à l'essor de l'économie numérique et au développement social et culturel, restent des outils dont l'utilisation malveillante permet de distordre la réalité, des voies et moyens de créer

" Nous sommes aujourd'hui au règne des Fake news et Deep fakes. Ce qui n'est pas normal ", regrette Madame la Ministre Minette LiBOM LIKENG

la psychose pouvant rompre l'équilibre social. Ainsi c'est à travers des campagnes de sensibilisation menées par le ***MINPOSTEL (Ministère des Postes et des Télécommunications)*** que le gouvernement cherche à assurer l'intégrité des activités dans le cyberespace en tout en luttant contre la cyberdélinquance.
Œuvrant dans le même sens que cette vision et cet appel à l'utilisation responsable des réseaux sociaux, nous avons participé et avons été présélectionnés à ***la 3e édition de la Semaine de l'Innovation Numérique***. Une belle expérience de challenge qui a permis à l'équipe non seulement de se confronter à d'autres participants tous aussi déterminés, mais aussi à booster le niveau à travers les différen-tes formations et bootcamp organisés par le ***MINPOSTEL*** au ***CDIC***.

À la sortie du challenge, ***15e*** de la cuvée, nous avons également reçu la louable somme de C***inq Cent Milles (500.000) FCFA*** et du ***matériel informatique*** (ordinateur et autres) qui nous ont permis d'avancer dans l'élaboration de notre projet.


STOP!
FAKES
NEWS
Company
9:30 PM
Search
Cameroun - CAN 2021
Like
Comment
Share
ANTIC
LPE
Le Petit Ecrivain

La démarche RSE du Groupe SABC repose sur 5 axes

Education

Encourager la performance en milieu scolaire, seul gage de réel succès. Depuis 1948, la SABC promeut l'excellence et le culte de la performance dans le domaine de l'éducation, à travers des programmes d'octroi des bourses scolaires aux écoliers et élèves méritants et des stages académiques. Un investissement fort sur les générations futures.

Santé

La contribution du Groupe SABC dans le domaine de la santé consiste en :

-Promotion de l'hygiène et la salubrité en milieu scolaire

-Lutte contre l'hypertension artérielle et le diabete

-Promotion de la consommation responsable et la protection des jeunes contre l'alcool

-Promotion du sport pour la santé.

Environnement

Notre stratégie consiste en la réduction des pollutions causées par notre activité et à l'utilisation rationnelle des ressources naturelles et énergétiques. Cela s'est traduit par la construction de 5 stations d'épuration des eaux usées qui permettent de traiter en moyenne chaque année 1 343 195m^3 d'eaux.

De plus, nous avons planté 10 000 arbres en 2018 pour lutter contre la sécheresse dans les régions du septentrion.

Art et Culture

Grâce au partenariat que nous avons signé avec l'Institut Français du Cameroun, nous donnons l'occasion aux écoliers, élèves, étudiants, salariés et à tous les membres de la grande famille du Groupe SABC de profiter des programmes de cette institution pour enrichir leurs connaissances dans différents domaines (Littérature, art, culture, etc.). Pour faire de jeunes talents des stars, le Groupe SABC à travers la marque Mützig investit chaque année, plus de 200 millions de FCFA dans la prise en charge des candidats pendant le consours Mützig Star.

Sport

Depuis 1948, le Groupe SABC promeut les valeurs sportives au Cameroun et soutient plusieurs mouvements sportifs afin de créer une saine émulation entre les différents acteurs au Cameroun.

Les Brasseries du Cameroun font œuvre de pionnier en mars 1989 avec la création de l'Ecole de Football Brasseries du Cameroun. Son objectif ? Former des jeunes joueurs en leur inculquant dès leur plus bas âge, toutes les qualités sportives, humaines et morales nécessaires à l'émergence de leurs talents.

MINISTÈRE DES POSTES & TÉLÉCOMMUNICATIONS | www.minpostel.gov.cm

CAMPAGNE NATIONALE POUR LA PROMOTION DE LA CULTURE DE LA CYBERSÉCURITÉ ET SENSIBILISATION À L'UTILISATION RESPONSABLE DES RÉSEAUX SOCIAUX

NATIONAL CAMPAIGN TO PROMOTE THE CULTURE OF CYBERSECURITY AND RAISE AWARENESS ON THE RESPONSIBLE USE OF SOCIAL MEDIA

"Tous mobilisés pour la cybersécurité au Cameroun"

"let all mobilized for cybersecurity in Cameroon"

LE JOURNAL DE L'ETUDIANT

LPE Le Petit Ecrivain

« De ma position de Chef de l'Etat, j'aperçois les signes d'un frémissement qui prouvent que vous vous intéressez de plus en plus aux affaires publiques.

Les réseaux sociaux vous offrent à cet égard un champ d'expression de prédilection. Chaque fois qu'en un clic, vous empruntez ces autoroutes de la communication qui vous donnent une visibilité planétaire, il vous faut vous souvenir que vous n'êtes pas pour autant dispensés des obligations civiques et morales, telles que le respect de l'autre et des institutions de votre pays. Soyez des internautes patriotes qui œuvrent au développement et au rayonnement du Cameroun, non des followers passifs ou des relais naïfs des pourfendeurs de la République.

Le Cameroun de demain, qui se construit sous nos yeux, n'aura plus grand-chose à voir avec celui d'hier. Vous en serez les premiers bénéficiaires. Il faudra vous en montrer dignes. »

Message du Chef de l'Etat à la jeunesse le 10 février 2018.

« From my position as Head of State, I perceive signs of your growing interest in public affairs.

In this regard, your favourite platform of expression is the social media. Whenever at a click, you access these communication highways that give you global visibility, you must bear in mind that you are not exempted from fulfilling civic and moral obligations, such as respect for others and your country's institutions. Be patriotic Internet users working for Cameroon's development and influence, and not passive followers or naive relays for staunch critics of the Republic.

The Cameroon of tomorrow, which is being forged before our very own eyes, will differ almost entirely from that of yesteryear. You will be its key beneficiaries. You will need to prove yourselves worthy of it. »

Head of State's message to the youth, 10 february 2018

« *Sous l'autorité et la coordination du Premier Ministre Chef du Gouvernement les pouvoirs publics élaborent des stratégies pour adresser la problématique de la cybercriminalité* »

Joseph DION NGUTE, Premier Ministre Chef du Gouvernement

« *Under the coordination and authority of thé Primé Minister Head of Government the public authorities have been developping strategies to adress the problem of cybercrime* »

Joseph DION NGUTE, Prime Minister Head of Government

The interview,

Madam Minister of Posts & Telecommunications

1/ Today, a citizen with an appropriate mobile phone often finds himself at the start of or in the chain of dissemination of an image or news item, regardless of whether these images or news items are true or false. The persistent publication of "fake-news" in the mainstream or social media has contributed towards sustaining falsehood, thus preventing many of our fellow citizens from getting the right information on key issues. Can you tell us what "fake news" is?

The term ***"fake news"*** is made up of two English words ***"fake"*** and ***"news"*** which mean ***"false information"***. Fake news" is defined as information that is widely disseminated in the media, especially on the internet and social media, and that is deliberately falsified in order to deliberately mislead the public by trying to attract attention with something that is supposedly "authentic", to shock or to influence the opinion of others. They are written by individuals or groups acting in their own interests or on behalf of others. The creation and dissemination of fake news is mainly driven by personal, political or economic motivations.

2/ What is the social impact of spreading fake news?

Fake news is meant to manipulate public opinion and steer it in the direction desired by the manipulator. On the internet, false informa-tion and rumours can be spread anywhere and target anyone at any time. Social media have become the perfect place for the dissemination and propagation of all kinds of fake news. The spread of fake news can be the cause of poor education of the population, depravity of morals, social unrest, popular uprisings and instability of a country.

3/ How can fake news tarnish the image of an individual and even an institution?

Fake news is extremely damaging to the image of individuals and institutions. It can lead to their discredit or decredibility in the eyes of public opinion,

"Let all mobilised for cybersecurity in Cameroon"

thus causing a loss of trust. An individual who is the victim of fake news may miss out on a job he or she would have applied for, or lose a position of responsibility in an organisation, or even miss out on a promotion that was promised. They can also become the laughing stock of a compa-ny. Fake news has contributed to tarnishing the image of several high-profile personalities in our country. An institution can lose human and financial resources as a result of false informa-tion that has tarnished its image.

4/ "Lately, we have witnessed an upsurge in unpatriotic behaviour, the proliferation of hate speech and the posting of violent, obscene and shameful videotapes which have shocked the nation's collective conscience. The Head of State of Cameroon addressed his compatriots in his traditional end of year message in December 2021, in what and how can a student be identified with it?

Students and young people in particular, in their near majority, if not all, use smartphones, and are connected every day on the internet in general and on social media in particular. They are inevitably in contact with the information that is conveyed there, including fake news. There is a lot of information exchange within the student community and between the student community and the outside world. This justifies the term ***"android generation",*** used by the Head of State. Students and young people are therefore the most exposed segment of the population.

5/ "Therefore, I appeal to your sense of individual responsibility and urge each of you to promote the culture of peace. I call on the Government to step up efforts to raise awareness on the responsible use of social media by all social classes". How should we understand this appeal by the Head of State?

Generally speaking, in terms of security, there is no such thing as zero risk and man is the weakest link in the chain. It is therefore important to keep one's awareness up in the face of the abuses observed on the internet and in social media. To maintain this awareness, a permanent sensitisation on the best practices and uses of the internet and social media is of capital importance. This call from the Head of State shows that he is aware of the magnitude of the phenomenon of fake news and the risks that it can create for Cameroon. The Head of State made us to understand that security is a matter that concerns each and every one of us. The malicious use of social media and the Internet in general is a source of various

types of conflict between individuals. Above all, it is a source of social unrest and destabilisation of states. It is therefore essential for every citizen to contribute to maintaining peace through the responsible use of social media.

6/ What is the risk for a student to pu-blish/ share obscene and dishonourable videos?

The first risk is that of the sanctions provided for by the regulations. In Cameroon, there is a legal frame-work that governs activities online. Regardless of who is the perpetrator of a cyberoffence, ***Law No. 2010/ 012 of 21 December 2010*** on cybersecurity and cybercrime in Came-roon has provided for sanctions against the sharing or publication of mali-cious messages or videos. Here are some of them :

- Article 77: (1) Any person who, by means of electronic communications or an information system, commits an offence against a race or religion shall be punished with imprisonment of 2 to 5 years and a fine of 2,000,000 to 5,000,000 or one of the two penalties only.

(2) The penalties provided for in paragraph 1 above shall be doubled when the offence is committed with the aim of stirring up hatred or contempt between citizens.

- Article 77: (1) Any person who, by means of electronic communications or an information system, commits an offence against a race or religion shall be punished with imprisonment of 2 to 5 years and a fine of 2,000,000 to 5,000,000 or one of the two penalties only.

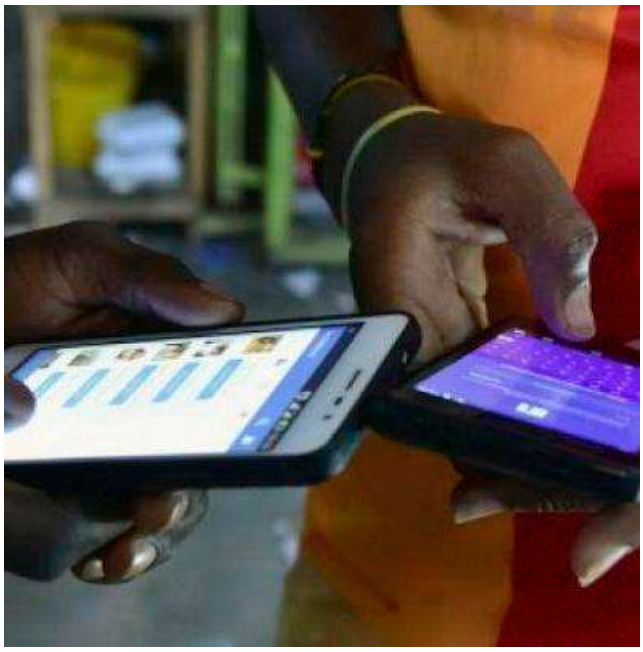
(2) The penalties provided for in paragraph 1 above shall be doubled when the offence is committed with the aim of stirring up hatred or contempt between citizens.

- Article 78: (1) Any person who publishes or propagates by means of electronic communications or an information system, a news item without being able to prove its veracity or justify that he had good reasons to believe in the truth of the said news item, shall be punished by an imprisonment of 6 months to 2 years and a fine of 5,000,000 to 10,000,000 or by one of these 2 penalties only.

(2) The penalties provided for in paragraph 1 above are doubled when the offence is committed with the aim of disturbing public peace.

- Article 80: (1) Any person who disseminates, fixes, records or transmits, for a fee or free of charge, an image showing paedophilic acts on a minor by means of electronic communications or an information sys-tem shall be punished by imprisonment of 3 to 6 years and a fine of 5,000,000 to 10,000,000 or by one of these 2 penalties only.

(2) Anyone who offers, makes available or disse-minates, imports or exports, by any electronic means



whatsoever, an image or representation of a paedophilic nature shall be punished by the same penalties as provided for in paragraph 1 above.
(3) Any person who holds in an electronic communications network or in an information system an image or representation of a paedophile nature shall be punished by imprisonment for a term of one to five years and a fine of 5,000,000 to 10,000,000 or by one of these two penalties only.
(4) The penalties provided for in paragraph 3 above shall be doubled where an electronic communications network has been used to disseminate the image or representation of the minor to the public.
(5) The provisions of this article are also applicable to pornographic images of minors.
Beyond these sanctions and many others provided for by the regulations of our country, in particular the penal code and the law mentioned above, it is necessary to warn our young people that everything posted on the Internet is not erased. As a result, their lives can be turned upside down overnight, because the information, photos or videos resurface a few years later, when they are least expected, putting an end to certain ambitions (political, employment, and others).

7/ What is the government's strategy to combat the fake news phenomenon?

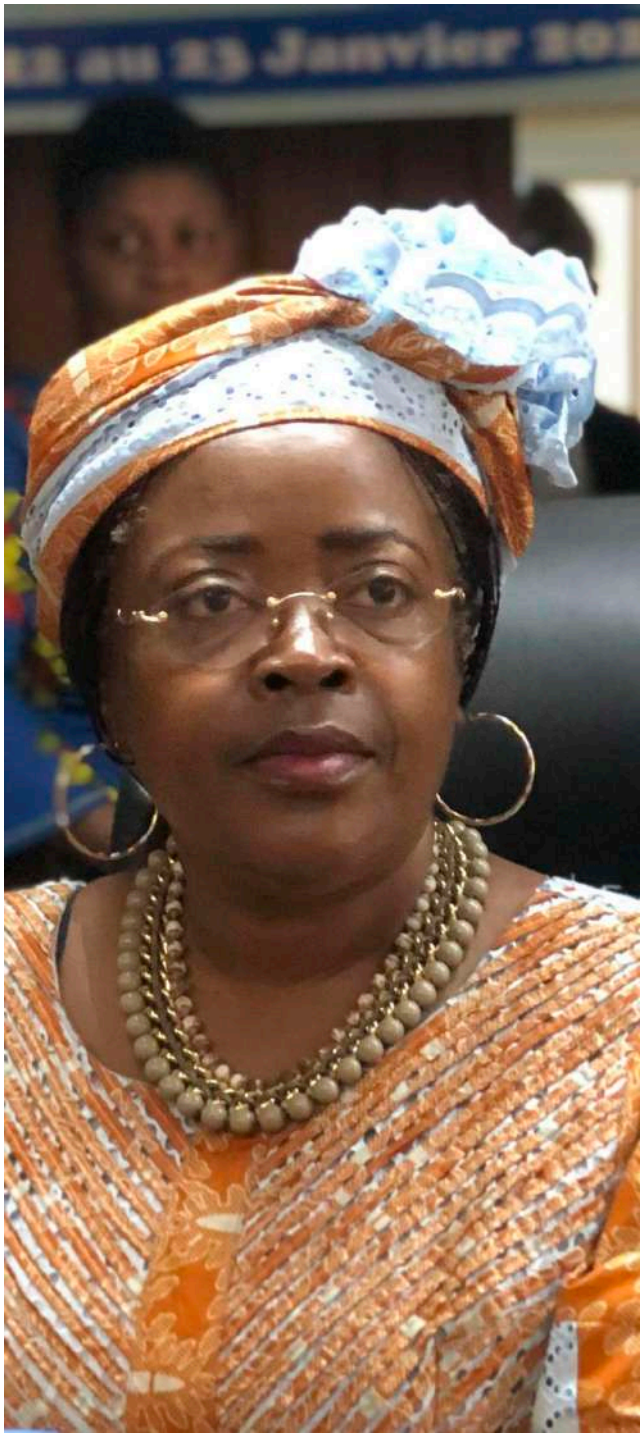
Cameroon has a government strategy to fight cybercrime, the objective of which is to build a safe and resilient cyber space. In addition, within this framework, we shall mention only three major strategic pillars, which are: The strengthening of the legal and regulatory framework, which we mentioned above. This law, which is already deterrent, is being updated to provide the government with a more severe legal instrument against cybercrimes, including disinformation, and is adapted to digital developments. In the area of regulation, the State has an Internet Regulator: NAICT, whose main mission is to fight cybercrime. Several other State structures are also at work: the SED, the DGSN and the DGRE. The second major guideline of this policy is the development of cybersecurity infrastructures that enable the prevention, detection and neutralisation of threats to networks and information systems. We would mention

In the event of a problem or to report abuses, use the ANTIC toll-free number: 8202

in particular the NAICT alert and response centre, the digital investigation laboratories of the Judicial Police Directorate. Finally, the last important component concerns awareness raising, capacity-building and change management, with the aim of increasing the skills of users to make better use of cyberspace. Reacting at the behest of the Head of State, the Ministry of Posts and Telecommunications has undertaken since 2020 a vast campaign to promote the culture of cybersecurity and raise awareness on the responsible use of social media.
Organised under the theme: ***"Let all mobilised for cybersecurity in Cameroon"***, this campaign is designed to mobilise all social classes in the fight against cybercrime and the misuse of social media and thus put in place a true national coalition for the promotion of civic use of social media. This campaign, which has been deployed successively in the Centre, Littoral, South-West, East and South regions, is set to intensify, following the recent revered Prescriptions of the Head of State. It is against this backdrop that awareness-raising operations through the media (TV, radio, social media, written press) and by SMS; billposting campaigns in public institutions and educational establishments were carried out. MINPOSTEL also has Goodwill Ambassadors for the culture of cybersecurity and the responsible use of social media, who also relay this awareness in their activities.

8/ How can young people participate?

Young people should be partners in the fight against false information on the internet. This is especially true as they tend to have a better understanding of how the internet and social media work. We commend the action of Goodwill Ambassadors and other part-



ners (Pressmen, Influencers, Professionals ...), who already accompany us in this fight, and who are very well equipped to sensitize other young people. In short, young people must be educated and sensitised. They should be more involved in awareness-raising campaigns because they are also more familiar with the content, trends and vocabulary likely to be appealing to young people, and can help to create content that will interest a wider audience and encourage them to change their behaviour. They should also be trained on tools to detect fake news.

9/ Will the creation or promotion of Cameroonian social media alleviate such deviant behaviour?

The creation of social media can only reduce deviant behaviour, not necessarily eradicate it. The current difficulty lies in the fact that the digital platforms that carry fake news are generally hosted in the USA and are therefore out of the control of Cameroonian authorities. The creation or promotion of local social media has the advantage that they will be better controlled at the national level, but education, awareness-raising of the population as well as the promotion and popularisation of tools for detecting fake news seem to be the most effective solutions for the time being.

10/ In the digital era, what advice can you provided to the so-called Android generation?

The so-called Android generation must adopt a civic-minded behaviour in social media. They must know that it is forbidden to spread false information, hateful, tribal and racist information. Young people must develop a critical mind and refuse to accept everything that is published on the internet and social media, without prior verification. They should not propagate or disseminate pornographic content, nor should they expose their own and other people's private lives on social media or the internet. Today, young people must always ask the following question, prior to the dissemination of information transferred to them: "why was it sent to me, is it proven to be true, and what are the consequences if I pass it on? ". Their future depends on it, the future of our country also depends on it.

Cybersecurity and the fight against Cybercrime DIGITAL SCAM

Expert/trainer Franck Arnold BAMA-SI
Engineer, PhD Student in Telecommunications

I- CASE OF FAKE JOB OFFERS

Some job offers posted on the Internet can be fraudulent. Cybercriminals pretend to be real recruiters to get money or personal information from victims.

1. What is a fake job offer scam ?

Some job offers posted on the Internet do not lead to real recruitment. They are apparently identical to real offers, most often very attractive to candidates, and comply with legal regulations on labour law (working hours, pay, etc.). Fraudsters who pretend to be real recruiters by using a company's name, address, the identity of an employee or a company manager, or its taxpayer number, create these fake job offers. Fraudsters make promises of a job without ever having met the jobseeker and send official-looking docu-ments (employment contract, application form, etc.) to reinforce their credibility.

Purpose

To extract money or steal personal information (bank details, national insurance number) for fraudu-lent use.

2. How to avoid this fraud ?

a. Beware of an offer that is too attractive or even out of the ordinary. Do not hesitate to talk about it with your friends and family or an employment professional (FNE, etc.).
b. Beware of unsolicited job offers. These offers are often sent to many people and your e-mail address is not always in the "recipient" field where several other names are present.
c. Beware of job offers that contain spelling mistakes or that ask you to reply to a "public domain" e-mail address. A large company will always send you a message from its domain name (for example: ***XX@minpos-tel.gov.cm*** and not ***erick258@XY.com).***
d. Never give a recruiter your personal details (bank details, social security number, account number or credit card number) until you have met them.
e. Do not pay any money to a potential employer for any reason (potential employment contract or pre-employment training) and by any means (purchase of prepaid cards or coupons, international express transfer).
f. Never buy materials on behalf of the company and never accept a cheque or bank transfer to make purchases for your job.
g. Do not accept any remuneration from your future employer until you have signed the employment contract.
h. Make sure that the company making the job offer is legally registered (trade register, taxpayer number).
i. Be careful if a recruiter contacts you at an unusual time or if he/she cannot meet you

because he/she is abroad.

j. Pay attention to what the recruiter says, especially if, for example, during the interview he or she offers you a different job than the one mentioned in the offer.

k. Do not continue the communication if you doubt the honesty of your interviewer.

l. Take the time to read carefully all the documents you are given and never sign a document without knowing exactly what you are committing yourself to.

m. Never cash cheques that are not from your employer. Even if the amount of a cheque deposited at your bank appears as a credit on your account, once the checks have been carried out (stolen cheque, etc.), the bank has several weeks to validate the transaction or cancel it by debiting the same amount from your account.

n. Keep your antivirus and operating system up to date.

3. What to do if you are a victim of a job scam ?

a) Immediately break off all relations with the pseudo recruiter, even if he or she is threatening by message or telephone.

b) Inform the organisation whose personal

data you have transmitted: if you have transmitted personal data (social security number, etc.), inform the organisation concerned (NSSF, NEF, etc.).

c) Inform your bank and regularly monitor the transactions on your accounts: if you have transmitted banking information, inform your bank and regularly monitor the transactions on your bank account.

d) Keep evidence, such as phone numbers, messages you have received or any other information that you can use to report the scam to the authorities. If you received the message by e-mail, keep it in a safe place.

e) Inform the organization whose identity has been stolen and/or the job site that posted the offer by providing, if possible, all the information you were able to collect to prove the job fraud (job offer reference, company name, name of the pseudo recruiter, contact information, etc.).

f) Report the facts to the National Agency for Information and Communication Technologies (NAICT) by calling 8202.

g) File a complaint: whether you are the victim of an attempted fraud, a theft of personal data or a financial fraud, file a complaint at the police station or at the gendarmerie brigade. This complaint will help you in your future steps in case of identity theft.

II- CASES OF SCAMS IN THE CELL PHONE SECTOR

The cell phone is one of the preferred playgrounds of criminals. Scams take different forms and have different objectives: money theft, identity theft, spying on your data...

1. What are phone scams?

Nowadays, cell phones are some of our most valuable assets, and cybercriminals are aware of this. We carry them with us all the time, and we use them to access some of the most private information in our lives. We have associated banking, email and other sensitive data with our phones, making them a perfectly centralized target for identity theft and fraud. The most common types of mobile device scams are :

Report the facts to the National Agency for Information and Communication Technologies (NAICT) by calling 8202

** Mobile Device Virus Scams*

Mobile device virus scams spread false alerts claiming that a virus has been detected on your phone. While browsing the web with your phone, you may have seen a page with this type of alert. The page will inform you that a scan of your phone has revealed a virus infection and will prompt you to take immediate action. Next, the scam prompts you to download an "antivirus" application, which is actually a malware or spyware. Once the malicious code is on your smartphone, the scammers can infect other devices or hijack yours. The easiest way to protect yourself from these types of attacks is to make sure your phone is equipped with a cybersecurity system, such as ***Android Anti-virus.***

** SMS phishing (smishing)*

SMS phishing, or "smishing", refers to a scam that tricks you into taking action via text message. Malicious links may be sent to you via SMS, and if you open the link, your device may be infected with malware or spyware. There may also be times when the criminal tricks you into taking a certain action. Other actions include calling a pay-per-minute phone number, getting you to sign up for a subscription, or coercing you to provide personal information.

** Voicemail Scams (Vishing)*

Vishing, or "voice phishing," refers to cell phone scams that trick you into doing something. Scammers pretend to be a genuine person or organization to gain your trust. They may pose as members of an official company or government department and convince you that you must provide personal information or money. These scams are designed to get you to act during the phone call. The scammers rely on ur-

gency and hope that you will react in a "panic" to give them what they want. This is why scammers will pressure you to make a payment or share information during the call itself, rather than asking you to call them back, (once they hang up).

* Missed Call Scams

Missed call scams are calls from an unknown number that only ring your phone once, with the intention of getting you to call back. This scam works because scammers usually bank on the fact that curiosity will override your critical judgment. However, here is the scam: you have to pay a fee when you make the call, and the scammers take advantage of it. These calls usually come from an international area code, which is part of the reason they charge. Sometimes a voicemail message will be left, to increase the chances that you will take action. So be careful if you receive a call or voice message from a number you do not recognize or from which you do not expect a call.

2. How to avoid mobile device scams

Each scam has its own characteristics, but these generally boil down to a few common methods and goals. As new types of scams are constantly appearing, you need to be prepared for the unexpected. To avoid falling for these mobile device scams, you need to pay attention to what you are being asked. In addition, you can put better protection in place throughout your digital life to ensure your safety. Scams of all kinds are usually about playing on your emotions and trying to build trust. Here are some of the emotional motivations behind scams :

- Urgency or threats may cause you to act more quickly. If you are afraid or fearful of consequences if you don't act, stop and ask questions. Anyone you trust will answer your questions and allow you to verify that their claims are true. Scammers will turn up the heat. The most common topics that impose urgency are debts, tax refunds or allegations of federal crimes.

- Empathy results from asking others in need for help, which prevents you from refusing. If you feel guilty about refusing or wondering if it is a real cause, it may be a red flag. Scammers may claim to be part of a charity or other social cause. They may seek to deceive you by citing a recent natural disaster or other current issue as part of their story.

- Lofty promises entice you to do what the scammer asks in exchange for a reward. Be cautious if you are excited about the offer or if it raises hopes. For example, you may be told that you have won a gift or have been offered a significant discount on a vacation package.

In every scam, you are encouraged to follow through on a request. These are the most common scam requests to watch out for :

- Making a payment, especially in cash or sometimes with a gift card. It is difficult to get reimbursed for purchases made with these payment methods.
- Giving out information, such as a bank account number, social security number or online ID.
- Visit a website via a link to log in to an account or to receive more information.
- Download an application or file, such as an anti-virus application.

Do not hesitate to go to your mobile operator for action regarding a proposal made to you by a third party.

Philippe MENGUE
22 years old, student in Communication and Marketing at the Institut Supérieur de Technologie Appliquée et de Gestion, ISTAG, shares her experience.

-Fake job offers

In this digital era, many companies use digital technology to post job offers and they quickly end up on facebook, WhatsApp, and one thing leading to another, they swarm in the social media. From the phone you can easily respond to a job offer, the only downside is that you do not know who is really behind it. Some people publish fake job offers for fictitious companies and even manage to usurp the names of serious companies. I was a victim of a fraudster and thanks to him; I did not go any further. He asked me for money to process my file ! *As far as I am concerned, as soon as someone asks for money for anything, it is a fake.*

-Publication of obscene content

Let us take the example of the young Cynthia F, whose videos went viral on the web and the direct consequence was: sexual depravity, indecent exposure, uncivil behaviour... *At my level, I delete and block the sender, not everyone wants to have these things in his phone.*

-Scam in the telephone sector

I have been a victim and now I am suspicious not only of unknown numbers, but also of giving my personal documents (CNI) to anyone to supposedly make a photocopy. From my experience, I think it is easy to identify the true from the fake: the operators' numbers are short (like 9500, 8917, 8706...) while scammers' numbers are the ordinary numbers. Rather than confusing you on the phone, the operator will always refer you to the nearest point for physical contact ! *I do not even stay 5 seconds on the phone with a stranger who has nothing concrete to tell me, especially if he pretends to be an MTN or ORANGE agent.*

FAKE NEWS DETECTOR

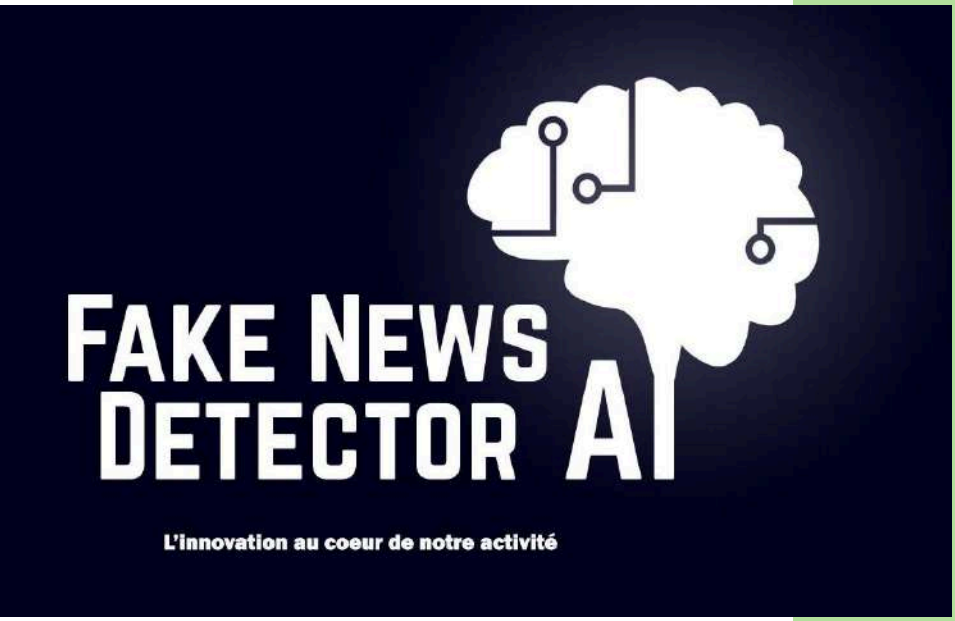
Shortlisted at the 3rd edition of the ICT Innovation Week

What is the Fake news Detector tool?

In this digital era, social media is becoming more and more important in our activity on the Internet. Initially intended to promote relationships with people who already know each other, they tend to become universal tools to meet the greatest possible number of demands: discuss and stay in touch with friends and family, have fun, stay informed ... It is in this last point that a fake information is likely to appear. Actually, the term ***"Fake news"*** refers to false information, in other words, information of which one or all its components are erroneous. It is with the aim of being able to prove the veracity of a piece of information (or its components) that **Bernadette ABODO** and her team have decided to set up a software based on artificial intelligence and which helps to detect, as the name indicates, if a piece of information is true or false.

How does it work?

We set up a system that works automatically, instantly, and based on artificial intelligence. It alerts web and social media users if a piece of information is true or false. This application can be installed on phones and computers and synchronizes with users' accounts while it guarantees the protection of their data and the veracity of the information.



Shortlisted at the 3rdedition of the ICT Innovation Week

15th of the 2022 competition,

benefited from several trainings and bootcamps organized by MINPOSTEL at CDIC

- Five hundred thousand (500,000) CFA Francs
- Donation of computer equipment

To verify information?

Our software will be able to:

- Identify the source of the information to know if it is reliable or not.
- Verify if there has been a modification of a component of the information (image or video).
- We also use human intervention.

What has been the contribution or approach of the government in its policy to support promising startups with such a project?

"Today we are in the reign of Fake news and Deep fakes. This is not normal," lamented ***Minister Minette LiBOM LIKENG*** on her Twitter account.
It goes without saying that social media and the web in general although they contribute to the growth of the digital economy and social and cultural development, remain tools whose malicious use can distort reality, as well as they can be ways and means to create psychosis that can break the social balance. Thus it is through awareness campaigns conducted by ***MINPOSTEL (Ministry of Posts and Telecommunications)*** that the government seeks to ensure the integrity of activities in the cyberspace while fighting against cybercrime.

"Today we are in the reign of Fake news and Deep fakes. This is not normal," lamented Minister Minette LIBOM LIKENG"

Working in the same vain as this vision and this call for the responsible use of social media, we participated and were shortlisted for the ***3rd edition of the ICT Innovation Week***. A great challenge experience that allowed the team not only to confront other equally determined participants, but also to boost their level through the various training sessions and bootcamp organized by ***MINPOSTEL*** at ***CDIC***. At the end of the challenge, 15th of the year, we also received the commendable sum of ***Five Hundred Thousand (500,000) CFA francs*** and ***computer equipment*** (computer and others) that allowed us to advance in the development of our project.


STOP!
FAKES
NEWS
Company
9:30 PM
Search
Cameroun - CAN 2021
Like
Comment
Share
CAMEROUN
POSTES ET TELECOMMUNICATIONS
ANTIC
LPE
Le Petit Ecrivain

La démarche RSE du Groupe SABC repose sur 5 axes

Education

Encourager la performance en milieu scolaire, seul gage de réel succès. Depuis 1948, la SABC promeut l'excellence et le culte de la performance dans le domaine de l'éducation, à travers des programmes d'octroi des bourses scolaires aux écoliers et élèves méritants et des stages académiques. Un investissement fort sur les générations futures.

Santé

La contribution du Groupe SABC dans le domaine de la santé consiste en :

-Promotion de l'hygiène et la salubrité en milieu scolaire

-Lutte contre l'hypertension artérielle et le diabete

-Promotion de la consommation responsable et la protection des jeunes contre l'alcool

-Promotion du sport pour la santé.

Environnement

Notre stratégie consiste en la réduction des pollutions causées par notre activité et à l'utilisation rationnelle des ressources naturelles et énergétiques. Cela s'est traduit par la construction de 5 stations d'épuration des eaux usées qui permettent de traiter en moyenne chaque année 1 343 195m^3 d'eaux.

De plus, nous avons planté 10 000 arbres en 2018 pour lutter contre la sécheresse dans les régions du septentrion.

Art et Culture

Grâce au partenariat que nous avons signé avec l'Institut Français du Cameroun, nous donnons l'occasion aux écoliers, élèves, étudiants, salariés et à tous les membres de la grande famille du Groupe SABC de profiter des programmes de cette institution pour enrichir leurs connaissances dans différents domaines (Littérature, art, culture, etc.). Pour faire de jeunes talents des stars, le Groupe SABC à travers la marque Mützig investit chaque année, plus de 200 millions de FCFA dans la prise en charge des candidats pendant le consours Mützig Star.

Sport

Depuis 1948, le Groupe SABC promeut les valeurs sportives au Cameroun et soutient plusieurs mouvements sportifs afin de créer une saine émulation entre les différents acteurs au Cameroun.

Les Brasseries du Cameroun font œuvre de pionnier en mars 1989 avec la création de l'Ecole de Football Brasseries du Cameroun. Son objectif ? Former des jeunes joueurs en leur inculquant dès leur plus bas âge, toutes les qualités sportives, humaines et morales nécessaires à l'émergence de leurs talents.