****

MINISTRY OF HIGHER

EDUCATION

\*\*\*\*\*\*\*

THE UNIVERSITY OF NGAOUNDERE

\*\*\*\*\*\*\*

FACULTY OF SCIENCE

\*\*\*\*\*\*\*

DEPARTEMENT OF MATHEMATICS AND COMPUTER SCIENCE

MINISTERE DES ENSEIGNEMENTS SUPERIEURS

\*\*\*\*\*\*\*

UNIVERSITE DE NGAOUNDERE

\*\*\*\*\*\*\*

FACULTE DES SCIENCES

\*\*\*\*\*\*\*

DEPARTEMET DE MATHEMATIQUE ET INFORMATIQUE

****

Filière : SYSTEMES ET LOGICIELS EN ENVIRONNEMENT DISTRIBUE

**UE: sécurité des systèmes et réseau**

**GROUPE 1.**

**Projet : Etude sur la sécurité des applications de paiement mobile sous Android**

Liste des membres :

1. TALA SIMO CECILE AUDE 16B739FS
2. ABDOUL WABOU EELH MAL YAYA 16B435FS
3. BABA SOULEY HAMIDOU 16B987FS
4. BELLO MAMOUDOU FIDELLE 15A412FS
5. MPON ADANG CHARLES 16B384FS
6. ABDOUL AZIZ 15A358FS
7. ABGOUDJA MAHAMAT OUMAR 16B387FS
8. ABDEL-HADI YUSSOUF ABDOULAYE 16A022FS
9. ALLAHASRA BEMADJIBEYE ISRAEL 16B104FS

**ENSEIGNANT: Dr Franklin Tchakounté**

**TUTRICE : Madame DJOYA ALIMA**

Année scolaire 2019\_2020

SOMMAIRE

[**Introduction 3**](#_Toc42542477)

[**I. Les 10 (dix) applications de paiement mobile les plus 4**](#_Toc42542478)

[**Exploitées au Cameroun : 4**](#_Toc42542479)

[**II. Citons quelques vulnérabilités les plus populaires dans ces applications tout en précisant si c’est un problème du côté développeur ou autres raisons. 4**](#_Toc42542480)

[**III. Méthodes et scénarios des différentes formes d’arnaques 8**](#_Toc42542481)

[**IV. Représentation sous forme d’automate générale 19**](#_Toc42542482)

[**1. Pour ORANGE MONEY 19**](#_Toc42542483)

[**2. Pour MTN MOBILE MONEY 20**](#_Toc42542484)

[**V. Implémentation d’un système intelligent : 21**](#_Toc42542485)

[**Conclusion 22**](#_Toc42542486)

[**References 23**](#_Toc42542487)

# Introduction

L’arnaque désigne le fait d’obtenir quelques choses par une manœuvre frauduleuse. Les arnaqueurs utilisent plusieurs moyens et méthodes pour escroquer les populations ; nous faisons allusion ici aux applications de paiement mobile vu qu’elles sont plus exploitées à cause de la crise sanitaire qui sévit dans le monde. Autrement dit ces applications étend plus utilisées pour diverse opérations sont devenus plus que jamais la cible des attaquants. Il est question pour nous dans ce projet d’investiguer sur les vulnérabilités des applications de paiement mobile les plus exploitées dans ce pays le Cameroun, de décrire quelques scenarios d’arnaques ; ensuite ressortir l’automate générale en s’appuyant sur les la sémantique des codes de MTN, ORANGE et enfin implémenter un système intelligent avec prolog pour permettre aux utilisateurs de connaitre en fonction du code en entré s’il s’agit d’une possibilité d’arnaques ou pas.

## **Les 10 (dix) applications de paiement mobile les plus**

## **Exploitées au Cameroun :**

* Orange Money,
* Express Union Mobile,
* MTN Mobile Money,
* Monetbil,
* Dohone,
* YUP,
* Mesomb
* Glomo Money
* Mobifone,
* Nexttel Possa.

Comme outils de détection des vulnérabilités nous pouvons citer entre autre : CHEX, QARK, Scandroid, Flwodroid, Collider, Horndroid, Amandroid, Mobile Security Framework, Findbugs, Error Prone, ARTdroid, Android lint, RevealDroid, TaintDroid ;

## **Citons quelques vulnérabilités les plus populaires dans ces applications tout en précisant si c’est un problème du côté développeur ou autres raisons**.

1. **ANALYSE STATIC DE « ORANGE MONEY V3.1.4 APK »**

Tout d’abord le statut de son certificat est ‘mauvais’ car l'application est signée avec SHA1 RSA. Or l'algorithme de hachage SHA1 est connu pour avoir des problèmes de collision

* Dans le manifeste, on constate que l’activité (com.orange.orangemoneylib.activity.ExternalSplashScreen) n’est pas protégée. Il existe un filtre d'intention
* Au niveau du fichier “defpackage/af.java” une activité se trouve être partagée avec d'autres applications sur l'appareil, ce qui la rend accessible à toute autre application sur l'appareil. La présence d'un filtre d'intention indique que l'activité est explicitement exportée. L'application utilise la base de données SQLite et exécute une requête SQL brute. Une entrée utilisateur non fiable dans les requêtes SQL brutes peut provoquer une injection SQL. Les informations sensibles doivent également être cryptées et écrites dans la base de données.
* Au niveau du fichier “defpackage/x.java” la mise en œuvre non sécurisée du SSL... fait confiance à tous les certificats ou accepter des certificats auto signés est une faille de sécurité critique. Cette application est vulnérable aux attaques du MITM

1. **ANALYSE STATIC DE « YUP 1.0 APK »**

* Au niveau du manifest l’activité (com.yup.app.MainActivity) n’est pas protégé car le programmeur à mi [android :exported=true] ainsi une activité s'avère être partagée avec d'autres applications sur l'appareil, ce qui la rend accessible à toute autre application sur l'appareil.
* Le service (com.yup.helper.MyFirebaseInstanceIDService) n’est pas protéger car le programmeur à mi [android :exported=true] ainsi un service s'avère être partagé avec d'autres applications sur l'appareil, ce qui le rend accessible à toute autre application sur l'appareil.
* Mode de lancement de l'activité (org.acra.dialog.CrashReportDialog) n'est pas une norme ainsi une activité ne doit pas avoir l'attribut "mode de lancement" réglé sur “singleTask/singleInstance” car il devient l'activité racine et il est possible pour d'autres applications de lire le contenu de l'intention d'appel. Il est donc nécessaire d'utiliser l'attribut "standard" du mode de lancement lorsque des informations sensibles sont incluses dans une intention
* Le service (com.google.android.gms.auth.api.signin.RevocationBoundService) est protégé par une autorisation, mais le niveau de protection de l'autorisation doit être vérifié. De même la permission (com.google.android.gms.auth.api.signin.permission.REVOCATION\_NOTIFICATI ON) [android :exported=true] ainsi un service s'avère être partagé avec d'autres applications sur l'appareil, le laissant ainsi accessible à toute autre application sur l'appareil. Il est protégé par une autorisation qui n'est pas définie dans l'application analysée. Par conséquent, le niveau de protection de l'autorisation doit être vérifié là où il est défini. S'il est défini comme normal ou dangereux, une application malveillante et interagir avec le composant. S'il est défini sur signature, seules les applications signées avec le même certificat peuvent obtenir la permission
* Récepteur de radiodiffusion (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) n'est pas protégée par une autorisation, mais le niveau de protection de l'autorisation doit être vérifié.
* Autorisation : android.permission.INSTALL\_PACKAGES [android :exported=true] ainsi un service s'avère être partagé avec d'autres applications sur l'appareil, le laissant ainsi accessible à toute autre application sur l'appareil. Il est protégé par une autorisation qui n'est pas définie dans l'application analysée. Par conséquent, le niveau de protection de l'autorisation doit être vérifié là où il est défini. S'il est défini comme normal ou dangereux, une application malveillante et interagir avec le composant. S'il est défini sur signature, seules les applications signées avec le même certificat peuvent obtenir la permission.
* Cette application utilise le Java Hash Code. C'est une fonction de hachage faible et ne devrait jamais être utilisée dans une implémentation Crypto sécurisée.
* L'application enregistre les informations. Les informations sensibles ne doivent jamais être enregistrées.
* L'application peut lire/écrire sur le stockage externe. Toute application peut lire les données écrites sur le stockage externe.
* L'application utilise un générateur de nombres aléatoires peu sûr
* Les fichiers peuvent contenir des informations sensibles codées en dur comme des noms d'utilisateur, des mots de passe, des clés
* Une entrée utilisateur non fiable dans les requêtes SQL brutes peut provoquer une injection SQL. Les données sensibles doivent également être cryptées et écrites dans la base de données.

1. **ANALYSE STATIC DE « EU Mobile Money V1.18 APK »**

* Le statut de son certificat est "mauvais" car l'application est signée avec SHA1 RSA. Or l'algorithme de hachage SHA1 est connu pour avoir des problèmes de collision
* Le trafic de texte en clair est activé pour l'application [android:usesCleartextTraffic=true] ainsi l'application prévoit d'utiliser le trafic réseau en clair, comme le HTTP en clair, les piles FTP, le DownloadManager et le MediaPlayer. La valeur par défaut pour les applications qui visent le niveau 27 de l'API ou un niveau inférieur est "true". La valeur par défaut des applications qui ciblent le niveau 28 ou plus de l'API est "false". La principale raison d'éviter le trafic en texte clair est le manque de confidentialité, d'authenticité et de protection contre la falsification ; un attaquant réseau peut écouter les données transmises et les modifier sans être détecté>
* Le Service (com.google.android.gms.auth.api.signin.RevocationBoundService) est protégé par une autorisation, mais le niveau de protection de l'autorisation doit être vérifié.
* La permission : (com.google.android.gms.auth.api.signin.permission.REVOCATION\_NOTIFICATI ON) [android :exported=true] ainsi un service s'avère être partagé avec d'autres applications sur l'appareil, le laissant ainsi accessible à toute autre application sur l'appareil. Il est protégé par une autorisation qui n'est pas définie dans l'application analysée. Par conséquent, le niveau de protection de l'autorisation doit être vérifié là où il est défini. S'il est défini comme normal ou dangereux, une application malveillante et interagir avec le composant. Si elle est définie sur signature, seules les applications signées avec le même certificat peuvent obtenir la permission.
* Le Service (com.google.firebase.iid.FirebaseInstanceIdService) n'est pas protégée car [android:exported=true] et Un service s'avère être partagé avec d'autres applications sur l'appareil, le laissant ainsi accessible à toute autre application sur l'appareil.
* Cette application utilise le code Java Hash. C'est une fonction de hachage faible et ne devrait jamais être utilisée dans une implémentation de cryptage sécurisé.
* Le MD5 est un hachisch faible connu pour avoir des collisions de hachisch

1. **ANALYSE STATIC DE « Nexttel Possa V1.4.2 APK »**

* Le service (com.nexttel.possa.services.MyFirebaseMessagingService) n'est pas protégée car [android:export=true] ainsi Un service s'avère être partagé avec d'autres applications sur l'appareil, ce qui le rend accessible à toute autre application sur l'appareil.
* Le service (com.nexttel.possa.services.MyFirebseInstanceIDService) n'est pas protégé. Il existe un filtre d'intention. Ainsi, un service est partagé avec d'autres applications sur l'appareil, le rendant ainsi accessible à toute autre application sur l'appareil. La présence d'un filtre d'intention indique que le service est explicitement exporté.
* Le Broadcast Receiver (Récepteur de radiodiffusion) (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) est protégé par une autorisation, mais le niveau de protection de l'autorisation doit être vérifié.
* La Permission: android.permission.INSTALL\_PACKAGES [android :exported=true] ainsi Un récepteur de radiodiffusion est partagé avec d'autres applications sur l'appareil, ce qui le rend accessible à toute autre application sur l'appareil. Il est protégé par une autorisation qui n'est pas définie dans l'application analysée. Par conséquent, le niveau de protection de l'autorisation doit être vérifié là où il est défini. S'il est défini comme normal ou dangereux, une application malveillante peut demander et obtenir la permission et interagir avec le composant. Si elle est définie sur signature, seules les applications signées avec le même certificat peuvent obtenir la permission.
* L'application utilise un générateur de nombres aléatoires peu sûr ➢ Le MD5 est un hachisch faible connu pour ses collisions avec le hachisch

1. **ANALYSE STATIC DE « MTN MoMo V1.0.1 APK ».**

* Tout d’abord son le statut de son certificat est 'mauvais' car l'application est signée avec SHA1 RSA. L'algorithme de hachage SHA1 est connu pour avoir des problèmes de collision.
* Le trafic de texte en clair est activé pour l'application car [android:usesClearTraffic=true] ainsi l'application prévoit d'utiliser le trafic réseau en clair, comme le HTTP en clair, les piles FTP, le DownloadManager et le MediaPlayer. La valeur par défaut pour les applications qui visent le niveau 27 de l'API ou un niveau inférieur est "true". La valeur par défaut des applications qui ciblent le niveau 28 ou plus de l'API est "false". La principale raison d'éviter le trafic en texte clair est le manque de confidentialité, d'authenticité et de protection contre la falsification ; un attaquant réseau peut écouter les données transmises et les modifier sans être détecté
* Le mode de lancement de l'activité (com.comviva.webaxn.ui.WebAxnActivity) n'est pas standard. Ainsi

## **Méthodes et scénarios des différentes formes d’arnaques**

Les attaquants utilises régulièrement plusieurs méthodes (les arnaques : par appel, par message, par points de vente, via le E-Commerce, les réseaux sociaux, par bout de papier, etc.) pour escroquer les utilisateurs ou encore en s’attaquant à la maison directement. Ainsi les différents scénarios d’arnaques par le paiement mobile au Cameroun sont :

1. Un appel disant MTN vous offre 50% de bonus sur le montant que vous avez dans votre compte; pour bénéficier de cela composer le … et quelques minutes après vous recevez un message disant « le transfert d’argent a été bien effectuer ».
2. Lorsqu’on active le forfait internet OM deals via l’opérateur Orange Money en tapant le code #150\*2\*3# on se limite à notre forfait mais en installant un VPN comme AnonyTun ou http Injector on peut surfer sans limite et perturbation durant la validité de notre forfait.
3. Lorsqu’on tape #150\*11#, l’opérateur nous demande d’ajouter le numéro du bénéficiaire et si on est fourni pas de réponse pendent un certain temps, une erreur ou arrêt se produit et on doit recommencer l’opération à zéro
4. Une personne te contacte par appel et dit qu’il a fait une erreur en faisant un dépôt sur votre compte :

-Bonjour madame, veillez m’excuser du dérangement, je vous ai fait un dépôt dans votre compte avez-vous reçu sinon vérifier votre boite de réception ensuite il vous demande de retirer un 10000(un montant) sur cette argent et transféré le reste svp qu’il a besoin de cette argent urgemment .La victime dans la panique, joie (bref je ne sais pas comment caractériser cela) ne fait aucune vérification et commence la transaction.

1. Vous faite connaissance avec une personne sur les réseaux sociaux et après un bout de temps (question pour lui de gagner votre confiance) elle vous dit qu’elle se trouve dans une situation compliquée et sollicite votre aide :

* Désolé vraiment, ma mère est aux urgences a besoin d’argent et là ou je suis-je ne peux pas faire de retrait car il n’y a pas de cabinet pour MTN ici, si vous pouvez m’aider à retirer l’argent dans mon compte et m’envoyer à orange.
* Ok pas de soucis, directement vous vous rendez devant un cabinet, le gérant lance le retrait sur son numéro
* L’arnaquer sans valider le message pour le retrait original envoi automatiquement un faux message »Le retrait à été effectuer avec les références sur le numéro du gérant ».

Et c’est comme ça que vous risquez d’être dans les ennuis.

1. "ORANGE!!! PROMO !!! PRIME!!! cher(e) client (e)vu votre consommation durant l'année ''2015''2016'' votre numéro a été tiré au sort; vous êtes gagnant (e)d'une somme de [400.000frs] veuillez appeler au numéro standard:[696832021] pour le retirer."
2. "BIENVENU AU SERVICE ORANGE PRIME PROMO 2016. Bravo oh!! Mr/Mme à l'occurrence de l'année 2016, du à vos multiples recharges effectuées, après tirage au sort dans les 10 régions votre numéro est tiré gagnant! vous bénéficiez d'une prime de [380.000frs] et Un Séjour A Kribi veuillez contacter votre service orange PRIME PROMO en partenariat avec le service EXPRESS UNION au numéro standard <> pour les modalités. orange vous remercie de votre fidélité.
3. Vous recevez le message « Orange ci : cher client votre numéro gagne des lots et bonus pour plus d’info  contacter l’agent commercial au 49 24 06 27 » et lorsque vous appelez on demande de composer le code suivant : #144\*1\*59886763\*0089955\*code secret orange money#
4. La technique consiste à introduire la carte identité ou le passeport du client dans la photocopieuse. C’est ensuite que ces délinquants informent l’intéressé que l’ancre n’a pas bien pris le format. C’est alors qu’ils jettent la première photocopie dans la poubelle, refont une autre qui plus claire et la remettent enfin au client. Seulement, la première photocopie qui est restée dans la poubelle va permettre à celui qui a photocopié d’accomplir sa sale besogne. Comme le cas de cette dame qu’on va nommer Mme xxx « J’avais logé dans mon compte orange money une somme de 80.000 Fcfa et jeudi passé j’ai reçu un message d’orange m’informant que je viens d’effectuer avec succès un retrait de 78.000 Fcfa. Aussitôt je me suis rendu à la direction d’Orange et voilà, c’est un individu qui est allé braquer mon compte au moyen de mon identification, je ne sais comment il a fait pour avoir mon code secret mais entre-temps, je reconnais avoir photocopié mon passeport quatre jours avant, auprès d’une dame installée à l’entrée du Tribunal criminel spécial. Une plainte a déjà été déposée contre inconnu »
5. Les arnaqueurs appellent leur victime en lui disant que son compte Orange Mobile n’est pas à jour. Ils proposent de l’aider à y remédier à distance, lui assurant que cette solution est l’une des mesures prises par Orange pour limiter les contacts dans le contexte de la crise sanitaire actuelle. Une fois que la victime a donné son assentiment, elle est invitée à taper un code pour que son compte soit à jour. Une fois que le code saisi, les arnaqueurs auront accès à votre compte et pourront ainsi soutirer l’argent qui s’y trouve.
6. « Mobile Money, vous avez reçu 56 500 FCFA de Achiri Walters Sonde (237 677 62 09 53) le 2018-11-23. 10 : 13 :31. Transaction Id : 445749491. Reference : 00000. Nouveau solde 59 500 FCFA ». Après le SMS, les victimes sont appelées pour qu’il communique leur code secret Mobile Money.
7. Les spécialistes d’arnaques au porte-monnaie électronique n’arrêtent pas le progrès. C’est ce que l’on peut dire à la lecture de la publication d’une internaute enregistrée sur Facebook sous le nom d’Ehivet Grâce Kouadio. Selon elle, hier sa mère aurait reçu un dépôt de 114.000 Francs CFA sur Orange à 21 heures. Elle consulte son solde qui est alors à 226 000 Francs CFA. Plus aucun doute puisqu’elle n’avait que 112.000 Francs CFA. Cinq minutes après, elle reçoit un appel. Son interlocuteur semble désemparé. Il lui confie s’être trompé et la supplie de lui ramener 90.000 Francs CFA les 24.000 Francs CFA restant étant un cadeau pour la remercier. En pleurs, il explique que les 90.000 Francs CFA serviront à soigner son frère gravement malade. La maman bien que disposée à rendre la totalité de l’argent, n’entend pas le faire nuitamment. Elle le fera le lendemain non pas de son portable mais d’une agence. Deux précautions valent mieux qu’une dit-on. Les supplications de l’homme n’y changeront rien. L’homme se résout à la rappeler le lendemain. Ce matin à 09 heures la maman de l’internaute se serait rendue à un point orange en vue d’effectuer la transaction comme promis. Elle décide de retirer d’abord 100.000 Francs CFA et là surprise, l’opérateur lui communique son solde résiduel qui n’est plus que de 112.000 Francs CFA. Elle ne sait par quel mécanisme les 114.000 Francs CFA indûment reçus la veille se sont volatilisés ne laissant que les 112.000 Francs qu’elle avait sur son compte. Jusqu’à 13 heures l’homme n’avait toujours pas appelé.
8. Quelques heures après avoir reçu un dépôt d’argent sur mon compte Orange Money, je reçois un appel. La voix au bout du fil se veut rassurante. Un responsable d’agence soucieux de la qualité de son service ; chose plutôt rare. Il venait vérifier que la transaction a réussi, car selon lui, le transfert de plusieurs clients effectués au cours de la journée, dans son agence, aurait échoué. Il tente de me mettre en confiance en disant le montant exact de la transaction et la ville. Je lui réponds que j’ai bien reçu ladite somme et le remercie de se soucier de ses clients. Je demande son nom, il n’hésite pas à me dire un nom. Puis il me dit qu’au retrait, au cas où il se poserait un problème, je devrais composer la syntaxe suivante : (#144\*621\*Code secret OM#). Je lui dis merci. Avant de me dire au revoir, il me dit qu’il m’appellerait pour s’assurer que j’ai effectivement composé ladite syntaxe. Incohérence, puisque je ne lui ai pas dit que je retirerais mon argent sur le champ ! Ce code généré n’est valable que pour cinq minutes et permet d’effectuer un seul retrait n’excédant pas la somme de 100.000 FCFA. Dans mon scénario, l’individu a déjà mon numéro et une idée du montant qui se trouve sur mon compte. Il ne lui reste que le code d’autorisation, qu’il m’aurait demandé afin de vider mon compte.
9. ORANGE PROMO 2018\_\_BRAVOOOO !!!Cher(e) client(e), votre numéro a été sélectionner par le « MEGAWIN2017-2018 »net vous vous a permis de bénéficier d’une prime de bonus de [280000]FCFA. Pour activer le reversement de votre compte orange Money, contactez le standard du service promotionnel au: [698907533].Orange vous remercie de votre fidélité. La vie change avec orange !!!
10. Arnaque par demande de retrait à travers un compte client quelconque : Claudia. N. a reçu en pleine nuit, un message ou il lui était demander de valider un retrait d’argent. Elle le supprime aussi tôt et se replonge dans le sommeil. Quelques minutes plus tard, un message similaire s’affiche. Elle annule encore. Arnaqueur à utiliser une technique très bref, lorsque la victime se précipite et valide la transaction alors elle se fait arnaquer.
11. Arnaque par l’envoi d’un message notifiant que vous avez reçu un dépôt par erreur : L’arnaqueur vous envoie un message de transfert d’argent et vous appel disant qu’il a fait une erreur lors de l’envoi, et vous supplie de le transférer la moitie. Une fois valider votre code secret alors l’arnaqueur profite et vide votre compte.
12. Arnaque par technique de bout de papier : Le client se rend dans un point de distribution mobile pour effectue un dépôt d’argent dans un compte. Il remet l’argent à déposer (un montant relativement important) à l’opérateur. Après que ce dernier est fini de compte l’argent et vérifier l’authenticité des billets, le client lui passe un bout de papier sous lequel est écrit le numéro de compte qui doit recevoir le dépôt d’argent. Si ce client n’est pas entre dans la boutique en conversation au téléphone, c’est à ce moment qu’il lance un appel. Pendant ce temps, l’opérateur initie la transaction pour le dépôt. À l’étape où l’opérateur communique le nom du bénéficiaire, le client se fait distrait au téléphone et demande à l’opérateur de lui remettre le bout de papier avec le numéro du dépôt. Ensuite, le/la client remet après quelques instants à l’opérateur, un bout de papier identique à celui qui a d’abord été donné mais à la différence que, sur ce nouveau bout de papier, le numéro est différent du premier ! La différence est au niveau généralement d’un chiffre. Le client toujours au téléphone, ne confirme pas le nom du bénéficiaire et dit plutôt à l’opérateur que c’est le numéro qui est sur le bout de papier. Si l’opérateur n’est pas vigilant, il va déposer l’argent dans le compte du premier numéro qui lui a été remis sur le bout de papier. Dès que le client est sûr que l’argent a été déposé, il va consulter le solde de son compte et dire à l’opérateur qu’il n’a encore rien reçu et demander par la suite de vérifier le numéro sur le bout de papier. En vérifiant, l’opérateur se rendra vite compte que le numéro n’est pas le même et croira que c’est lui/elle qui a fait erreur.
13. Arnaque par distraction d’un agent Orange Money ou MoMo : Un groupe de personnes arrive dans un point de retrait et demande à la fois à l’agent de faire un retrait et d’autre dépôt. Une fois l’agent est occupé alors il distrait en disant qu’il a déjà remis une somme pour le dépôt.
14. Arnaque par réception d’un message via une adresse email : L’arnaqueur envoie un message via l’adresse email contenant un lien qui permettra à la victime réinitialise son compte, une fois entre ces informations personnelles alors l’arnaqueur récupère ces informations nécessaires et accèdent à son compte.
15. **Des personnes se présentant comme agents de l’une des entreprises de téléphonie mobile appâtent leurs cibles par des gains faramineux :** Lambert N. a vécu une triste aventure le 29 octobre dernier. Alors que cet habitant de la ville de Bafoussam mène paisiblement ses activités quotidiennes, il reçoit un message venant d’un abonné au réseau Orange, indiquant que son numéro a été tiré au sort en raison de son importante consommation de crédit téléphonique au cours des années 2015 et 2016. Le message était accompagné d’un numéro de téléphone présenté comme celui du standard avec qui, Lambert devait prendre attache pour ample information. Très enthousiaste, cet homme le fait, sans se poser de question. « J’ai appelé le numéro du standard (supposé), la personne qui était à l’autre bout de la ligne m’a fait savoir que mon numéro a été tiré au sort et que Orange m’offre 400 000 FCFA »*,* explique-t-il. Ayant visiblement constaté que le poisson est entrain de mordre l’hameçon, son bourreau va passer à la vitesse supérieure. Et lui demande de faire le transfert d’un montant de 10 500 FCFA dans son propre compte « Orange Money » et de revenir vers eux pour la suite qui se passe de tout commentaire. « Je suis allé faire le transfert dans mon compte et quand j’ai rappelé, il m’a demandé de suivre les instructions qu’il aller me donner au fur et à mesure. Quand je l’ai fait le transfert que je venais d’effectuer dans mon compte a tout disparu »*,* ajoute-t-il. A partir de cet instant, il commence à soupçonner qu’il serait la cible des arnaqueurs, mais ne désespère pas. Par la suite, son interlocuteur virtuel lui fait parvenir un autre message lui demandant ses coordonnées (nom et prénom complets ; ville de résidence ; numéro de cni…). Toutes ses coordonnes lui sont retournées en lui demandant de faire un autre transfert, cette fois-là, d’une somme de 20 000 FCFA afin que lui soit envoyé le code pour aller toucher les 400 000 FCFA dans une micro finance spécialisée dans le transfert d’argent. Le doute va dès lors s’enfler et Lambert s’arrêtera là, convaincu d’avoir été arnaqué.
16. Arnaque direct: Lors d’un voyage ou d’agression, l’arnaqueur force le client à lui fournir son code mobile pour qu’il vider le compte.
17. Bravos !!! cher(e) client(e) à l’occurrence du à vos transactions et opérations faite durant l’année, votre numéro a été tiré au sort vous bénéficiez d’une prime de bonus de [180000], un écran plasma 42 pouces, un téléphone 4G et un parapluie ORG. Appelez immédiatement M. Vincent responsable du service promotionnel Orange pour le reversement et le retrait de vos lots au numéro standard [6997785456].ensuite allez retirer vos lots aux agences ORANGE MONEY du territoire national. Orange vous remercie de votre fidélité.
18. Manny reçoit un dépôt orange de 114000fcfa, elle avait d’abord une somme de 112000fcfa dans son compte, elle consulte son solde et voit belle et bien un montant 226000fcfa le nouveau solde ; 5minutes après un monsieur l’appelle pour lui demander pardon de renvoyer 90000fcfa que c’est pour acheter des médicaments son ami est entre la vie et la mort qu’il a urgemment besoin de cette argent et de garder les 24000F restant. Manny répond en disant qu’elle ne peut pas garder cette somme et que le lendemain elle va ramener tout mais qu’elle préfère retirer dans une agence avant de transfère après afin d’éviter d’être arnaquer, le monsieur pleurait déjà disant que son amis risque de mourir mais elle ne céda point et raccrocha le téléphone. le lendemain elle est allée faire le retrait, voulant vérifier une seconde fois elle s’est rendu compte qu’il ne restait plus que 112000 dans son compte.si elle n’était pas très prudente ce monsieur devait l’arnaquer mais ces plans n’ont pas réussi.
19. Un arnaqueur t’appel et dit qu’il est un agent de orange que tes points orange s’élevé à 52500 qu’il faut verse dans ton compte mais avant il demande le solde que tu as dans ton compte ensuite il te demande de composer une suite de code sur un autre téléphone y compris votre mot de passe dans ce code et également le montant.si vous exécuté ces codes un montant sera débité de votre compte.
20. Un monsieur vous appelle et vous met sur le coup de l’émotion avec quelque mot ensuite il demande de composer le #150\*44# ensuite le code secret, vous recevez un message et l’arnaquer vous demande de lui communiquer le code sur le message (c’est le code de paiement) .entre temps il un déjà sur un site de vente en ligne prêt à utiliser ce code pour faire un paiement en ligne. votre compte est débité du montant de son article.
21. Au cours de l’année 2018-2019 à l’université de Ngaoundéré ; une étudiante Y de niveau 1 était victime d’une arnaque qui s’était déroulée comme suit :

Il était mis en scène deux personnages fictifs ; l’une malade se trouvant à Dang ; qui a usurpé l’identité Z de l’amie de la victime et l’autre (le tuteur du malade) se trouve à N’Djamena. Le personnage Z a fait savoir qu’il va recevoir via l’EUM de la victime un dépôt de 40 000 Francs pour qu’elle puisse soigner sa maladie (sous prétexte que son passeport était oublié à la maison et qu’elle en a besoin de cet argent urgemment). La victime dans sa réaction naïve a envoyé les 40 000 Francs dans le compte OM du sois disant malade avant même que le dépôt qui devrait venir du tuteur ne soit effectué… Une fois la transaction effectuée, les personnages fictifs ne répondaient plus.

1. Lambert N. a vécu une triste aventure le 29 octobre dernier. Alors que cet habitant de la ville de Bafoussam mène paisiblement ses activités  quotidiennes, il reçoit un message venant d’un abonné au réseau Orange, indiquant que son numéro a été tiré au sort en raison de son importante consommation de crédit téléphonique au cours des années 2015 et 2016. Le message était accompagné d’un numéro de téléphone présenté comme celui du standard avec qui, Lambert devait prendre attache pour ample information. Très enthousiaste, cet homme le fait, sans se poser de question. « J’ai appelé le numéro du standard (supposé), la personne qui était à l’autre bout de la ligne m’a fait savoir que mon numéro a été tiré au sort et que Orange m’offre 400 000 FCFA »*,* explique-t-il. Ayant visiblement constaté que le poisson est entrain de mordre l’hameçon, son bourreau va passer à la vitesse supérieure. Et lui demande de faire le transfert d’un montant de 10 500 FCFA dans son propre compte « Orange Money » et de revenir vers eux pour la suite qui se passe de tout commentaire. « Je suis allé faire le transfert dans mon compte et quand j’ai rappelé, il m’a demandé de suivre les instructions qu’il aller me donner au fur et à mesure. Quand je l’ai fait le transfert que je venais d’effectuer dans mon compte a tout disparu »*,* ajoute-t-il. A partir de cet instant, il commence à soupçonner qu’il serait la cible des arnaqueurs, mais ne désespère pas. Par la suite, son interlocuteur virtuel lui fait parvenir un autre message lui demandant ses coordonnées (nom et prénom complets ; ville de résidence ; numéro de cni…). Toutes ses coordonnes lui sont retournées en lui demandant de faire un autre transfert, cette fois-là, d’une somme de 20 000 FCFA afin que lui soit envoyé le code pour aller toucher les 400 000 FCFA dans une micro-finance spécialisée dans le transfert d’argent. Le doute va dès lors s’enfler et Lambert s’arrêtera là, convaincu d’avoir été arnaqué.
2. Lyne K. a failli aussi tomber dans les mailles de ces mêmes hors-la-loi. « Cher(e) client, durant l’année 2015, votre numéro a été tiré au sort ; vous êtes gagnant d’un lot d’une valeur de 350 000 FCFA à retirer dans toutes les agences Express Union du territoire camerounais. Activez rapidement vos (compte, n° de bordereaux, mot de passe) et appeler le service promotionnel Mtn n° standard : 680 450 774. Mtn vous remercie de votre fidélité », tel est le message qui est arrivé dans son téléphone il y a quelques jours. En le lisant à plusieurs reprises la jeune étudiante est aux anges. Elle croit être à côté d’une manne qui tombe du ciel. Entrée en contact avec le supposé standard, elle est invité à faire un transfert Mtn mobile money d’une valeur de 100 FCFA à au moins deux personnes et de rappeler pour la suite*.* Lorsqu’elle raconte l’histoire à l’un de ses ainés, ce dernier lui demande d’arrêter toutes démarches, parce qu’il s’agit des bandits. D’abord, Lyne ne croit pas et ne sera convaincu qu’après un coup fil passé au service client de Mtn.
3. Un site internet présentant faussement les signes distinctifs de MTN Mobil Money propose au abonnées de fournir leurs informations confidentielle (numéro mobile et mot de passe) afin de bénéficier d’un bonus mensuel en appel et data allant de 300% jusqu’à 400% mais MTN décline toutes responsabilité quant à l’utilisation de ce site internet.
4. Alvine reçoit un email Fabrice André directeur du service client disant qu’elle a été débitée deux fois de sa facture du mois de Mai et que si elle ne donne pas ces coordonnées à travers le formulaire dans le lien ci-dessous elle ne sera pas rembourse du double prélèvement de la facture. Si a jamais alvine ouvre le lien et renseigne le formulaire elle envoi ces coordonnées aux arnaqueurs ainsi ils auront la libre voie de faire tout ce qu’ils veulent autrement dit vider votre argent dans le compte.
5. Un attaquant se rend devant un point de vente Orange Money et demande à faire un dépôt ; le gérant demande les informations nécessaires (montant et numéro de téléphone) ensuite il dit au gérant donné je vérifie le numéro vous allez faire comme ça et envoyé à une autre personne ; dès l’instant o il prend le téléphone il modifie le montant et le remet au gérant; et lui confiant que rien n’a modifier valide le montant et c’est ainsi qu’il s’en rend compte parfois trop tard qu’il a été arnaqué.
6. En utilisant MSVF pour créer un payload
7. **L’attaquant intercepte un client et entame des discutions dans le but de lui livrer son code secret ainsi que ses éventuels bien matériels**.
8. Les arnaqueurs font croire à leurs victimes qu’un de leurs proches est décédé. Le but inavoué est d’obtenir le numéro du compte ou de la carte et une signature sous prétexte que les personnes vont recevoir un héritage et qu’il faut dans un premier temps payer des frais de dossiers .cella permet par la suite aux escrocs d’effectuer des virements grâce aux informations collectées.
9. Les arnaqueurs envoient des emails excitant à cliquer sur un bouton pour participer à une loterie et désigner un heureux vainqueur. Mais pour récupérer son « lot » il faudrait envoyer de l’argent pour les frais de port. Et si c’est de l’argent que l’on a gagné alors ce sont les coordonnées bancaires ou d’un compte qu’il faudra transmettre afin qu’ils puissent effectuer un virement.
10. L’attaquant à plagier sur face book la page de JUMIA et propose des services aux clients. Il leurs demande d’effectuer des dépôts pour un tiers ou des transferts P2P sur un compte ORANGE MONEY qu’il a indiqué. Apres la transaction le client se rend compte que le site n’existe plus et que ce n’était qu’un arnaqueur.
11. Le retrait frauduleux effectuer par le point de vente sur le compte du client et arnaque client par le point de vents via le retrait à distance : le point de vente lance des retraits sur des comptes clients (cash out) en vue d’arnaquer le client. Lorsque celui-ci par mégarde valide l’opération, son compte Orange Money est débité automatiquement.
12. Les arnaqueurs appellent leur victime en lui disant que son compte Orange Mobile n’est pas à jour. Ils proposent de l’aider à y remédier à distance, lui assurant que cette solution est l’une des mesures prises par Orange pour limiter les contacts dans le contexte de la crise sanitaire actuelle.

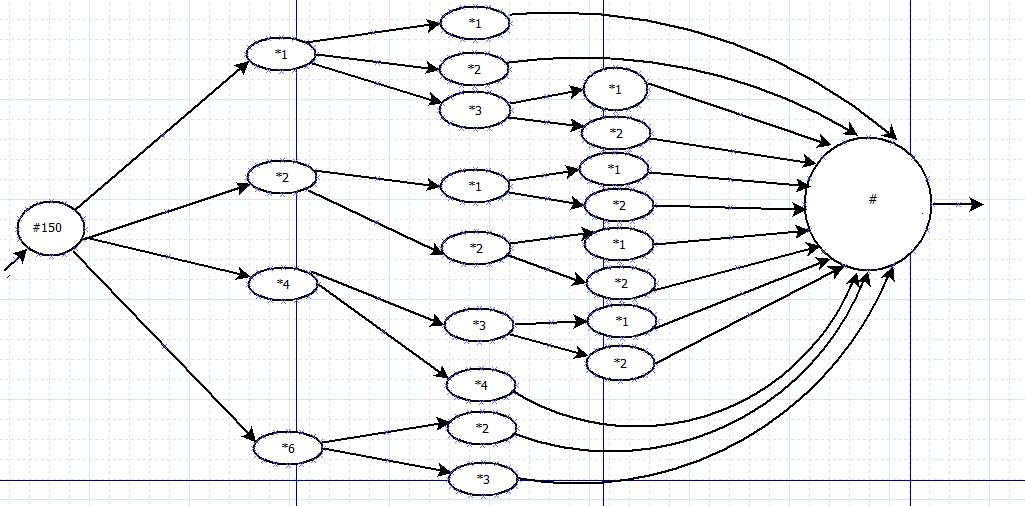
Une fois que la victime a donné son assentiment, elle est invitée à taper un code pour que son compte soit à jour. Attention, c’est là qu’intervient l’arnaque ! Une fois que le code saisi, les arnaqueurs auront accès à votre compte et pourront ainsi soutirer l’argent qui s’y trouve. Alors, vigilance !

1. Vous recevez un appel d’une certaine connaissance qui prend contact avec vous et disant être un ami(e) de longue date. Cette personne vous faite régulièrement signe dès lors et après un certain moment des quelles gagne votre confiance elle vous dit être en difficulté et a besoins d’une certaine somme, vous ayant confiance en cette personne vous faite le dépôt, après un certain temps vous essayer d’appeler ou de contacter cette personne mais le numéro n’est plus disponible.
2. Apres avoir fait une demande d’allocation familiale, vous recevez un appel vous disant que votre dossier est bloqué a un certain niveau de l’évolution du dossier il vous est demander une certaine somme pour que le dossier avance bien, vous étant pressez d’acquérir vos allocation êtes abuser et faites le dépôt au numéro donner par l’operateur cet ainsi que vous vous faite avoir par ces arnaqueurs.
3. Bonjour Mme/Mr/Mlle X je suis le frère ou la sœur de Mr/Mme Y ma mère est très malade et je n’ai plus d’argent est ce que vous pouvez me faire un dépôt d’argent pour résoudre cette urgence comme la fin de ce mois dès que j’aurai mon salaire je vous rembourserai.
4. Vous allez faire un dépôt a un point de vente spécialisé, l’agent vous dit qu’il a bien effectué le dépôt à Mr X et vous montre un faux message que le dépôt a été effectuer. Vous ayant confiance vous vous en allez après un certain temps celui qui était censé réceptionner le dépôt vous appel et vous dit qu’il n’a pas reçus vous retournez chez l’agent et il a disparu.
5. Lorsque vous faite un dépôt a une personne chez un agent après votre départ l’agent appel celui ou celle à qui il a envoyé l’argent qu’il a fait une erreur qu’au par exemple de 20000 il a envoyé 25000 et demande de renvoyer le surplus cet ainsi qu’on se fait avoir.
6. L’attaquant se rend au niveau d’un point de vente et échange le téléphone du distributeur contre un autre similaire. Connaissant le code secret du distributeur, ils effectuent des transferts frauduleux vers des comptes Orange Money personnels.
7. Le distributeur utilise son propre compte monnaie électronique en lieu et place et place de son compte. Le distributeur pour réceptionner les UVE (unités des valeurs électroniques) lors des opérations de retrait (Cash Out).
8. Le gérant du point de vente est contacté par une personne prétendant être un agent de l’émetteur ; il l’informe d’un approvisionnement en cours serait bloqué à cause d’un incident techniques et il signale la présence du responsable dans leurs locaux pour trouver une solution, plusieurs argumentaires sont proposées par le prétendu agent afin de gagner la confiance du point de vente pour régler le problème évoquer cette syntaxe autorise un dépôt sur un compte final.
9. L’attaquant ne dispose pas d’UVE sur son compte de monnaie électronique, il se rend dans un point de vente muni de sa pièce d’identité pour un retrait ; le gérant du point de vente initie l’opération de retrait et demande de valider; en lieu et place de la validation par le #150# le client envoi une fausse notification message au distributeur du point de vente via une application installe dans son téléphone. le gérant après notification décaisse l’argent au profit du client sans toutes fois vérifier son solde orange money. à la fin de la journée le gérant constate un écart dans son compatibilité correspondant au montant de la fraude.
10. un hacker installe un logiciel espion sur votre téléphone pour intercepter vos données de connexion bancaire. Ensuite, une fois les informations utiles obtenues, il réussira à fabriquer une fausse carte d'identité et, en la présentant, obtiendra une copie de votre carte SIM auprès de votre opérateur.Il ne lui restera donc plus qu'à se connecter au réseau du téléphone pour effectuer un ordre de virement et recevoir un SMS contenant un code de validation. Une carte nouvellement enregistrée (copie) provoquera des problèmes avec votre connexion réseau, et donc toute éventuelle perte de réseau ou déconnexion devra être le premier signe que quelque chose d'anomale est en train de se passer.
11. Les escrocs envoient de façon active de fausses notifications, et se font passer pour les célèbres réseaux sociaux. Il s’agit souvent de nouveaux amis, de leurs activités, de leurs commentaires, de leurs « j’aime », et de bien d’autres choses. Il est généralement impossible de les distinguer des vrais messages. La seule différence est qu’ils contiennent un lien d’hameçonnage, et qu’il est parfois difficile de s’en rendre compte. Lorsque les utilisateurs suivent le lien, on leur demande alors de saisir leur identifiant et leur mot de passe sur une fausse page de connexion.
12. Vous recevez un email vous invitant à mettre à jour vos informations chez un de vos fournisseurs (EDF, Opérateurs téléphoniques, Banque, etc.) voire même des services des impôts. Vous vous retrouvez sur une page quasi similaire à celle de votre fournisseur ou service des impôts dans lequel vous êtes invité à remplir vos coordonnées et vos informations bancaires. Toutes ces informations sont récupérées en règle générale à l’étranger par un pirate informatique qui les utilise immédiatement pour réaliser des achats voire des [virements bancaires](http://www.choisir-ma-banque.com/fr/frais-de-virements-bancaires-nationaux).
13. l’escroc se porte rapidement acquéreur d’un objet en vente. Il propose l’envoi de la somme via paypal. Le vendeur reçoit une confirmation du transfert par email. Cet email peut être à la fois un vrai courrier provenant de paypal ou un faux courrier provenant de l’escroc. Rassuré, le vendeur envoie alors l’objet à une adresse souvent un point relais ou à l’étranger. Après l’envoi, le vendeur se rend compte que son compte paypal n’est pas réellement crédité. Ou bien il reçoit un vrai courrier de Paypal quelques jours plus tard lui indiquant que le transfert est bloqué car basé sur ’un moyen de paiement douteux. Entretemps, le fraudeur disposera de votre bien qu’il pourra revendre ou utiliser à loisir.
14. Un client effectue un paiement PayPal supérieur au prix d'achat de la commande, puis il vous demande de lui verser la différence. Il peut vous dire qu'il vous a accidentellement payé en trop, que l'argent en surplus est destiné aux frais d'expédition, qu'il vous donne une prime pour votre service de qualité ou que l'argent sert à compenser le stress qu'il vous a causé. Il peut même vous demander de verser les frais d'expédition à son service d'expédition. Cet escroc a probablement payé avec une carte de crédit volée, ou un numéro de compte bancaire ou de compte chèque volé. Il ne vous suffit pas de simplement recevoir un paiement sur votre compte pour que cet argent vous appartienne. Si le titulaire légitime du compte signale une activité non autorisée, l'argent peut être retiré de votre compte. Dans ce cas, vous perdrez l'argent que vous avez envoyé au fraudeur, le produit que vous avez expédié, les frais d'expédition et votre paiement.
15. Les messages vous demandant de payer des frais de traitement modiques pour obtenir des prix fabuleux sont généralement une arnaque. Vous payez les frais de traitement et ne recevez rien en retour.
16. Les fraudeurs profitent des catastrophes pour inciter les gens généreux à faire des dons à des organismes de bienfaisance frauduleux. Cela se produit généralement en cas de crise de réfugiés, d'attaque terroriste ou de catastrophe naturelle (comme un tremblement de terre, une inondation ou une famine).
17. L'acheteur vous demande d'utiliser son compte d'expédition, parce qu'il bénéficie de rabais, ou qu'il traite avec ce fournisseur depuis des années, ou bien que ce service d'expédition est moins cher ou plus fiable. Dans d'autres situations, l'acheteur peut aussi vous demander de payer les frais d'expédition à son expéditeur préféré. Si vous utilisez le compte d'expédition de l'acheteur, celui-ci peut facilement communiquer avec l'entreprise d'expédition et réacheminer la commande vers une autre adresse. L'acheteur peut alors déposer une réclamation demandant un remboursement, car il n'a pas reçu sa commande. Vous n'êtes pas en mesure de prouver que l'acheteur a reçu sa commande et vous avez perdu votre produit, les frais d'expédition et votre argent. S'il vous demande d'envoyer l'argent à une fausse entreprise d'expédition, il peut voler votre argent. Une fois que vous avez envoyé l'argent, vous découvrez que la commande a été effectuée avec une carte ou un compte bancaire volé. Vous pouvez être tenu de renvoyer les fonds au client légitime dont le compte a été volé.
18. Vous recevez une commande d'un client qui vous demande d'utiliser son étiquette prépayée pour couvrir les frais d'expédition. (Il vous dit peut-être qu'il peut se procurer ses étiquettes à un prix réduit.) En fournissant l'étiquette, le client contrôle la destination du colis. Il peut l'envoyer dans un autre pays, à une boîte postale ou dans un autre lieu introuvable. Pour être protégé par le [Règlement sur la Protection des Marchands](https://www.paypal.com/us/webapps/mpp/security/seller-protection), vous devez effectuer l'expédition à l'adresse figurant sur la page Détails de la transaction. L'étiquette d'envoi peut également avoir été achetée avec une carte de crédit volée.
19. Un acheteur passe une commande et fournit une adresse d'expédition incorrecte ou fausse. L'entreprise d'expédition tente de livrer le colis, mais n'est pas en mesure de le faire. L'acheteur surveille les informations de suivi en ligne et voit que l'expéditeur n'a pas pu livrer le colis. L'acheteur communique avec votre entreprise d'expédition et demande que le colis soit envoyé à sa bonne adresse. L'entreprise d'expédition livre le colis à la nouvelle adresse. L'acheteur dépose ensuite une réclamation pour se plaindre de ne pas avoir reçu l'objet. Étant donné que le colis a été réacheminé, vous ne pouvez pas prouver que l'objet a été livré à l'adresse indiquée sur la page Détails de la transaction. L'acheteur conserve l'objet et l'argent. Étant donné que le colis n'a pas été livré à l'adresse indiquée sur la page Détails de la transaction, vous n'êtes pas couvert par la Protection des Marchands. Malheureusement, vous avez perdu le produit, les frais d'expédition et l'argent. En plus, vous devrez peut-être aussi payer à votre expéditeur des frais supplémentaires pour le réacheminement.
20. L’attaquant se rend dans un point de vente et dis qu’il aimerait effectuer un dépôt, il remet le montant au responsable du quiosque ou de la boutique après avoir vérifié si ce sont les faux billets ensuite demande si c’est avec les frais de retrait, ce dernier accepte sachant qu’il doit reprendre son argent pour aller compléter étant dehors il insère les faux billet et entre à ce moment le responsable ne vérifie plus la véracité des billets et c’est ainsi que l’attaquant réussit à merveille son coup.
21. Vous recevez un appel d’un certains monsieur X responsable de l’équipe de développement qui vous fait croire qu’il y a un nouveau service MTN en cours permettant de faire un prêt pour ton compte (ces arnaqueurs ont tous les informations nécessaires sur vous, parfois ce sont des proches qui connaissent tout vous concernant) tout en sachant que vous êtes dans le besoin alors il demande de taper une suite de code et si vous le faite vous videz votre compte sans le savoir.
22. On n’appelle et dis que le réseau est perturbé ,tous les comptes serons bloqués qui n’aura ni retrait, ni dépôt, ni transfert bref que tous les options ne serons plus disponible et même après la résolution de ce problèmes les comptes seront vide mais qu’il peut vous accorder une faveur en vous octroyant un code temporaire vous permettant de faire votre retrait ; avec le code de paiement vous allez vous rendre dans un point de vente et remettre ce code au gérant une fois cella fait votre compte est vidé.
23. Il vous appel et se présente comme un responsable employé dans une entreprise qui fait dans les tombolas gagnant et vous demande de vérifier si vous faite partie de la liste des gagnants, il vous demande de faire une série de manipulation sur les touches du téléphone (chaque touche émet un son diffèrent) juste pour vérifier que son logiciel détecte les touches une fois rassure il vous demande de taper votre code secret. L’attaquant détient déjà votre numéro de téléphone et votre code alors il peut également faire ce qu’il veut de votre compte.
24. On vous appelle et dit qu’un membre de votre famille résident a l’étranger vous a envoyer un colis (avec tous les informations sur cette personne) et vous demande de faire un transfert d’argent pour le carburant ; une fois le transfert fait le numéro de l’arnaqueur ne fonctionne plus et vous ne recevez jamais le colis.
25. L’attaquant utilise une puce spéciale , prend le numéro de la victime et fait croire a l’ordinateur de orange money que la victime souhait faire un retrait , le serveur dit d’accord pour le retrait mais avant je veux son code secret ;comme l’attaquant ne connait pas le code secret il envoie un faux message a la victime pour faire croire qu’il vient de recevoir un dépôt ;quelque instant après il appel pour dire qu’il a fait une erreur et supplie la victime de lui renvoyer un partie ; à ce moment la victime interroge son solde avec son code secret entre temps le serveur reçoit 2 requêtes( retrait et vérification) et comme le retrait est plus prioritaire le serveur considère le code plutôt pour le retrait et c’est ainsi que la victime se retrouve avec un compte vide.
26. Vous recevez un message : « ORANGE MONEY »

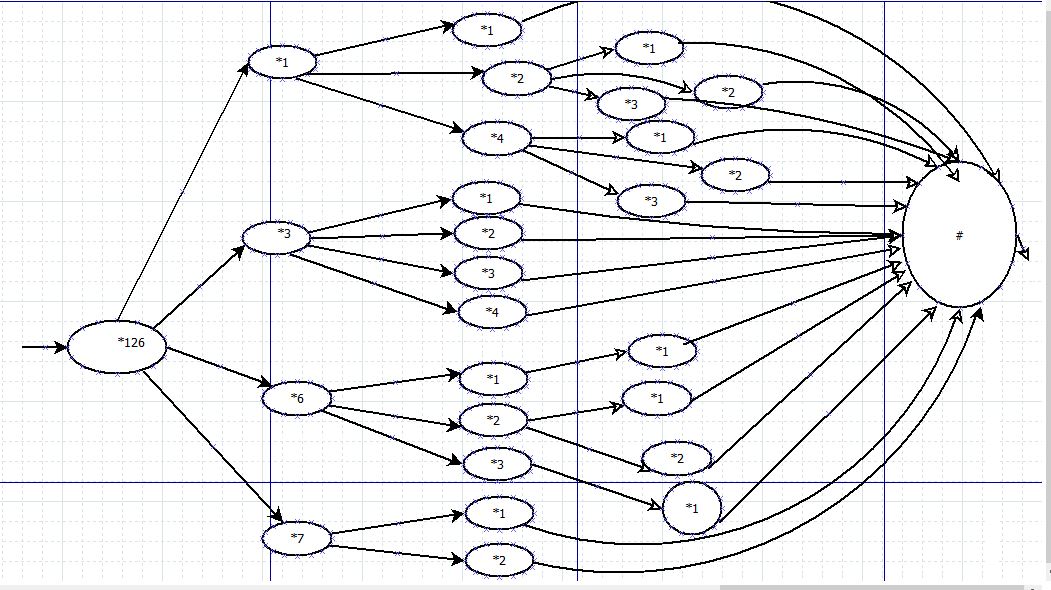
Cher(e) client(e), vu vos consommations durant les années antérieure, votre numéro a été tiré au sort dimanche sur canal2 internationale et vous bénéficiez d’un prime bonus d’une valeur de 280000 F à retirer dans toutes les agences !!! Pour plus d’informations contacter le directeur de vos prime bonus Mr Aboma jean jacke au 657424918.» si vous faite l’erreur d’appeler on vous donne les instructions vous permettant de vider votre compte tout en vous faisant croire que c’est pour bénéficier ces lots.

1. On n’appel et dit que vous venez de gagner des lots et vous demande qu’il faut au préalable répondre à quelques questions (quel est votre dernier transaction ?dépôt ou retrait ? les montants ? etc. ensuite il demande de taper une combinaison de code (#150\*11 numéro\*logo orange\*code secret\*1#) pour activer vos lots .une fois taper ce code vous vider votre compte automatiquement.
2. **Représentation sous forme d’automate générale**

### **Pour ORANGE MONEY**



### **Pour MTN MOBILE MONEY**



## **Implémentation d’un système intelligent :**

Il s’agit d’utiliser la programmation logique ayant pour but de définir les règles logique attendues d’une solution et de laisser le compilateur la transformer en séquence d’instruction permettant aux utilisateurs de savoir si une suite de code tapé est pour l’arnaquer ou non.

# Conclusion

**P**arvenu au terme de notre analyse, force est de constater que au fur et à mesure que le temps passe les escrocs multiplient les stratégies et les méthodes pour arnaquer les populations utilisant les applications de paiement mobile dans le but de nuire en jouant sur leur psychologie. Ces individus qui pensent que la vie est rose, facile et qu’on gagner de l’argent a Tor et à travers oubliant qu’il ne faut pas aimer la vie facile car il faut cultives la souffrance dans la persévérance pour la compétence ou le mérite et également qu’il faut toujours vérifier les informations qu’on reçoit avant de réagir éviter les fecs news et la panique. Cependant pouvons-nous espéré mettre définitivement fin à cette forme d’arnaques dans le monde ???

# References

* https://arxiv.org/pdf/1807.11840.
* <https://www.google.com/url?sa=t&source=web&rct=j&url>=
* https://www.orange.cm/particuliers/1/27/arnaques111943.html&ved=2ahUKEwjlJmFl8PpAhXcFjQIHX3wCpMQFjAGegQIBRAB&usg=AOvVaw2wysKHt3DTv1ntOBNc9241&cshid=1590003589185
* <https://www.google.com/amp/s/actucameroun.com/2019/11/15/cameroun-des-photocopieurs-a-yaounde-utilises-pourvider-les-comptes-mobile-money/amp/>
* https://www.stopblablacam.com/culture-et-societe/0312-2298-attention-des-arnaqueurs-deguisent-de-simples-smssous-forme-de-notifications-de-transfert-dargent-parmobile-money
* https://www.stopblablacam.com/e-arnaques/0805-4011-attention-des-individus-malveillants-continuent-darnaquer-sur-orange-money
* <https://www.google.com/url?sa=t&source=web&rct=j&url=https://pepesoupe.com/consommateur/techniques-darnaquesur-orange-money/&ved=2ahUKEwjlJmFl8PpAhXc> FjQIHX3wCpMQFjARegQIBhAB&usg=AOvVaw0rd\_KzN2sEMG3WnUbwRm4g&cshid=1590003589185
* <https://droitmediafinance.com>