shineyoureye

Sabi

The First Truly Pan-African Toolkit for Seniors

French

Also available in English, Pidgin, Yoruba, Igbo, Hausa, Swahili and Zulu

Powered by cybersafe. FOUNDATION

PROTECCIÓN DE REDES SOCIALES

Qu'est-ce que l'authentification à 2 facteurs, aussi appelée 2FA?

"Est-ce vraiment vous?" est la question que l'authentification à deux facteurs pose quand vous voulez vous connecter à vos comptes en ligne. L'authentification à 2 facteurs offre une couche de sécurité supplémentaire et ne vous donne pas accès juste parce que le nom d'utilisateur et le mot de passe sont corrects, mais demande un autre code quand vous essayez de vous connecter. Ce code peut être envoyé à votre téléphone sous forme de SMS (texto), de courriel ou peut être généré par une application sur votre téléphone (une application d'authentification), dépendant de vos paramètres.

Comme les dispositifs antivols qui séparent vos objets de valeur des voleurs, 2FA se place entre vos comptes en ligne et les cybercriminels (fraudeurs).

Raisons d'adopter la 2FA

- C'est gratuit et facile à mettre en œuvre.
- Cela permet d'ajouter une couche de sécurité supplémentaire même si vos identifiants (nom d'utilisateur ou mot de passe) ont été volés.
- Cela vous protège contre une perte de données et une usurpation d'identité.
- Cela rend la tâche plus difficile aux fraudeurs de vous voler.

Les trois choses dont vous avez besoin pour implémenter la 2FA

Avez-vous déjà entendu parler d'une application d'authentification?

C'est une application qui permet de compléter le processus d'authentification à deux facteurs en générant des mots de passe. L'application n'est pas reliée à votre numéro de téléphone, donc c'est une des méthodes les meilleures et les plus recommandées pour activer la 2FA. Un exemple d'application d'authentification est le Google Authenticator (disponible sur le Play Store et l'App Store d'iOS).

Laissez-moi vous aider à activer l'authentification à deux facteurs sur WhatsApp et Facebook.

P.S. Vous pouvez activer l'authentification à deux facteurs sur tous vos comptes sur les réseaux sociaux et les applications bancaires mobiles.

Vous pouvez activer la 2FA partout

Les Etapes pour Allumer 2FA sur WhatsApp

- Ouvrez l'application WhatsApp sur votre téléphone
- Appuyez sur les trois points dans le coin supérieur droit
- Appuyez sur Réglages
- Appuyez sur Compte
- Appuyez sur Vérification en deux étapes
- Appuyez sur Activer
- Saisissez un code PIN personnalisé
- Confirmez votre PIN
- Saisissez votre adresse électronique
- Appuyez sur Suivant
- Confirmez votre adresse électronique
- Appuyez sur Sauvegarder
- Appuyez sur Terminé

Les Etapes pour Allumer 2FA sur Facebook

- Connectez-vous à votre compte Facebook
- Allez à Paramètres et Confidentialité
- Cliquez sur Paramètres
- Faites défiler vers le bas et cliquez sur Sécurité et Connexion
- Cliquez sur Authentification à 2 facteurs
- Choisissez message SMS et cliquez sur Continuer
- Saisissez votre numéro de téléphone et cliquez sur Confirmer
- Saisissez votre mot de passe et confirmez que c'est bien vous
- Saisissez le code qui vous a été envoyé
- Vous verrez alors un écran de confirmation

Que faire quand vous perdez votre telephone

La perte d'un téléphone portable peut être très inconfortable, mais ce qui serait encore plus grave, c'est que cette disparition entraîne la perte de votre argent durement gagné. Vous vous demandez comment c'est possible? Par les services bancaires mobiles.
Presque tout le monde utilise les services bancaires mobiles, en employant soit un USSD (code abrégé) ou une application mobile pour effectuer des transactions bancaires sur son téléphone portable.

L'USSD, aussi connu sous le nom de code abrégé, est une méthode utilisée par les clients pour communiquer avec leurs fournisseurs de services téléphoniques ou les services financiers mobiles. Quand vous composez un numéro qui commence par * et se termine par #, vous utilisez l'USSD.

Il y a deux actions à prendre pour éviter la perte de votre argent quand votre téléphone a été volé:
1.Verrouiller votre carte SIM (cela doit être fait avant que le téléphone ne soit volé)

2.Bloquer votre compte bancaire; cela doit être fait immédiatement après le constat de la disparition de votre téléphone.

Comment verrouiller votre carte SIM

Appareille iOS

- Allez dans Réglages sur votre appareil iOS
- Appuyez sur Données Cellulaires
- Localisez PIN de la carte SIM et appuyez dessus
- Activez le code PIN de la carte SIM
- Entrez le code PIN de la carte; si la carte n'était pas verrouillée, utilisez le PIN de base documenté ci-dessous
- Appuyez sur Changer le PIN
- Entrez de nouveau le PIN courant
- Entrez un nouveau PIN pour verrouiller votre carte SIM
- Appuyez sur Terminer
- Assurez-vous de vous rappeler votre nouveau code PIN

Appareille Android

- Allez dans Paramètres, puis Sécurité
- Si vous utilisez un téléphone à deux cartes SIM, sélectionnez celle que vous voulez verrouiller
- Appuyez sur Verrouillage de la carte SIM
- Activez le verrouillage de la carte SIM
- Appuyez sur Modifier code PIN carte SIM
- Entrez le code PIN de la carte; si la carte n'était pas verrouillée, utilisez le PIN de base documenté ci-dessous, et pressez OK
- Entrez un nouveau PIN pour verrouiller votre carte SIM
- Confirmez le nouveau PIN à quatre chiffres
- Appuyez sur OK et Sortie

Le PIN de base pour
MTN = 00000, Airtel = 1234, Glo = 0000 and
9mobile = 0000

Les abréviations que vous devez connaître

CVV
Le nombre à trois chiffres écrit sur votre carte de débit ou de crédit

OTP (Mot de passe à usage unique)
Un code généré automatiquement, envoyé par un fournisseur de services, qui est utilisé une seule fois pour un processus d'authentification. C'est généralement un code à 6 chiffres, souvent transmis par SMS.

BVN (Numéro de vérification bancaire)
Un nombre à 11 chiffres, unique pour chaque personne, utilisé pour vérifier l'identité d'un client à travers toutes les institutions financières.

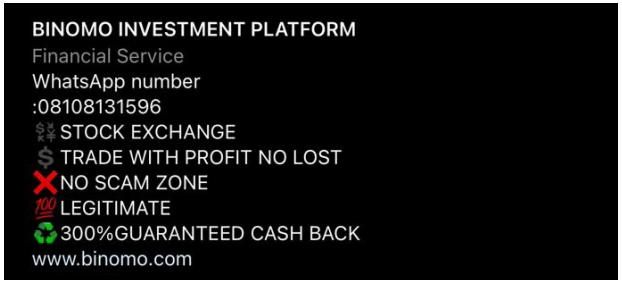
ESCROQUERIES À L'INVESTISSEMENT

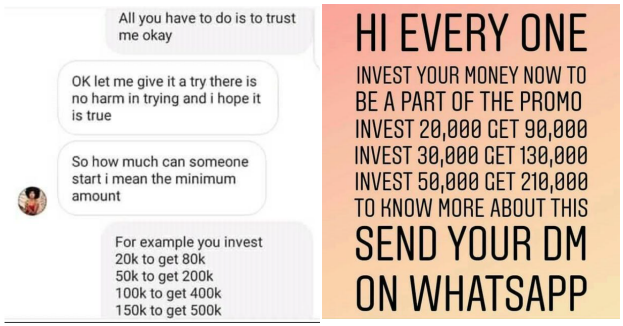
Les fraudeurs se cachent souvent derrière de faux plans d'investissement pour tromper les individus sans méfiance et prendre leur argent. Tant que cette tendance continue à croître, nous devons trouver un moyen de nous protéger tout en cherchant des moyens d'accroître nos revenus

Signaux de danger de fraude à l'investissement

- On promet un profit important et peu de risques.
- L'investissement se fait à très court terme (investissez 50.000 et recevez 300.000 dans 2 semaines).
- Le message principal est "tout le monde le fait et cela paie".
- On met la pression pour investir immédiatement.
- Ils ne possèdent pas de licence pour vendre des investissements.

Exemples d'investissement frauduleux





Comment vous protéger contre les fraudes à l'investissement

- Vérifiez l'identité des vendeurs. Ne soyez pas trompés par un titre ronflant ou d'autres apparences de succès, assurez-vous qu'ils sont bien autorisés à vendre des investissements.
- Ne poursuivez pas les schémas "devenez riche rapidement". Soyez méfiant envers les propositions d'investissement qui garantissent un bénéfice fixe ou promettent des profits spectaculaires.
- Méfiez-vous des arguments de vente qui se concentrent sur le nombre de personnes qui investissent sans vous démontrer pourquoi l'investissement a du sens. Ne croyez pas les mensonges qui disent que "tout le monde" investit dans le schéma proposé.
- Méfiez-vous des opportunités d'investissement qui promettent un gros bénéfice avec peu ou pas de risque.
- Refusez de vous presser. Si le vendeur vous dit que l'offre n'a qu'une durée limitée, ou que les opportunités d'investir sont limitées, considérez cela comme un signal de danger. Un investissement légitime sera encore là demain.
- Si vous sentez qu'une offre d'achat d'actions pourrait être légitime, vérifiez toujours le cours de bourse de la société et les performances récentes de ses actions. Certaines offres d'achat d'actions pourraient être bien en-dessous du prix du marché.
- Ne donnez pas vos coordonnées à quelqu'un qui vous appelle sans que vous l'ayez demandé, et ne répondez pas à des courriels qui offrent des recommandations financières ou des opportunités d'investissement - raccrochez ou effacez le courriel.
- Ne prenez jamais d'engagement d'investissement lors d'une séance d'information - prenez toujours le temps d'analyser l'opportunité et demandez l'avis à une personne plus expérimentée en finances.
- Ne vous sentez jamais obligé d'investir parce que le vendeur vous donne un cadeau gratuit.
- Armez-vous de connaissance. Apprenez à détecter les signaux de danger de la fraude à l'investissement pour pouvoir vous protéger, vous et vos proches.