CHAABI PAY PRO

Règles de confidentialité

Collecte et utilisation des données client

Le client pour créer un compte Chaabi Pay Pro, et conformément aux exigences du régulateur, devra avoir un profil* de commerçant

L'accès à Chaabi Pay Pro, de façon sécurisée, nécessite

- De renseigner un ensemble de données client.
- De renseigner un numéro GSM valide et opérationnel sur lequel il recevra l'OTP de validation des opérations
- De choisir un mot de passe personnel et confidentiel qu'il ne devra divulguer

Les données collectées sont cryptées suivant des normes internationales
Aucune donnée obtenue par notre application n'est partagée ou transmise à des entités externes

L'accès à Chaabi Pay Pro donne au client la possibilité de consommer les services destinés aux commerçants

* 5 profils :
Personne Physique
Personne Physique Auto-entrepreneur
Personne Morale
Personne Morale: Coopérative
Personne Morale : Association

Sécurité et traitement des données à caractère personnel

En application des dispositions de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, le Client donne consentement à MarocTraitement de Transactions à l'effet de traiter ses données personnelles collectées.
Le Client consent en outre, que ses données à caractère personnel soient communiquées à la Banque Centrale Populaire, pour l'exécution de certaines opérations bancaires, aux autorités compétentes ou de tutelle habilitée, aux centrales d'information, aux compagnies et courtiers d'assurances dûment habilités, aux ayants droit, tuteurs et mandataires habilités.

Les risques

Faut-il avoir peur d'internet ?
Non bien sûr ! Les risques sont à appréhender comme ceux de la vie courante.Mais mieux les connaître, c'est mieux s'en protéger !

Apprenez à les identifier

Le phishing

Le phishing (ou hameçonnage et parfois filoutage), est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale (sécurité de l'information). Le phishing peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.

Les mules

Une « mule » est le nom donné à une personne utilisée pour transporter des matériaux illicites : explosifs, armes, drogues, parfois à son insu. Sur Internet, les mules sont "recrutées" par e-mail pour "transporter de l'argent" contre rémunération. Pour la recruter, le pirate abuse un internaute qui se rend ainsi complice d'une fraude (vol, détournement ou blanchiment d'argent) passible de poursuites.

Le pharming

Le pharming (ou dévoiement en français) est une technique de piratage informatique exploitant des vulnérabilités DNS. Cette technique consiste à détourner l'accès à un site Internet vers un site pirate. l'URL est correcte, mais l'internaute est sur un faux site. Les informations confidentielles saisies sont capturées par le pirate.

Le spam

Le spam, pourriel ou polluriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. Le phishing et les canulars utilisent en partie cette technique.

Les arnaques et canulars

A l'instar du spam, une arnaque est un e-mail que vous n'avez jamais demandé à recevoir et qui vous propose en général un gain d'argent facile et rapide (loterie, bourse, etc.) ou qui sollicite votre compassion. Dans certains cas, l'arnaque peut consister à faire de vous une mule. Mais attention,vous devenez complice du pirate, de ses malversations et vous risquez gros. Les canulars (appelés hoax en anglais) se trouvent souvent sous la forme de courriel ou de simple lettre-chaîne. Dans ce dernier cas, Internet ne fait qu'amplifier un phénomène qui existait déjà à travers le courrier traditionnel. À la différence des spams qui sont la plupart du temps envoyés de manière automatisée à une liste de destinataires, les canulars sont, eux, relayés manuellement par des personnes de bonne foi à qui on demande de renvoyer le message à toutes ses connaissances, ou à une adresse de courrier électronique bien précise.

Les virus

Un virus informatique est un logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc.

Les spywares

Un spyware est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

Les chevaux de Troie

Un cheval de Troie est un logiciel d'apparence légitime conçu pour exécuter subrepticement (de façon cachée) des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur. Windows Live Messenger, le téléchargement de programmes gratuits et le partage des programmes ou autres fichiers sont les principales sources de diffusion des chevaux de Troie. Ils sont également très fréquents dans certains types de courriels.

Les informations transmises

Lorsqu'on utilise les services d'un site Internet, des informations souvent personnelles sont transmises (e-mail, nom, prénom, identifiant, mot de passe, N° de carte bancaire, etc.). Pour être certain de communiquer en toute sécurité avec son site bancaire ou d'achat en ligne, quelques précautions et vérifications s'imposent. Consultez notre rubrique « Bonnes pratiques ».