Umnia Bank أُمنية بنك

ليطمئن قلبي

LA SÉCURISÉE

Umnia Bank, Société anonyme à Directoire et à Conseil de Surveillance, au capital de 1 100 000 000 dirhams, dont le siège est sis au 397, route El Jamiâa (ex route d'El Jadida), Casablanca, Maroc, autorisée par Bank Al-Maghrib sous agrément N° 58 en tant que banque participative, immatriculée au Registre de Commerce de la ville de Casablanca sous le N° 347111, CNSS N° 18756770, Patente N° 37991108, ICE N° 001529642000035, Tel N° 0522646264. www.umniabank.ma

LES BONNES PRATIQUES POUR UNE NAVIGATION SÉCURISÉE SUR INTERNET :

Voici l´essentiel des réflexes sécurité que vous devez suivre tout au long de la navigation sur internet :

- Ne téléchargez surtout pas d´application ou de logiciel et ne vous connectez pas à un site Internet suite à une sollicitation ou autre,
- Méfiez-vous des messages (mail, SMS, chat, lien ...) ou appels téléphoniques d´origine inconnue ou inattendus, Umnia Bank ne vous demandera jamais de lui fournir votre mot de passe ou un code reçu par SMS,
- Ne téléchargez des applications que depuis les sites ou «stores», magasins officiels des éditeurs d´applications, ne faites jamais confiance à des applications envoyées en dehors des stores
- Tapez vous-même l´adresse du site,
- Vérifiez la fiabilité (https ou cadenas devant l´adresse) et la réputation des sites visités,
- Prenez le temps de faire les vérifications nécessaires, surtout si le message est alarmiste et demande une action urgente (paiement, envoi d´informations personnelles, etc.),
- Ou encore faites attention aux demandes de dons frauduleuses envoyés par des personnes que ne vous connaissez pas...

Il est aussi très important de vérifier la sécurité de vos appareils et de votre connexion Internet :

- Téléchargez la mise à jour de votre système d´exploitation,
- Installez sur votre ordinateur comme sur votre mobile un antivirus et un pare-feu efficaces avec des mises à jour automatiques,
- Vérifiez que le site Internet est sécurisé (https devant l´adresse du site, ou cadenas fermé, ou icône d´une clé dans le navigateur).

QUE FAIRE SI VOUS AVEZ FOURNI VOS COORDONNÉES BANCAIRES ?

Si vous pensez que vous avez communiqué les données de votre carte bancaire sur un site frauduleux, que devez-vous faire ?

- Si vous avez fourni vos informations personnelles et numéros de carte bancaire, contactez immédiatement votre **conseiller Umnia Bank en agence pour lui signaler et faire opposition sur votre carte.**
- Surveillez votre compte et en cas de débit frauduleux, contactez immédiatement votre **conseiller Umnia Bank en agence pour lui signaler et faire opposition sur votre carte.**

QUELLES SONT LES DIFFÉRENTES TECHNIQUES DE FRAUDE ET D'ARNAQUE UTILISÉES SUR INTERNET QUE VOUS DEVEZ ÉVITER ?

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.

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.