

PROTÉGEZ-VOUS DES TENTATIVES DE FRAUDE

**N'ouvrez pas un mail potentiellement frauduleux.
Parlez-en à votre banque.**



MESSAGE DE LA SECURITE INFORMATIQUE A L'ATTENTION DES CLIENTS DE LA SG BÉNIN

Cher(e) client(e),

Des individus malintentionnés pourraient vous contacter, en se faisant passer pour votre banque par mail, au téléphone, par sms ou par un moyen quelconque vous invitant à effectuer une action particulière (click sur une pièce jointe, click sur un lien, installation d'un logiciel, etc.).

Nous vous invitons à redoubler de vigilance si vous recevez un message (sous forme de courrier, mail, sms ou autre) semblant provenir de la SG Bénin.

Pour vous prémunir des tentatives de fraude, nous vous exhortons fortement à suivre les recommandations suivantes :

- Ne cliquez jamais sur un lien fourni dans un mail non désiré.-
- Accédez uniquement à votre site de banque à distance en saisissant manuellement son adresse dans votre navigateur :
 - Site institutionnel - <https://www.societegenerale.bj/fr/>
 - Site ebanking - <https://www.connect.societegenerale.bj/login>
- Avant de saisir vos identifiants et mots de passes, assurez-vous que l'adresse du site commence par "<https://>" et qu'aucun message d'erreur ne s'affiche sur la page.
- Si le mode d'authentification de votre site a subitement changé sans que vous en ayez été averti au préalable, ne saisissez aucune donnée et prenez contact avec le Centre de Relations Clients au numéro +229 21 31 82 91.
- Changez régulièrement le mot de passe d'accès à votre site bancaire.
- En cas de réception d'un mail, d'un message vocal et/ou d'un SMS inhabituel, veillez à informer la banque par les moyens habituels.
- En cas de moindre doute, veuillez contacter votre banque par les moyens habituels.