Malgré nos conseils, vous avez déjà communiqué des informations sensibles en pensant bien faire ?

Contactez votre conseiller dans les plus brefs délais. N'hésitez pas à faire opposition à vos instruments de paiement via l'application Banxo ou à modifier votre code personnel.

Renseignez-vous
auprès de votre conseiller ou sur :

www.caisse-epargne.fr/grand-est-europe/votre-banque/securite/bons-reflexes-adopter

Coût de connexion selon votre fournisseur d'accès Internet.

Téléchargez l'application mobile Caisse d'Epargne depuis le store de votre smartphone.

Banque | Banxo

CAISSE D'EPARGNE
Grand Est Europe
Vous être utile.

Document à caractère publicitaire et sans valeur contractuelle.

CEGEE, Banque coopérative régie par les articles L.512-85 et suivants du Code Monétaire et Financier, société anonyme à Directoire et Conseil d'Orientation et de Surveillance au capital de 681.876.700 € - siège social à STRASBOURG (67100), 1, avenue du Rhin – 775 618 622 RCS STRASBOURG - immatriculée à l'ORIAS sous le n° 07 004 738.
• Crédit photo : Adobestock. Impression : Vagner Graphic - 10/2022.

Savoir repérer une tentative de fraude, c'est savoir l'éviter.

Des astuces simples mais qui vous protègeront efficacement des fraudeurs.

CAISSE D'EPARGNE
Grand Est Europe
Vous être utile.

E-MAIL FRAUDULEUX ET HAMEÇONNAGE

Vous pouvez être amené à recevoir un e-mail malveillant, qui visuellement ressemble à nos communications, mais dont l'objectif est de vous inciter à vous rendre sur une page Internet pour vous faire saisir vos identifiants et codes secrets afin de vous les subtiliser.

Pour déjouer cette tentative de fraude, **vérifiez bien la qualité du message** (expéditeur, fautes d'orthographe, formulation incorrectes, ...), mais aussi le site de destination (url sécurisée par le protocole *https* et la présence du certificat de sécurité avec le cadenas). Notre site internet a pour unique adresse : **https://www.caisse-epargne.fr***.

Vous avez reçu un email suspect : **ne cliquez sur rien** et contactez votre conseiller pour faire la lumière sur ce message.

LE SPOOFING OU FRAUDE PAR TÉLÉPHONE

Des fraudeurs **se font passer pour des collaborateurs de votre Caisse d'Epargne** par téléphone et tentent, par exemple, de vous alarmer en vous signalant une tentative de paiement sur votre compte ou la détection d'une fraude en cours.

Le but de cette pratique : vous soutirer vos codes d'accès à votre espace sécurisé sur Internet, récupérer vos données de carte bancaire ou le code d'identification **Sécur'Pass** permettant de valider un achat sur internet ou un virement.

Certains vous demanderont de valider un paiement avec Sécur'Pass afin « d'annuler » l'opération frauduleuse : **raccrochez, vous êtes en présence d'un escroc** au bout du fil.

Il est important de retenir que jamais un conseiller Caisse d'Epargne ne vous demandera, ni à l'écrit, ni à l'oral, de lui communiquer vos informations personnelles.

*Coût de connexion selon votre fournisseur d'accès Internet.

LA FRAUDE PAR SMS

Les fraudeurs peuvent vous envoyer des sollicitations par SMS en se faisant passer pour la Caisse d'Epargne.

En cas de réception d'un SMS suspect, vous invitant à valider une opération, à vous connecter à vos comptes ou à communiquer des coordonnées (personnelles, bancaires, ...), **ne répondez pas** et ne cliquez pas sur un lien : **supprimez simplement le message**.

En cas de doute, votre conseiller peut vous accompagner pour démêler le vrai du faux.

POUR VOUS PROTÉGER, *3 RÈGLES D'OR*

- Ne communiquez jamais vos données personnelles, bancaires (identifiants BAD, RICE..) ou votre code **Sécur'Pass**.
- Par téléphone ou sur internet, ne validez que les opérations que vous avez **vous-même** initiées.
- En cas de doute, un seul interlocuteur : **votre conseiller** Caisse d'Epargne.