

Consignes de sécurité pour le particulier

Afin de vous aider à lutter efficacement contre toute tentative de fraude, votre banque vous recommande de respecter les principes suivants :

Principe n°1 : maintenir un environnement informatique sûr.

- Mettez à jour votre matériel informatique* pour éviter des difficultés de compatibilité.
- Equipez votre matériel informatique* d'anti-virus et de pare-feu (firewall), régulièrement mis à jour.



Ne téléchargez jamais de logiciel de prise en main de votre matériel informatique sous divers prétextes (tests ...).

Ne cliquez jamais sur un lien hypertexte ou fichier en pièce jointe dans un mail, même si votre banque y est mentionnée, il peut s'agir de phishing (e-mail frauduleux imitant une communication de la banque).

Principe n°2 : prendre en compte les consignes communiquées par votre banque.

- Déconnectez-vous systématiquement de votre espace personnel à la fin de votre navigation.
- Consultez régulièrement les informations sécuritaires sur le site de votre banque.
- Vérifiez régulièrement vos coordonnées personnelles (numéro de téléphone, adresse e-mail) et la liste des appareils inscrits pour Confirmation Mobile.
- Privilégiez pour vos achats en lignes des sites commerçants de confiance proposant une sécurisation des paiements.



Ne communiquez jamais vos données confidentielles permettant l'accès à votre espace personnel ou à la réalisation d'opérations.

N'effectuez jamais d'opérations de paiement (virements, achat par carte bancaire...) à la demande de personnes dont vous ne pouvez pas vérifier l'identité.



Pour tout complément d'information ou pour signaler une opération frauduleuse, contactez votre conseiller.

* ordinateur, smartphone, tablette ou tout autre appareil électronique ayant un accès à internet.