

NOUVEAUX DROITS BANCAIRES



REMBOURSÉ NE VEUT PAS DIRE PROTÉGÉ !

La Cour de justice de l'Union européenne (CJUE) a fait évoluer la règle (arrêt du 15 octobre 2026) :

En cas de fraude ou de phishing, la banque doit appliquer la loi et procéder au **remboursement immédiat du client**. C'est à l'établissement d'apporter la preuve d'une « négligence grave », et non plus à la victime de prouver son innocence.

Une avancée juridique importante... mais attention au **piège de la fausse sécurité** !

POURQUOI LE REMBOURSEMENT NE VOUS PROTÈGE PAS DE TOUT ?

Rembourser votre argent n'efface pas les conséquences d'une cyberattaque : en tombant dans le piège d'un faux site bancaire ou d'un SMS piégé, vous subissez des dégâts irréparables :

	USURPATION D'IDENTITÉ	Vos identifiants, mots de passe et données personnelles finissent sur le Dark Web et serviront à d'autres escroqueries.
	RE-CIBLAGE MASSIF	Un piratage réussi fait de vous une cible prioritaire pour des arnaques encore plus sophistiquées (faux conseillers, chantage).
	RECOURS ULTÉRIEURS DE LA BANQUE	Si l'établissement prouve que vous avez validé une transaction (code SMS, notification d'application) en ignorant les alertes, il pourra exiger le remboursement des sommes avancées.

3 RÉFLEXES SIMPLES POUR GARDER LE CONTRÔLE

- 1 Doutez de l'urgence** : Aucune banque ne vous demandera de valider une opération ou de donner un mot de passe sous pression.
- 2 Vérifiez l'URL** : Ne cliquez jamais sur un lien reçu par SMS ou email. Tapez vous-même l'adresse de votre banque.
- 3 Protégez vos accès** : Activez la double authentification et ne validez JAMAIS une notification si vous n'êtes pas à l'origine de l'action.

SAGESSE CYBER : le remboursement ne doit pas remplacer la vigilance !