Neuflize OBC
ABN AMRO



Neuflize OBC - ABN AMRO

Les bons réflexes sécurité

Table des matières

Introduction **3**

Cybersécurité **4**

Soyez vigilants quand vous vous connectez au portail de Neuflize OBC (https://www.neuflizeobc.fr/) 4

Utilisez des mots de passe robustes et différents 6

Fraude **7**

Faux conseiller bancaire 8

Faux livrets / placements / investissements 9

Faux RIB 10

Contacts utiles **11**

Introduction

La protection de vos données personnelles et la sécurisation de vos opérations sont une priorité majeure pour Neuflize OBC.

Cette brochure a vocation à vous accompagner dans cette démarche de sécurisation. Elle décrit les bons réflexes à adopter face aux risques de fraudes et aux cybermenaces, qui sont en constante évolution.

Les bonnes pratiques et conseils énoncés dans les pages suivantes peuvent vous être utiles autant pour la gestion de vos activités bancaires que dans votre vie quotidienne[1].

[1] Ils sont fournis à titre informatif et ne sauraient être exhaustifs. Face aux méthodes évolutives et toujours plus novatrices utilisées par les fraudeurs, il appartient à chacun de rester vigilant et de se tenir régulièrement avisé

Cybersécurité

Les principaux conseils en matière de cybersécurité

Soyez vigilants quand vous vous connectez au portail de Neuflize OBC (https://www.neuflizeobc.fr/)

L'accès à votre espace bancaire en ligne est particulièrement sensible (données personnelles, informations confidentielles, opérations). Les personnes malveillantes peuvent en effet chercher à récupérer ces accès pour détourner des fonds. Pour cela, adoptez quelques réflexes simples pour protéger vos identifiants et vos transactions.

- Bannissez les moteurs de recherche pour retrouver l'adresse de votre banque en ligne : les liens affichés peuvent rediriger vers des sites non fiables.
- Contrôlez toujours l'adresse du site (URL du site) : soyez attentif à la moindre anomalie (lettres inversées, caractères manquants, extension inhabituelle, etc.).
- Privilégiez la création et l'utilisation d'un favori pour accéder au site officiel de votre banque afin de vous prémunir contre les sites pirates visant à voler vos identifiants.
- Ne cliquez jamais sur des liens reçus par SMS, e-mail, messagerie (WhatsApp, etc.), même s'ils semblent provenir de votre banque.
- Méfiez-vous des demandes inhabituelles (numéro de téléphone, code supplémentaire, information non demandée habituellement, etc.) ou lorsqu'un écran noir apparaît pendant votre navigation sur le site.
- Lisez toujours les messages de validation avant de confirmer une action.
- Ne validez jamais une action que vous n'avez pas initiée ou qui ne correspond pas à ce que vous êtes en train de faire :
  - Vous ne reconnaissez pas l'action demandée : refusez et quittez immédiatement la session.
  - Demande d'un code additionnel pour sécuriser votre connexion alors que le message reçu concerne l'installation ou l'activation de l'application mobile de Neuflize OBC : ne validez pas !

En cas de doute, déconnectez-vous immédiatement puis contactez nos services sans attendre.

Utilisez des mots de passe robustes et différents

NB : les accès au site de Neuflize OBC ne se faisant pas via identifiant et mot de passe, ce paragraphe s'applique dans le cadre de votre vie quotidienne.

- Utilisez un mot de passe différent pour chaque service ;
- Utilisez des générateurs de mot de passe (le site de la CNIL propose ce service gratuit : **https://www.cnil.fr/fr/generer-un-mot-de-passe-solide) ;**
- Utilisez un gestionnaire de mot de passe (Keepass, Keeper) ;
- Changez votre mot de passe régulièrement (nous préconisons une fréquence trimestrielle) et immédiatement au moindre soupçon ;
- Ne communiquez jamais votre mot de passe à un tiers.

MÉMO

Fraude

Les bonnes pratiques à adopter face aux tentatives de fraude que vous pouvez rencontrer

Faux conseiller bancaire

Les fraudeurs tentent régulièrement de se faire passer auprès de nos clients pour un collaborateur de Neuflize OBC. Ils peuvent pour cela vous envoyer un email alarmant vous demandant d'activer un lien ou de rappeler un numéro, soit tenter de vous joindre directement (parfois en utilisant notre numéro de téléphone). Sous prétexte d'une potentielle opération frauduleuse ils vous demandent d'effectuer des manipulations (scanner un QR Code, valider l'annulation d'une opération, transférer des fonds vers un compte ouvert à votre nom pour les sécuriser). Ils peuvent également tenter d'obtenir des informations confidentielles (identifiants de connexion, informations de votre carte bancaire).

Les bons réflexes :

- Aussi crédible que puisse vous paraître la démarche, raccrochez et contactez nos services ;
- Si l'appel a lieu le soir ou le weekend, c'est une tentative de fraude, n'effectuez aucune manipulation ! En effet, nous ne vous appellerons jamais en dehors des heures ouvrées ;
- Si quelqu'un vous propose le service d'un coursier pour accélérer le renouvellement de votre carte, ou sécuriser vos objets de valeur : **REFUSEZ !** C'est une escroquerie. La banque n'enverra jamais un collaborateur à votre domicile, de ce fait, ne communiquez jamais vos données personnelles.

Faux livrets / placements / investissements

Vous pouvez faire l'objet de sollicitations pour des placements ou des investissements rémunérateurs, par email, via des réseaux sociaux, ou pour donner suite à vos propres recherches sur internet lors desquelles vous avez fourni vos coordonnées. Les fraudeurs prétendent le plus souvent tirer profit de stratégies d'investissement en cryptomonnaies, de trading haute fréquence ou d'algorithmes d'intelligence artificielle pour justifier des gains élevés et rapides. Ils usurpent généralement la marque d'une banque ou d'un courtier (français ou étranger) pour crédibiliser la démarche, et se font parfois passer pour un véritable collaborateur de cet établissement. Le but est de gagner votre confiance pour vous amener à verser progressivement des sommes conséquentes. À cet effet, vous percevrez les premiers mois des versements d'intérêts.

Les bons réflexes :

- Vérifiez toujours qui sont vos interlocuteurs. Appelez directement l'établissement financier représenté, sur un numéro figurant dans des annuaires publics ou via le site internet officiel. Demandez à parler au collaborateur supposé vous avoir contacté pour vérifier qu'il est bien à l'origine de la proposition.
- N'hésitez pas à contactez le service de protection des épargnants de l'Autorité des Marchés Financiers (AMF Protect Epargne - Qu'est-ce que « Epargne Info Service » ? | AMF), qui peut vous aider dans vos vérifications, et vous confirmer si l'intermédiaire financier est autorisé à proposer ses services en France.
- Gardez à l'esprit qu'un taux d'intérêt ou de rendement trop élevé (qui de plus est présenté sans risque pour le capital investi) cache souvent une arnaque. Vérifiez toujours avant d'investir, surtout si l'offre semble trop belle pour être vraie. Méfiez-vous des offres à durée très limitée et réservées à quelques personnes privilégiées.
- Soyez vigilant quant à la destination des fonds. Transférer des fonds dans un pays différent de celui de l'intermédiaire est un signal d'alerte, tout comme la multiplication des comptes destinataires des fonds.

Faux RIB

La fraude au changement de coordonnées bancaires est devenue très courante. Une fois un ordre de virement émis, il ne peut pas être annulé, ce qui est d'autant plus vrai avec les virements instantanés.

Si vous recevez, de la part de l'un de vos créanciers (bailleur, opérateur téléphonique, fournisseur, etc.), une information de changement de coordonnées bancaires, faites preuve de la plus grande vigilance avant d'effectuer un paiement vers le nouveau compte. De fausses demandes, exploitant de boîtes mail piratées ou de fuites de données, sont régulièrement constatées.

Les bons réflexes :

- Vérifiez la véracité de l'information en contactant la personne (ou l'organisme) aux coordonnées habituelles, ou trouvées sur un annuaire public ;
- Informez votre banque et la personne (ou organisme) dont l'identité a été usurpée ;
- Signalez toute anomalie ou opération bancaire suspecte à votre banque.

Protégez vos moyens de paiements

Vos moyens de paiements (carte bancaire, chéquier) sont sensibles. Pour vous prémunir de tout risque d'utilisation malveillante, ils ne doivent pas être facilement accessibles à des tiers.

Les bons réflexes :

- Conservez dans un endroit sûr vos chéquiers et cartes bancaires.
- Ne communiquez à personne vos informations de cartes bancaires.
- Surveiller régulièrement et attentivement vos relevés de comptes, et signalez au plus tôt à votre banque tout débit suspect.

Contacts utiles

Support digital

Du lundi au vendredi de 8h30 à 18h30

Téléphone

+33 (0) 1 56 21 94 99

E-mail

supportdigitalnobc@fr.abnamro.com

Service prévention fraude

Du lundi au vendredi de 8h30 à 18h30

Téléphone

+33 (0) 1 56 21 78 00

E-mail

nobc.prevention.fraude@fr.abnamro.com

www.neuflizeobc.fr

Neuflize OBC, au cœur de la gestion de vos patrimoines privés et professionnels

ABN AMRO BANK N.V., société néerlandaise. Société au capital de 940 000 001 euros, immatriculée auprès de la chambre de commerce d'Amsterdam (n°34334259). Siège social : Gustav Mahlerlaan 10, 1082 PP, Amsterdam, Pays-Bas. Etablissement de crédit agréé par la De Nederlandsche Bank (Pays-Bas), supervisé par la Banque Centrale Européenne et l'Autoriteit Financiële Markten. Succursale Française exerçant sous le nom commercial **'Banque Neuflize OBC'** – n° 850 479 718 RCS Paris - 119 - 121, boulevard Haussmann, 75008 Paris, France - Numéro ORIAS : 12 020 215 - Intermédiaire en assurance - supervisée pour certaines activités et services par l'Autorité de Contrôle Prudentiel et de Résolution et l'Autorité des Marchés Financiers - Carte professionnelle de l'immobilier n° CPI 75012023000000163 délivrée par la CCI Paris Île-de-France; engagement de non détention de fonds, absence de garantie financière.

56604_DP-Brochure_Cyber_PP-Juillet_2026