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

Sensibilisez vos collaborateurs 6

Établissez des modes de fonctionnement sécurisés avec vos partenaires 7

Sécurisez votre site internet 8

Maitrisez la diffusion des données relatives à votre société 9

Choisissez les mots de passe avec soin 10

Fraude **11**

Fraude au Président 12

Fraude aux faux RIB / IBAN (ou fraude au fournisseur) 13

Fraude aux faux chèques 13

Sécurisez vos processus de paiements 14

Contacts utiles **15**

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.

Sensibilisez vos collaborateurs

La plupart des cyberattaques en entreprise ciblent les collaborateurs en utilisant les failles humaines. Ils peuvent être contactés afin d'obtenir des informations sur l'entreprise, des identifiants de comptes bancaires ou leur faire réaliser des paiements.

- Sensibilisez vos collaborateurs à la cybersécurité dans leur quotidien professionnel avec des exemples concrets.
- Adoptez une charte informatique pour préciser les règles d'utilisation du matériel informatique, de la messagerie, y compris lors des déplacements professionnels ou en cas d'utilisation mixte de l'ordinateur (usage professionnel et personnel).
- Organisez des formations spécifiques pour les fonctions les plus exposées(par exemple : personnes habilitées à réaliser des paiements) et planifiez des séances de rappel car les méthodes de fraudes et d'attaques cyber se renouvellent régulièrement.
- Mettez en place des protocoles et des consignes de sécurité, particulièrement pour les paiements, les changements de coordonnées bancaires et contrôlez leur bonne application.

En cas de fraude avérée :

- Contactez votre banque immédiatement pour stopper les transactions frauduleuses ;
- Faites opposition à votre carte bancaire ;
- Changez vos mots de passe ou codes, s'ils ont été révélés ;
- Surveillez vos comptes bancaires pour détecter toute anomalie et la contester.

Établissez des modes de fonctionnement sécurisés avec vos partenaires

Les liens que vous entretenez avec vos partenaires (clients, fournisseurs, comptables, banquiers, etc.) sont autant d'opportunités pour les cybercriminels de tenter de vous escroquer. L'identité d'un de vos partenaires peut être usurpée en vue de vous faire croire à un changement de domiciliation bancaire à des fins de détournement de paiement, ou encore vous faire réaliser une action pour prendre le contrôle/pirater votre système informatique.

Bonnes pratiques :

- Établissez des protocoles précis pour la réalisation de toutes vos opérations bancaires ;
- Contrôlez les informations diffusées sur votre entreprise notamment sur Internet et n'échangez pas d'informations sensibles avec vos partenaires en dehors de circuits sécurisés.

Sécurisez votre site internet

Sur Internet, les cyberattaques peuvent concerner vos transactions ainsi que le vol de données de vos clients. Votre site peut également être piraté et bloqué (c'est le « déni de service »). Vous devez assurer la sécurité de votre site et des données de vos clients. Il en va de votre crédibilité professionnelle et donc de la survie de votre activité.

Bonnes pratiques :

- Installez un certificat de sécurité en « https », choisissez un hébergement sécurisé avec une assistance 24h/24 ;
- Mettez en place l'authentification forte pour vos clients en e-commerce comme la réglementation l'exige ;
- Chiffrez les données de vos clients et ne conservez que les données utiles : évitez de stocker les numéros de carte bancaire ;
- Changez régulièrement vos mots de passe, mettez à jour vos antivirus et vos logiciels.

En cas d'incidents potentiels ou avérés :

- Déposez plainte auprès de la police en communiquant les informations recueillies (type de carte, adresse IP...) et prévenez votre banque/prestataire de paiement.
- En cas d'attaque informatique, demandez l'assistance d'un professionnel labellisé sur cybermalveillance.gouv.fr. Contactez aussi le CSIRT de votre région (Computer Security Incident Response Team). Ce centre de réponse aux incidents cyber propose notamment aux PME et associations une assistance gratuite de 1er niveau, complémentaire à celle proposée par les prestataires de Cybermalveillance (Assistance aux victimes de cybermalveillance | Site Officiel).
- En cas de violation des données personnelles de vos clients, signalez l'incident à la Commission Nationale de l'Informatique et des Libertés (Professionnel | CNIL) dans les 72 heures.

Maîtrisez la diffusion des données relatives à votre société

De nombreuses escroqueries sont rendues possibles grâce aux informations récupérées sur Internet (annonces légales, site de l'entreprise ou de ses partenaires commerciaux, réseaux sociaux…).

Elles peuvent aussi être recueillies auprès des collaborateurs par téléphone par exemple. Ces pratiques sont appelées « ingénierie sociale ».

Bonnes pratiques :

- Assurez-vous que les contenus publiés sur votre site et sur les réseaux sociaux ne révèlent pas d'informations sensibles (exemple : organigramme de votre entreprise) ;
- Contrôlez régulièrement les informations disponibles en tapant le nom de votre entreprise dans les moteurs de recherche.

Choisissez les mots de passe avec soin

Les attaques informatiques reposent souvent sur le déchiffrage d'un mot de passe que ce soit pour compromettre ou accéder à un logiciel, un site marchand, un site Internet, une application bancaire...

Bonnes pratiques :

- Définissez un mot de passe spécifique pour chaque service, appareil, logiciel, application utilisée par votre entreprise :
  - Il ne doit contenir aucune information professionnelle ou personnelle qui pourrait être découverte facilement par un tiers, à partir de votre k-bis par exemple (date de création de l'entreprise, votre date de naissance…).
  - Il doit combiner si possible des lettres (majuscules, minuscules), des chiffres, des caractères spéciaux et être suffisamment long (12 caractères minimum). N'hésitez pas à consulter le site de la CNIL (https://www.cnil.fr/fr/generer-un-mot-de-passe-solide) ;
- Les mots de passe ne doivent jamais être enregistrés sur vos appareils, utilisez plutôt un gestionnaire de mots de passe ou un fichier chiffré (exemple : Keeper ou Keepass) ;
- Adoptez une hygiène des mots de passe : pensez à les modifier à minima tous les 90 jours.

Fraude

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

Fraude au Président

Le fraudeur contacte une personne habilitée à effectuer des paiements, en se faisant passer pour un membre exécutif de votre société (Président, Directeur Général, etc.), le plus souvent en son absence.

Il prétexte une opération stratégique à effectuer en urgence et dans le plus grand secret (éventuellement de faux avocats interviennent pour accentuer le caractère légitime et urgent de l'opération).

Des méthodes sophistiquées et une observation méthodique du fonctionnement de la société et du rôle des collaborateurs clés peuvent être employées (ingénierie sociale, spoofing, deepfake, …) pour cibler un interlocuteur au sein de la société victime. Les montants en jeu étant conséquents (plusieurs centaines de milliers d'euros, voire plus), les fraudeurs n'hésitent pas à investir du temps pour cibler leur victime et le moment de l'intervention (voyage du dirigeant usurpé par exemple, changement de l'un des membres de la Direction, …).

Une opération d'une telle envergure ne se réalise jamais dans de telles conditions. L'urgence et la confidentialité excessives sont des signaux d'alertes. Prenez contact directement avec le dirigeant sur un numéro connu ou referez-en à votre responsable.

Pour prévenir ce risque formez/informez vos équipes !

Fraude aux faux RIB / IBAN (ou fraude au fournisseur)

Un escroc se fait passer pour votre fournisseur. Il a pour cela préalablement piraté une boîte mail ou exploite des données volées. Il vous demande, le plus souvent par email, de faire vos virements sur un nouveau compte bancaire. Si vous payez sur ce compte sans vérification préalable, l'argent est perdu.

Contactez toujours votre interlocuteur sur ses coordonnées habituelles avant toute modification (ou création) d'un IBAN.

Nous constatons une variante de plus en plus fréquente visant le détournement de virements de salaires. Un fraudeur se fait passer pour un employé auprès des services RH (via une adresse e-mail usurpant celle du collaborateur, ou par téléphone) et demande la modification de ses coordonnées bancaires. Une vérification systématique doit être effectuée auprès de l'employé de préférence via des canaux internes.

Fraude aux faux chèques

N'acceptez jamais de rembourser par virement tout ou partie d'un chèque encaissé !

Un escroc peut volontairement émettre un chèque d'un montant supérieur à ce qu'il vous doit, puis vous contactez pour vous signaler l'erreur et vous demander de lui rembourser la différence par un virement.

Le chèque, même s'il est dans un premier temps crédité sur votre compte, pourrait-être annulé durant un délai de 2 mois s'il s'avère volé ou faux. Vous perdriez donc le montant du virement effectué.

C'est un procédé couramment utilisé par des escrocs dans le cadre d'achat d'œuvres d'art par exemple.

Sécurisez vos processus de paiements

Pour éviter qu'un paiement d'un montant conséquent puisse être réalisé par un unique employé, pensez à mettre en place des délégations de signature limitées au strict nécessaire en termes de montant, et favorisez une double signature des paiements de votre entreprise.

Vous limiterez ainsi le risque d'une fraude interne par un employé malveillant, ainsi que le risque d'une fraude par manipulation de l'un de vos collaborateurs.

Depuis le mois d'octobre 2025, un contrôle permet de s'assurer de la cohérence entre l'IBAN et le nom du bénéficiaire d'un virement SEPA. Ce contrôle est intégré à notre application mobile et à notre site internet transactionnel pour vos virements unitaires.

Pour vos remises de fichiers de virements SEPA, cette vérification n'est pas automatique lors de l'exécution des paiements. Pensez à vérifier cette concordance, soit au travers de l'outil que nous mettons à votre disposition sur notre site transactionnel, soit au moyen de votre propres outils avant de nous transmettre vos fichiers pour exécution. Toute différence signalée par le contrôle nécessite une vérification complémentaire de la validité des coordonnées bancaires pour réduire le risque de fraude.

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.

56603_DP-Brochure_Cyber_PM-Juillet_2026