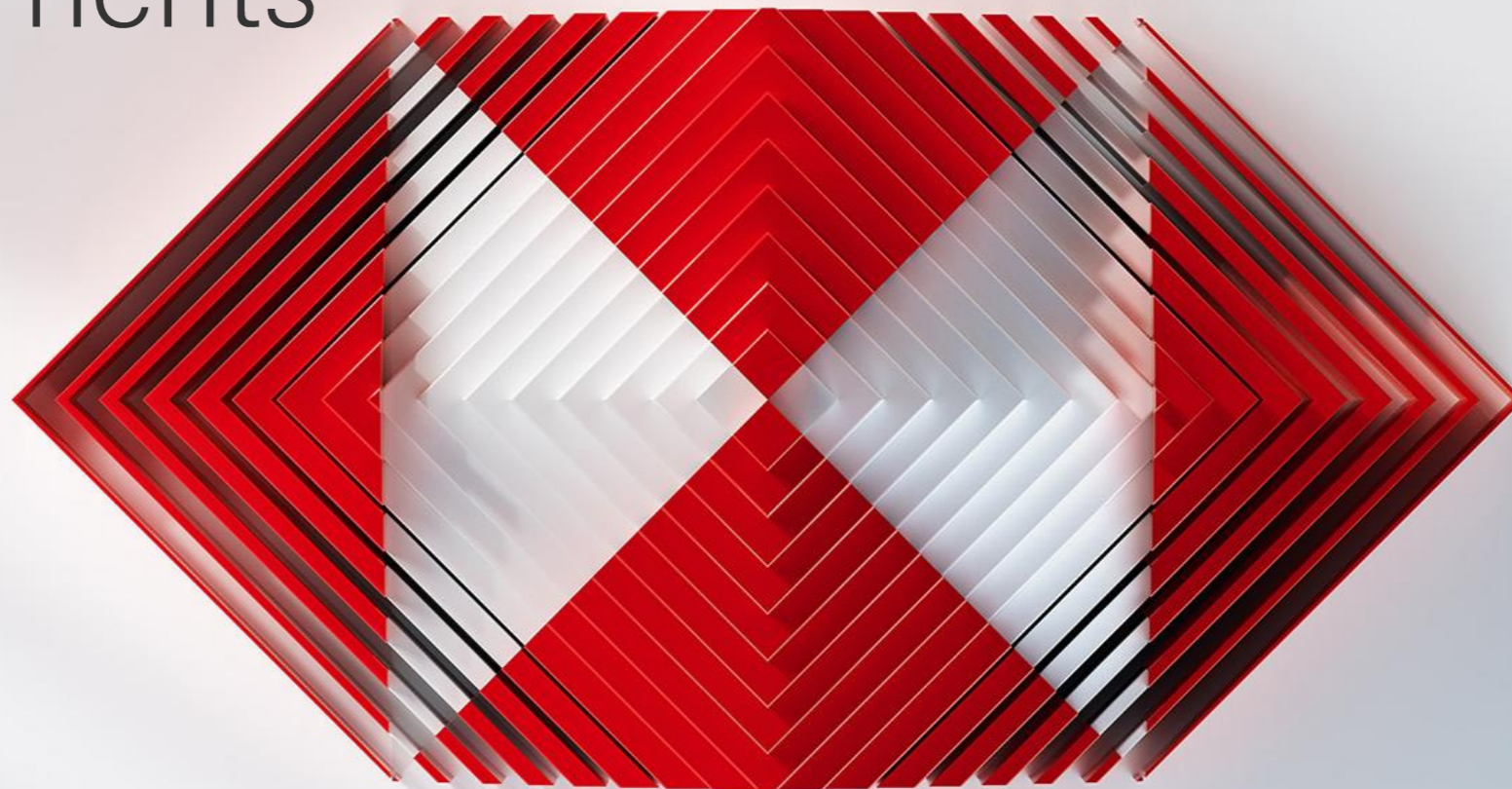


Corporate & Institutional Banking

# Guide HSBC de Sensibilisation à la Fraude aux Paiements



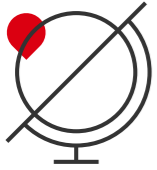
Protégez votre  
entreprise contre  
la fraude et la  
cybercriminalité



# Fraude : protégez votre entreprise

La fraude est aujourd'hui l'une des menaces les plus courantes qui pèse sur les entreprises.

La fraude peut entraîner des pertes financières importantes. Toutes les entreprises sont exposées à ce risque, quelle que soit leur taille. Ce guide a été conçu pour vous accompagner ainsi que vos collaborateurs dans le but de détecter et d'éviter les escroqueries autant que possible, mais aussi de prendre les mesures nécessaires si vous en êtes victime.

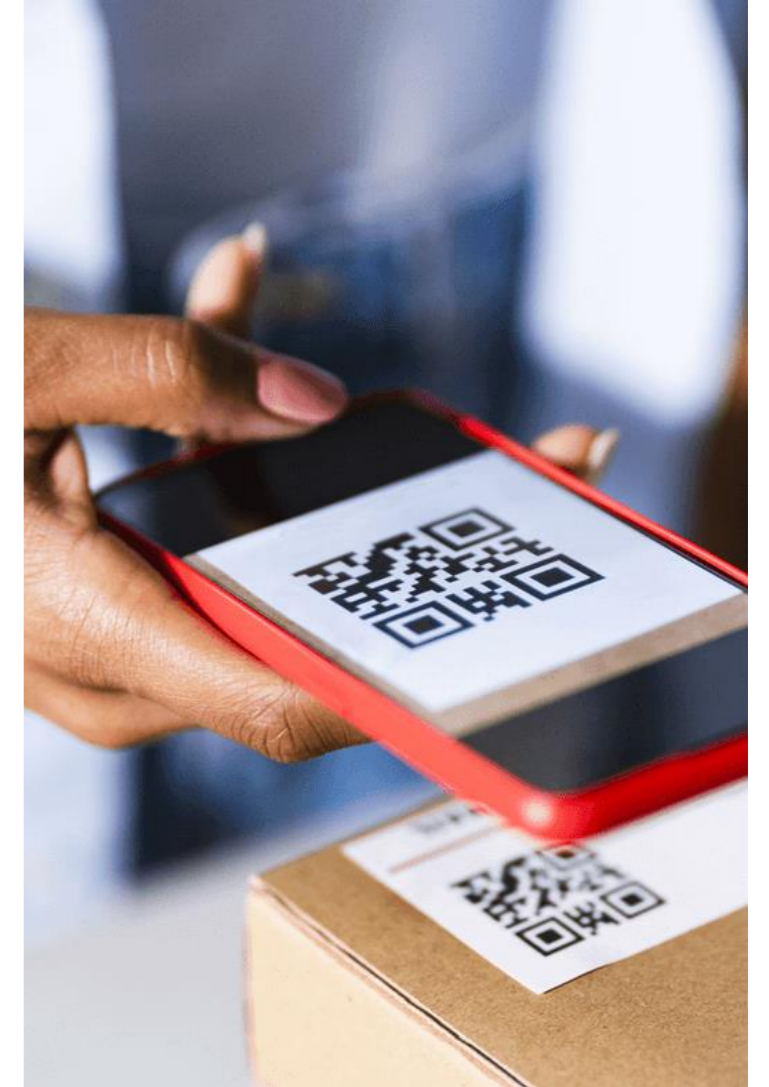


## 55 milliards \$

Coût mondial des attaques par usurpation des e-mails professionnels entre octobre 2013 et décembre 2023

Source : Centre des plaintes liées à la cybercriminalité du FBI

Ce guide présente les principaux types de fraude, susceptibles de viser votre entreprise et propose des mesures pratiques à mettre en place pour prévenir la fraude. Former votre personnel sur les risques de fraude permet de mieux se protéger. Ce guide fournit de nombreux conseils et des checklists à partager avec vos équipes responsables de la gestion et des paiements.

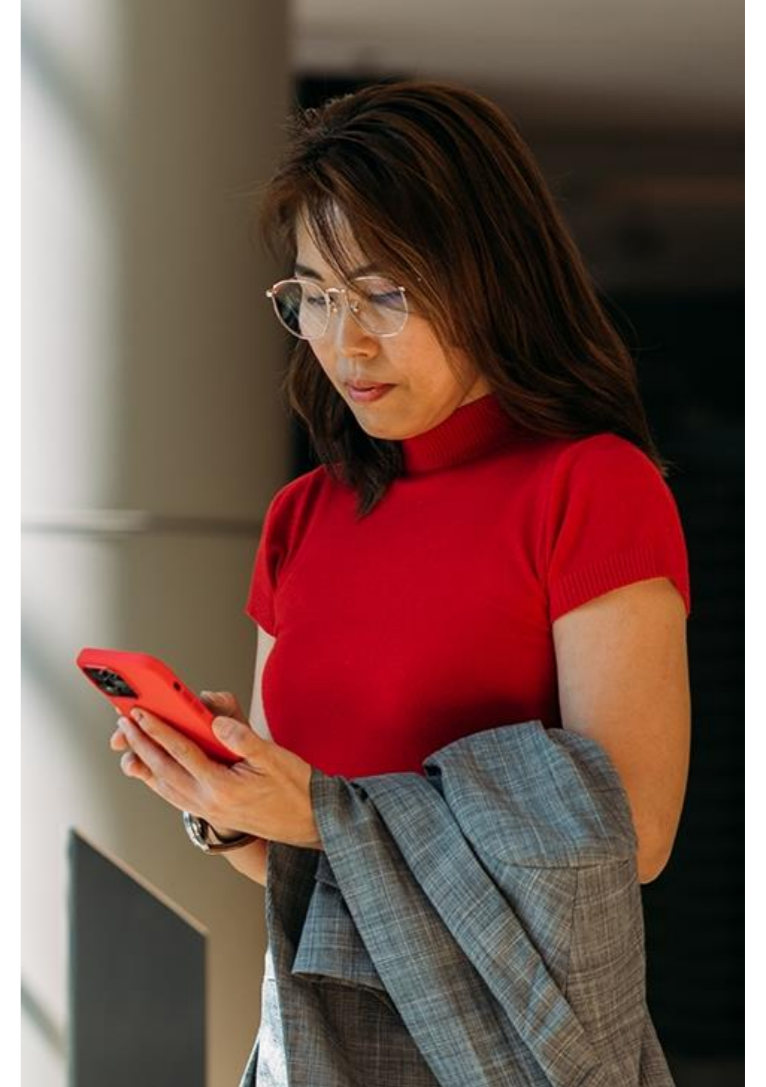


Les différents  
types de fraudes  
susceptibles de  
viser votre  
entreprise

# Comment un fraudeur pourrait vous contacter?

Les escroqueries **APP** (Authorized Push Payment) se produisent lorsqu'une entreprise est trompée et incitée à envoyer de l'argent à un fraudeur qui se fait passer pour un bénéficiaire légitime. Il est important de comprendre comment les criminels peuvent entrer en contact avec vous.

- ◆ Le **phishing** (ou hameçonnage) est une pratique commune à de nombreuses escroqueries APP. Cela consiste à tromper la victime pour l'inciter à cliquer sur un lien qui téléchargera un logiciel malveillant ou les dirigera vers un faux site Web, par exemple. Les liens de phishing peuvent être intégrés aux messages reçus par e-mail, ou via des plateformes de messagerie (WhatsApp, Viber...).
- ◆ Le **vishing** (ou arnaque par téléphone) : si vous recevez un appel téléphonique inattendu à propos d'argent, il y a de fortes chances qu'il s'agisse d'une escroquerie. Les fraudeurs peuvent prétendre être votre banque ou une entreprise de confiance. Ils peuvent avoir connaissance de certaines de vos informations personnelles, et peuvent même appeler d'un numéro que vous connaissez à l'aide d'une technique d'usurpation de numéro de téléphone ou « Phone Number Spoofing ».
- ◆ Le **smishing** consiste à envoyer de faux SMS, dans lesquels le fraudeur se fait passer pour votre banque ou une autre organisation légitime. L'objectif est d'obtenir vos informations personnelles ou financières afin de pouvoir accéder à votre compte. Les fraudeurs peuvent également utiliser des plateformes de messagerie connue.



La fraude par  
usurpation  
d'e-mails  
professionnels

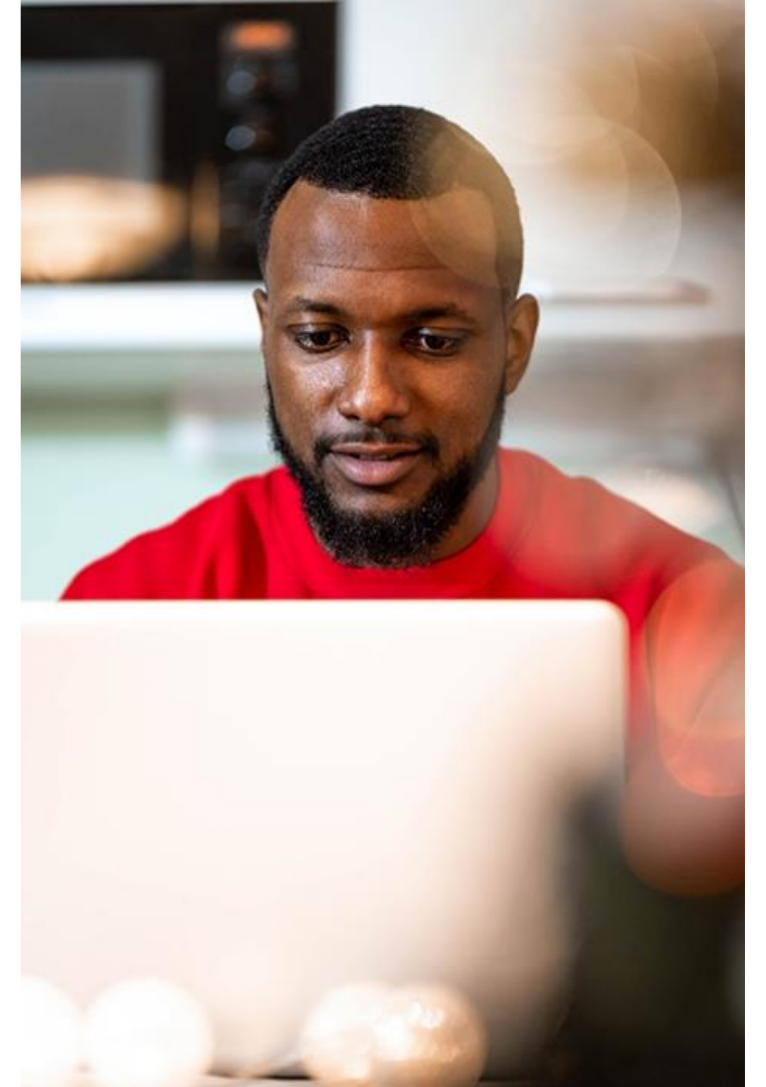
# Fraude par usurpation d'e-mails professionnels

L'e-mail frauduleux est souvent utilisé lors des fraudes au changement de coordonnées bancaires.

Lorsque les paiements sont exigibles, les fraudeurs envoient un e-mail qui paraît être un message authentique d'un fournisseur. Ils vous annoncent que les données bancaires pour votre paiement ont changé, vous fournissent de nouvelles données et une nouvelle demande.

## Ces e-mails sont parfois difficiles à repérer :

- ◆ Les fraudeurs utilisent souvent l'adresse de messagerie habituelle du fournisseur ou une adresse de messagerie usurpée qui ressemble à l'adresse légitime.
- ◆ Les e-mails envoyés paraissent authentiques.
- ◆ Il peut ne pas y avoir de différence notable dans la signature électronique de l'employé du fournisseur ou dans le style de communication.
- ◆ Dans certaines circonstances, le fraudeur peut avoir obtenu l'accès à la boîte de réception de votre expéditeur, et dans ce cas l'e-mail proviendra d'une adresse électronique authentique. Il aura ainsi accès aux échanges d'e-mails et pourra répondre en utilisant un langage et un ton similaires.
- ◆ Information importante : le paiement qui est demandé par les fraudeurs est très souvent dû.
- ◆ **La seule différence vient souvent du changement de données bancaires.**



# Comment se produit la fraude par e-mail ?

## Prise de contrôle de compte de messagerie

- ◆ Le fraudeur utilise le piratage ou des informations d'identification de compte volées, pour accéder à un compte de messagerie professionnel.
- ◆ Les informations de connexion du compte peuvent avoir été obtenues par une attaque par phishing ou par une violation de données.
- ◆ Le fraudeur peut recueillir des renseignements sur les contacts de l'utilisateur le type de courrier électronique et les données personnelles pour rendre ses messages plus convaincants.

## Usurpation d'identité par e-mail

- ◆ Le fraudeur crée un compte avec une adresse très similaire à la vraie.
- ◆ Ou bien il peut falsifier l'en-tête de l'e-mail, en espérant que le destinataire ne le remarque pas et traite l'e-mail comme s'il s'agissait d'un message légitime.



## Fraude au président

Les criminels usurpent l'identité d'un cadre supérieur de l'entreprise.

- ◆ Ils envoient un e-mail au service comptable, demandant qu'un paiement de montant important soit effectué d'urgence. Cela peut même concerner une acquisition ou une autre opération importante.
- ◆ Les fraudeurs opèrent souvent lorsque la personne dont l'identité a été usurpée est loin/absente, ce qui rend plus complexe la vérification des données.
- ◆ Encore une fois, la messagerie peut avoir été compromise par le phishing ou la violation des données, et les informations avoir été recueillies par le biais de sites Web d'entreprises ou de réseaux sociaux.

# Fraude par la prise de contrôle de compte

# Fraude par la prise de contrôle de compte

## Qu'est-ce que la prise de contrôle de compte ?

Ce type de fraude survient lorsqu'un fraudeur accède à votre banque en ligne, généralement en vous incitant à divulguer des informations, ou à réinitialiser vos mots de passe et numéros de sécurité afin que vous ne puissiez plus accéder à votre compte. Il peut modifier le numéro de téléphone et l'adresse e-mails associés au compte, ce qui lui permet de se faire passer pour un utilisateur légitime.

## Prise de contrôle de l'accès à la banque à distance

Ce type de fraude se produit lorsqu'un fraudeur prend le contrôle de votre appareil et l'utilise pour effectuer des paiements depuis votre compte bancaire à votre insu. Cela survient généralement lorsque les fraudeurs vous ont envoyé un lien, demandé de visiter un site Web ou de télécharger un logiciel, leur permettant d'accéder à distance à votre appareil.

La suite de ce guide vous propose des mesures pratiques à mettre en place pour prévenir la fraude.



### Usurpation de numéro de téléphone

Il s'agit d'une technique modifiant l'identité visible de l'appelant (le numéro depuis lequel ils appellent) pour faire apparaître un numéro officiel pouvant, par exemple, appartenir à votre banque. Le numéro peut être exactement le même ou rester très similaire. Ils peuvent également vous appeler depuis un numéro masqué.



### Logiciels malveillants et phishing

Les fraudeurs utilisent des logiciels et des liens malveillants pour récupérer des informations personnelles.

Ces informations seront utilisées pour paraître plus authentique ou pour pirater votre compte bancaire.



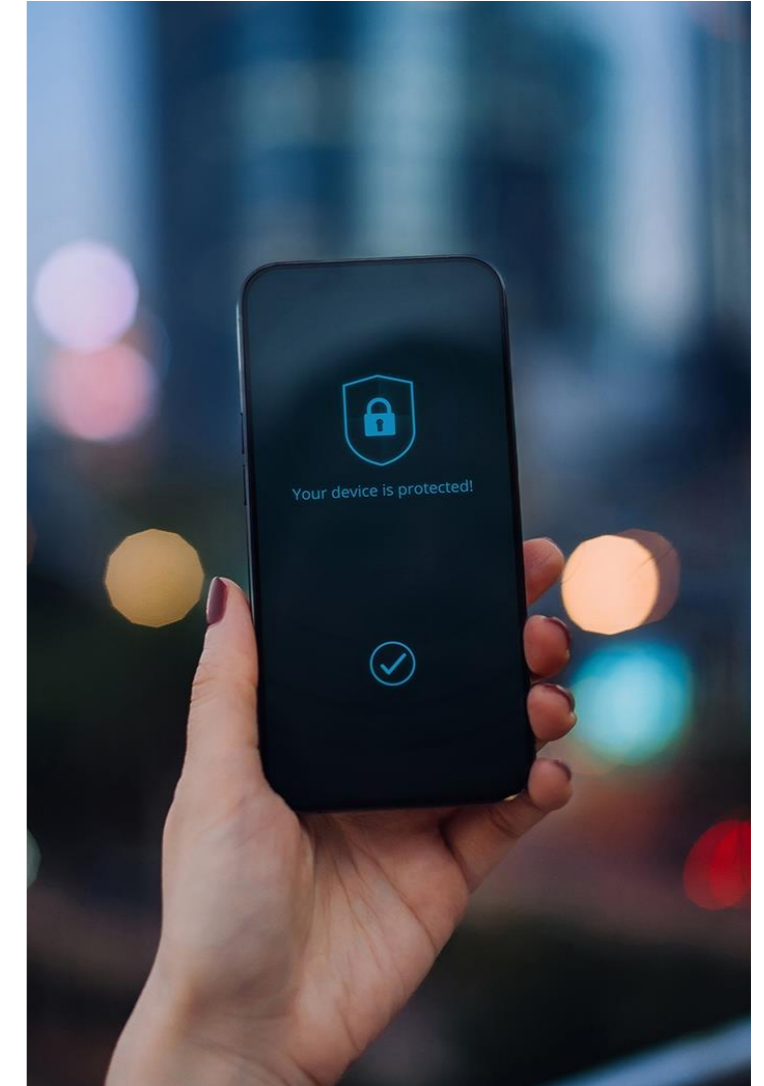
### Codes d'autorisation

Personne, pas même votre banque, ne vous donnera d'instructions sur la manière d'utiliser votre dispositif de sécurité physique ou numérique (également appelé clé de sécurité), et personne ne vous demandera de codes d'autorisation d'accès aux services bancaires en ligne.

# Prise de contrôle de votre compte à distance

## Recommandations

- ◆ Ne communiquez jamais vos noms d'utilisateur, mots de passe, codes d'autorisation ou mots de passe à usage unique (OTP) de vos services bancaires en ligne.
- ◆ N'oubliez pas que les numéros peuvent être usurpés et ne vous fiez jamais à l'ID de l'appelant pour savoir qui appelle.
- ◆ En cas d'appels inattendus, n'hésitez pas à rappeler en utilisant un numéro que vous connaissez, comme un numéro officiel ou celui au dos de votre carte bancaire. Utilisez un autre téléphone ou appelez d'abord un contact connu pour vous assurer que la ligne est « libre ».
- ◆ Méfiez-vous des e-mails et SMS suspects, à plus forte raison lorsque ceux-ci contiennent des liens et des demandes d'informations. Validez toujours ces demandes directement avec l'entreprise, en utilisant les conseils de prise de contact ci-dessus.
- ◆ Ne cliquez jamais sur des liens, ne visitez jamais de site Web suspect et ne téléchargez jamais de logiciels en raison d'un appel téléphonique que vous n'attendiez pas.
- ◆ Votre dispositif de sécurité (ou clé de sécurité) vous est strictement personnel. Si quelqu'un vous appelle et vous demande d'utiliser cet appareil, mettez fin à l'appel et contactez immédiatement votre banque.
- ◆ HSBC ne vous demandera jamais de participer à une enquête en cours, ne vous conseillera jamais sur la façon de répondre à des questions, ni ne vous demandera d'envoyer de l'argent sur un compte sécurisé.
- ◆ Assurez-vous de disposer d'une procédure de sécurité claire pour les équipes responsables des paiements, et que ces équipes ne puissent pas autoriser des paiements nouveaux ou modifiés, sans qu'il y ait de validation appropriée.
- ◆ Formez vos équipes : assurez-vous que tous les collaborateurs sont sensibilisés à la fraude par prise de contrôle de l'accès à distance et qu'un processus d'escalade est en place.
- ◆ Développez une culture de vigilance accrue dans votre entreprise pour tous les paiements pouvant inclure un processus d'approbation à deux niveaux.



# Comment réduire le risque de fraude lors des paiements

# Réduisez le risque de fraude aux paiements

Chaque entreprise peut prendre des mesures simples et abordables pour permettre de réduire les risques de fraude. Chacun a un rôle à jouer.

- ◆ Renforcez la vigilance des services de votre entreprise qui pourraient être vulnérables.
- ◆ Formez les employés sur la façon d'identifier et d'éviter les arnaques, assurez-vous qu'ils sont informés des politiques et procédures de sécurité de l'entreprise.
- ◆ Vérifiez tout particulièrement **chaque nouveau bénéficiaire ou compte doit être vérifié.**
- ◆ Interrogez-vous sur chaque demande inhabituelle ou hors contexte.

Les prochaines diapositives fournissent des conseils plus détaillés pour les personnes responsables des paiements.



# Vérifiez l'adresse de messagerie

## Les fraudeurs se font passer pour des personnes de confiance.

- ◆ Si le nom de l'expéditeur de l'e-mail vous est familier (le nom de quelqu'un que vous connaissez ou avec qui vous échangez régulièrement), **assurez-vous que l'adresse e-mail correspond bien.**
- ◆ S'il s'agit d'un collaborateur de votre entreprise, l'adresse e-mail doit être enregistrée dans le répertoire d'e-mails de la société (si vous en avez un).
- ◆ Assurez-vous que le nom du domaine est correctement orthographié. Souvent, les fraudeurs créent de faux domaines qui ressemblent de près aux vrais, mais modifient une lettre ou deux en espérant que les destinataires ne le remarquent pas. Par exemple, J@**rn**business.com, au lieu de J@**m**business.com.
- ◆ Il faut savoir que le nom affiché peut cacher la véritable adresse électronique de l'expéditeur, et peut être révélé en passant la souris dessus.

# Vérifiez attentivement l'e-mail

## L'urgence est un signal d'alerte

- ◆ Considérez tout e-mail relatif aux paiements comme suspect s'il utilise un langage urgent, ou s'il justifie l'absence d'option de contre-appel.
- ◆ Certains e-mails de phishing sont mal écrits. Même si l'orthographe est correcte, ils contiennent souvent des erreurs de grammaire. Traitez les e-mails externes avec une extrême prudence, en particulier ceux qui contiennent des liens ou des pièces jointes. Sachez que l'IA générative permet aux fraudeurs de créer plus facilement des e-mails malveillants convaincants.
- ◆ Si vous ne vous attendez pas à recevoir une telle communication et/ou ne reconnaissez pas l'expéditeur, **ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes.**



# Vérifiez les nouveaux bénéficiaires et les changements de données bancaires

## Vérifiez auprès du donneur d'ordre en utilisant des coordonnées connues.

- ◆ Dans la mesure du possible, essayez de parler à quelqu'un que vous connaissez. Par exemple, si la demande de modification provient d'une personne de l'entreprise, essayez de confirmer la demande directement auprès de cette personne par téléphone. Si elle provient d'un fournisseur, appelez votre contact habituel par téléphone.
- ◆ **Ne répondez pas à l'e-mail et n'utilisez pas les coordonnées transmises dans l'e-mail avant de les avoir vérifiées.**
- ◆ Souvent, les cybercriminels envoient des e-mails de phishing à des personnes figurant dans les listes de contacts du compte auquel ils ont réussi à avoir accès. Cela signifie que vous pouvez reconnaître l'expéditeur parce que l'adresse électronique est exacte, alors que le message est suspect. Appelez votre contact et confirmez la demande envoyée par e-mail. Cela peut aussi permettre de l'avertir que sa messagerie a été compromise.



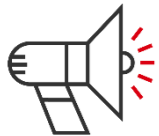
# Réduisez le risque de fraude aux paiements

La fraude peut viser tout type d'entreprise et de diverses façons.



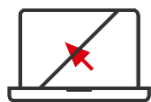
## Rédigez et mettez en place des procédures de sécurité claires pour les équipes responsables des paiements

Veillez à ce que tous les paiements soient correctement validés est l'action la plus importante en matière de prévention de la fraude. Rédigez une procédure pour que les équipes responsables des paiements ne puissent pas autoriser des paiements nouveaux ou modifiés, sans qu'il y ait de validation appropriée. Ainsi, les équipes responsables des paiements ne valideront pas de paiements sur la base d'e-mails non vérifiés ou d'instructions téléphoniques, même lorsqu'elles paraissent dignes de confiance. L'une des bonnes pratiques consiste à encourager vos collaborateurs à communiquer directement avec les bénéficiaires pour confirmer les demandes de paiement nouvelles ou modifiées.



## Sensibilisez les employés

Dispensez une formation adéquate aux employés. La sensibilisation à la fraude est la responsabilité de chacun dans une entreprise. Développez une culture axée sur les risques, et mettez en place une procédure pour que les employés signalent toute préoccupation à la direction. Le personnel doit se sentir en mesure de remettre en cause les instructions reçues concernant les paiements.



## Ayez conscience de votre empreinte numérique

Le partage d'un trop grand nombre d'informations sur les réseaux sociaux permet également aux escrocs de recueillir des informations sur vous, vos amis, votre famille et vos contacts, et peut être utilisé à des fins d'ingénierie sociale ou d'usurpation d'identité. Réduisez les risques de fraude en limitant la quantité d'informations personnelles que vous publiez.



## Encouragez tous les employés à réfléchir avant de cliquer

Il est concevable de cliquer sur les liens lorsque vous êtes sur des sites web de confiance. Cependant, évitez de cliquer sur les liens qui apparaissent dans des e-mails non vérifiés et des messages instantanés. En pointant votre souris sur un lien, vous serez en mesure de voir l'URL cachée et de vérifier sa légitimité. Vérifiez l'adresse e-mail, ainsi que la qualité de l'orthographe et de la grammaire avant de cliquer sur les liens ou de télécharger les pièces jointes.



## Renforcez vos mots de passe

Pensez à utiliser des gestionnaires de mots de passe ou une phrase secrète - une chaîne de mots qui est généralement plus longue qu'un mot de passe classique. Ces mots de passe sont faciles à mémoriser mais très difficiles à trouver pour les fraudeurs. Encouragez les employés à choisir trois mots aléatoires et à choisir un mélange de caractères et de symboles alphanumériques.



## Sachez comment agir en cas de fraude/cyberattaque

Si votre entreprise ou vous-même êtes victime d'une fraude, il est important d'agir rapidement. Signalez des incidents de sécurité connus ou suspectés aide à protéger l'environnement de travail. Contactez vos partenaires bancaires.

# Checklist : Equipe de Direction

Le moyen le plus efficace pour limiter l'impact de la fraude est d'empêcher qu'elle ne se produise. Cette checklist donne des conseils clés pour préserver la sécurité de votre entreprise.

- Votre entreprise a-t-elle des procédures qui prévoient la validation des nouvelles instructions de paiement ou des modifications des instructions de paiement? Vos collaborateurs savent-ils où trouver les coordonnées de vos contacts habituels ?
- Avez-vous des procédures décrivant comment, qui et par quels moyens vos collaborateurs peuvent saisir des paiements et comment ces demandes de paiement peuvent-elles être vérifiées en cas de doute ?
- Les mots de passe sont-ils suffisamment robustes ? (par exemple doivent-ils contenir un nombre minimum de caractères, des caractères alphanumériques et des caractères spéciaux ?). Avez-vous envisagé d'utiliser un gestionnaire de mots de passe ou d'imposer l'utilisation de phrases secrètes ?
- L'authentification à deux facteurs (2FA) a-t-elle été envisagée et appliquée dans la mesure du possible ?
- Vos collaborateurs savent-ils comment agir en cas d'envoi de paiement frauduleux ?
- Avez-vous un plan d'intervention en cas de cyber-incident, comme par exemple une adresse e-mail compromise ?
- Discutez-vous régulièrement des risques de fraude potentiels avec les personnes qui saisissent les paiements ?
- Est-ce que la politique de votre entreprise spécifie de ne jamais partager de nom d'utilisateur ni de mot de passe permettant d'accéder aux systèmes de paiement ?
- Le double contrôle (ou approbation à deux niveaux) est-il a-t-il été envisagé et appliqué pour chaque transaction ?



# Checklist : Equipe de traitement des paiements – 1/2

Il est important d'adopter un état d'esprit de sensibilisation et d'action dans les services de votre entreprise qui pourraient être vulnérables. La checklist ci-dessous a été créée pour accompagner les collaborateurs responsables des paiements dans le but d'entretenir une culture de sensibilisation à la fraude.

- Demandez-vous si la demande est inhabituelle ou hors contexte? A-t-elle du sens ?** Tout e-mail relatif à des paiements ou à des comptes bancaires qui crée un sentiment d'urgence ou qui justifie l'absence d'option de contre-appel doit être traité comme extrêmement suspect. Si vous n'attendez pas la communication et/ou si vous **ne reconnaissez pas l'expéditeur, ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes.**
- Vérifiez que l'adresse e-mail est légitime** Si le nom de l'expéditeur de l'e-mail vous est familier (quelqu'un avec qui vous correspondez régulièrement), assurez-vous que l'adresse e-mail correspond bien. Les fraudeurs se font passer pour des personnes de confiance. S'il s'agit d'un collègue, l'adresse e-mail doit être enregistrée dans l'annuaire de l'entreprise (si vous en avez un).  
  
Vérifiez également que le nom de domaine est correctement orthographié. Souvent, les fraudeurs créent de faux domaines qui ressemblent de près aux vrais, mais ils modifient une lettre ou deux pour que les destinataires ne le remarquent pas. Par exemple, J@**rn**business.com au lieu de J@**m**business.com. Sachez que le nom affiché peut masquer l'adresse e-mail réelle de l'expéditeur.
- En cas de doute, interrogez-vous sur le paiement, même si la demande vient d'un membre de la direction.** Les fraudeurs savent que vous êtes plus susceptible d'agir lorsque les instructions sont données par un cadre supérieur. Par conséquent, ne vous fiez pas aux instructions de paiement reçues par e-mail, même si elles proviennent d'un cadre supérieur ou d'un partenaire commercial. Les fraudeurs peuvent également utiliser des plateformes de messagerie courantes pour faciliter la fraude.



Rappelez-vous que le fraudeur a peut-être accès à la messagerie avec laquelle vous correspondez

# Checklist : Equipe de traitement des paiements – 2/2

La vérification des informations de paiement, nouvelles et modifiées, est essentielle pour limiter l'impact de la fraude et des escroqueries en matière de paiement. Bien qu'il soit important d'effectuer des contre-appels, il existe d'autres considérations pour vous assurer de réduire le risque.

## Vérifiez tous les nouveaux bénéficiaires et toutes les demandes de modification des données du compte

Vérifiez auprès de la personne à l'origine de la demande en utilisant des coordonnées connues. Dans la mesure du possible, essayez de parler à la personne responsable de la demande de modification des données. Si la demande provient d'un fournisseur, et que vous parlez avec votre contact habituel, demandez-lui de confirmer avec la personne responsable de la demande de modifications des données **par téléphone**. N'oubliez pas que le fraudeur peut avoir accès à la messagerie de cette personne, donc les instructions et les confirmations envoyées par e-mail peuvent venir du fraudeur !

Dans cette situation :

- ◆ Ne répondez pas à l'e-mail et n'utilisez pas les coordonnées contenues dans l'e-mail. Si les fraudeurs ont obtenu l'accès au compte de quelqu'un d'autre, ils modifieront probablement les coordonnées et vous pourriez finir par parler au fraudeur.
- ◆ Appelez la personne à l'origine de la demande, ne comptez pas sur son appel. Les fraudeurs savent qu'un contre appel peut faire partie du processus et peuvent donc essayer de contourner cette étape en vous contactant en premier.



**N'oubliez pas qu'une fois le paiement effectué, il n'est pas toujours possible de récupérer les fonds**

# Fraude par Intelligence Artificielle (IA) Généralive

# Fraude par IA générative

Les fraudeurs peuvent utiliser l'IA générative pour escroquer les personnes et les entreprises

Pour vous protéger, il est important que vous compreniez les différentes façons dont les fraudeurs peuvent utiliser cette technologie.

L'IA générative est un outil auquel les fraudeurs ont recours pour rendre leurs escroqueries plus sophistiquées. Cela leur permet d'usurper plus facilement l'identité de chef d'entreprises ou de personnes haut placées en clonant l'apparence et le style de communication (vidéo et audio).

## Voici quelques exemples :

- ◆ L'**usurpation vocale** peut survenir lorsqu'un fraudeur essaye de se faire passer pour le chef d'entreprise. Il demande à un employé d'effectuer un paiement « confidentiel » vers un compte d'attente où l'argent ne fait que transiter. Pensant parler à son PDG, il autorise le paiement sans autre vérification.
- ◆ Les **deepfakes** utilisent l'IA générative afin de reproduire l'apparence et la voix d'une personne. Lors d'un appel, le fraudeur peut se faire passer pour un fournisseur de l'entreprise et demander un changement des coordonnées bancaires pour un paiement urgent ou programmé. Pensant parler à son fournisseur habituel, l'employé autorise la modification sans autre vérification.



Ne présumez pas de l'authenticité d'un appel téléphonique ou vidéo. Soyez particulièrement vigilant si l'individu demande des informations sensibles, souhaite effectuer un paiement vers un nouveau bénéficiaire ou formule des demandes urgentes.

Assurez-vous de disposer d'une procédure de sécurité claire concernant tous paiements nouveaux ou modifiés. Ces procédures ne doivent pas être contournées, quel que soit le degré de « confiance » qu'un employé a pour le bénéficiaire.



## Qu'est-ce que l'IA générative ?

- ◆ L'intelligence artificielle (IA) est une technologie qui permet aux ordinateurs de réaliser des tâches complexes et d'interagir avec des êtres humains. Ces outils d'IA peuvent également prendre des décisions en analysant de grandes quantités de données et s'appuyant sur des modèles avancés.
- ◆ Ces décisions s'affinent à mesure que l'outil d'IA recueille davantage de données. Avec suffisamment de données, un outil d'IA peut prendre des décisions semblables à celles d'un humain.
- ◆ L'IA générative repose sur une technologie similaire pour générer du contenu. Il peut s'agir de texte, d'images, de fichiers audio ou encore de vidéos.

# Comment vous protéger de ces menaces ?

L'IA générative améliore la capacité des fraudeurs à tromper leurs victimes. Cependant, de nombreux contrôles existants restent efficaces pour atténuer ce risque. Certains contrôles clés sont répertoriés ci-dessous.

## Maintenir les contrôles habituels en matière de fraude

- ◆ Méfiez-vous des e-mails, appels téléphoniques et vidéos qui vous demandent d'agir rapidement. Ceci est souvent révélateur d'une escroquerie.
- ◆ Redoublez d'attention en cas de demandes d'informations personnelles, financières ou relatives à un compte. HSBC ne vous demandera jamais ces informations.
- ◆ Veillez, dans la mesure du possible, à ne suivre que les instructions de paiement reçues depuis les canaux de communication approuvés par l'entreprise. Les fraudeurs doivent souvent contacter leurs victimes via des canaux de communication ouverts, comme des applications de messagerie, car ils ne peuvent pas accéder aux canaux approuvés par l'entreprise.
- ◆ Vérifiez et validez toujours les informations que vous recevez par e-mail ou en ligne, en particulier sur les forums ou les sites Web open source. En cas de doute, consultez un responsable hiérarchique ou un collaborateur HSBC officiel.

## Codes de sécurité journaliers

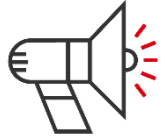
Les codes de sécurité journaliers sont des codes uniques à durée limitée, générés chaque jour et distribués au personnel autorisé. Ces codes peuvent être utilisés pour authentifier les communications et les transactions, ce qui ajoute un niveau de sécurité difficile à reproduire pour les fraudeurs. Voici comment les mettre en œuvre efficacement :

- ◆ **Codes journaliers uniques** : générez chaque jour un code unique, à utiliser par les collaborateurs.
- ◆ **Distribution sécurisée** : distribuez ces codes par le biais de canaux sécurisés comme des e-mails chiffrés ou via des plateformes internes sécurisées. Ne partagez aucun code avec des personnes extérieures à l'organisation.
- ◆ **Processus de vérification** : Exigez que le code journalier soit présenté lors de transactions sensibles, de communications importantes ou de toute situation où la vérification d'identité s'avère primordiale.

## Maintenir les contrôles habituels en matière de fraude

- ◆ **Supervision humaine** : conservez un niveau de supervision humaine pour l'approbation des transactions importantes ou inhabituelles. Agir en personne n'est pas toujours possible, mais dans le cadre de transactions importantes, cela représente un contrôle clé.
- ◆ **Sensibilisation aux deepfakes** : informez les collaborateurs des risques engendrés par les deepfakes, et de la manière dont ceux-ci peuvent être utilisés dans les procédés frauduleux.
- ◆ **Sensibilisation au phishing** : assurez une formation continue pour aider les collaborateurs à identifier les tentatives de phishing et à y réagir de manière appropriée, car celles-ci constituent souvent des signes avant-coureurs d'attaques plus sophistiquées.

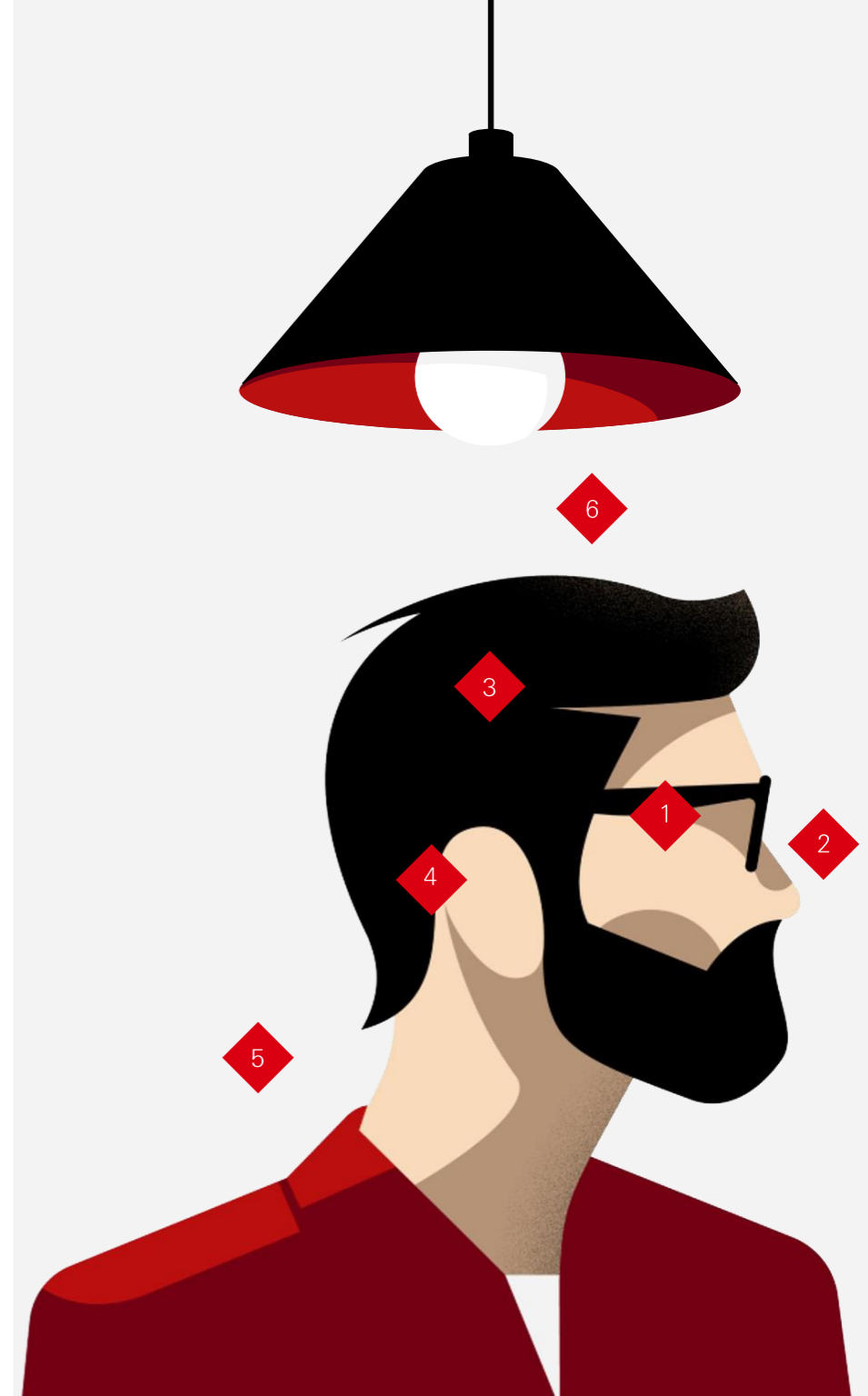
# Repérer un deepfake : conseils complémentaires



L'innovation constante dans le domaine de l'IA peut amener à penser que les deepfakes deviendront un jour presque impossibles à distinguer de la réalité. Bien que ces conseils puissent vous aider à détecter les attaques moins sophistiquées, des contrôles supplémentaires doivent être envisagés.

**À RETENIR :** Même si l'interlocuteur ressemble à quelqu'un de votre entreprise, restez vigilant si la demande est inhabituelle. Il est toujours pertinent de procéder à des vérifications adéquates, notamment en contactant directement la personne concernée par les canaux habituels, pour l'approbation des transactions importantes ou inhabituelles.

- 1 Les lunettes peuvent sembler étranges, présentant un reflet inhabituel ou même disparaître.
- 2 Les contours du visage peuvent sembler étrange ou bouger de manière anormale.
- 3 La peau ou les cheveux de la personne peuvent sembler flous.
- 4 Il se peut que le son ne soit pas synchronisé avec la voix. Soyez attentif aux changements de tonalité et de volume.
- 5 L'arrière-plan peut ne pas correspondre au contexte de l'appel, affichant des reflets étranges ou anormaux.
- 6 L'éclairage peut sembler étrange. Des ombres peuvent apparaître.

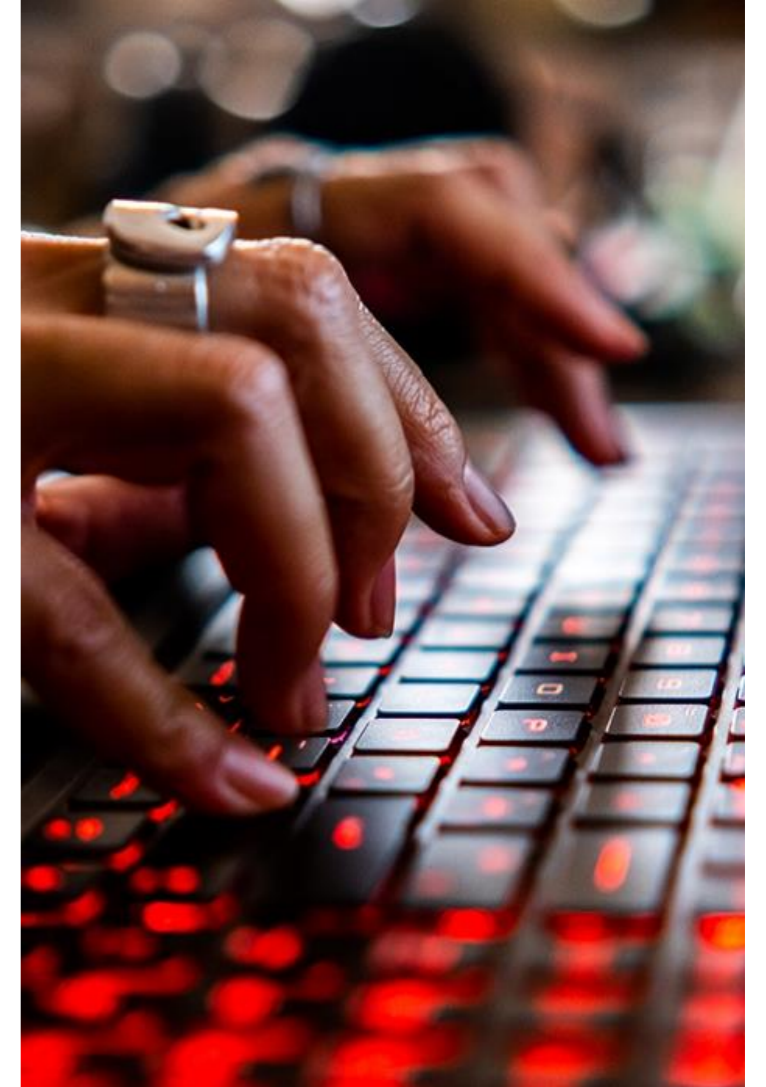


# Que faire si vous êtes victime d'une fraude

# Si vous êtes victime d'une fraude

Agissez immédiatement pour réduire au minimum les dommages résultant de la fraude et augmenter les chances de retour de fonds.

- ◆ **Arrêtez toute communication** avec l'escroc.
- ◆ **Prévenez toutes les personnes concernées** (employés, clients et institutions financières). Il est extrêmement important de prendre contact avec la banque afin de demander un retour de fonds dès que possible. Les fonds se déplacent très rapidement et il peut être très difficile de récupérer des fonds une fois qu'ils ont été envoyés.
- ◆ **Signalez la fraude** aux autorités compétentes.
- ◆ **Vérifiez vos états financiers** pour identifier toute transaction non autorisée ou toute activité suspecte.
- ◆ **Conservez tous les documents** relatifs à l'escroquerie, y compris les e-mails, les factures et toute autre correspondance.
- ◆ **Revoyez et mettez à jour vos stratégies de sécurité** et vos procédures.



# Signaler une fraude à HSBC

Si votre entreprise est victime de fraude, il est crucial d'agir rapidement !

## J'ai reçu un e-mail suspect qui ne paraît pas authentique

- ◆ Arrêtez tout. Ne répondez pas.
- ◆ Ne cliquez sur aucun lien.
- ◆ N'ouvrez aucune pièce jointe.

Signalez cet e-mail à votre administrateur système HSBCnet et transférez-le à l'adresse **hsbcnet.phishing@hsbc.com** pour que nous puissions enquêter.

## Je souhaite signaler une activité frauduleuse

Si vous avez autorisé un paiement et que vous pensez avoir été victime d'une fraude, ou si vous pensez avoir divulgué des informations de sécurité, **appelez immédiatement votre Centre d'assistance HSBCnet local.**

Il est également important d'en informer votre chargé d'affaires, votre gestionnaire de compte ou votre représentant du service client.

Par téléphone au :

- 08 10 41 42 43 (depuis la France) - (0.06 €/min)
- +48 123 993 981 (depuis l'étranger)

Ou via [support\\_hsbcnet\\_france@hsbc.com](mailto:support_hsbcnet_france@hsbc.com)

## Une personne suspecte m'a appelé en prétendant travailler pour HSBC

Une personne suspecte vous a appelé en se faisant passer pour HSBC

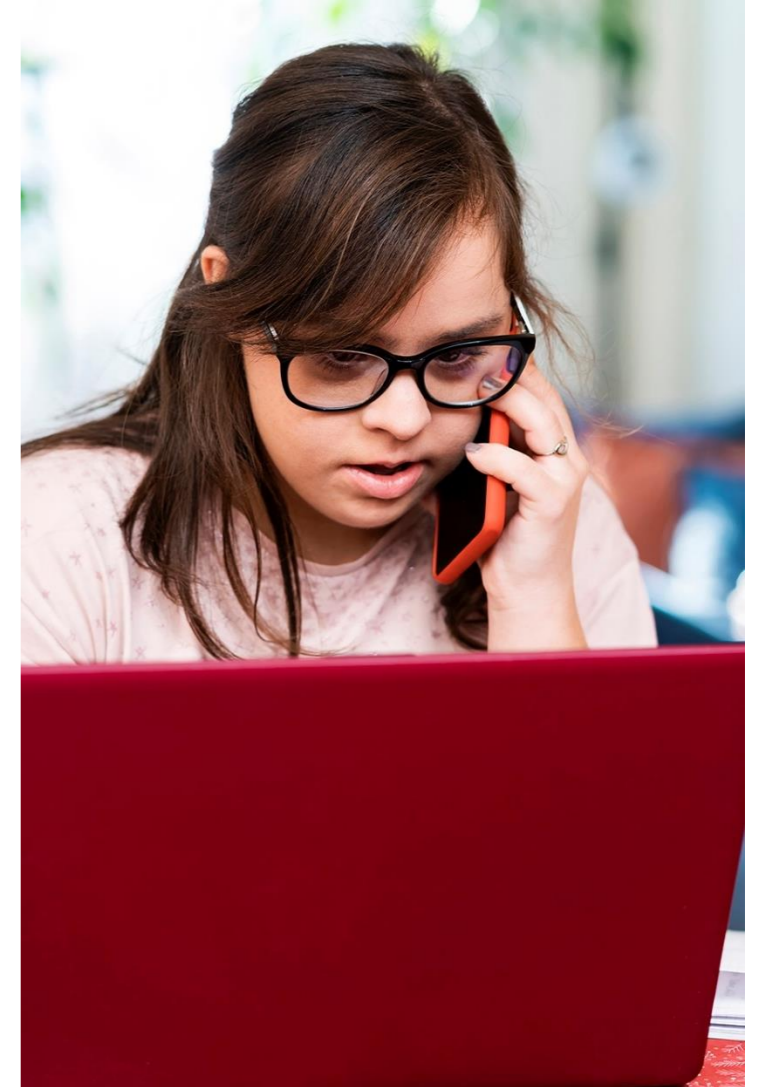
**Mettez fin à l'appel et appelez la personne à l'aide d'un numéro de téléphone vérifié pour confirmer que l'appel est authentique.**

Ne fournissez aucune information à cet interlocuteur. HSBC ne vous demandera jamais de fournir le code généré par votre dispositif de sécurité.

# Si vous êtes victime d'une cyberattaque

Envisagez les actions suivantes :

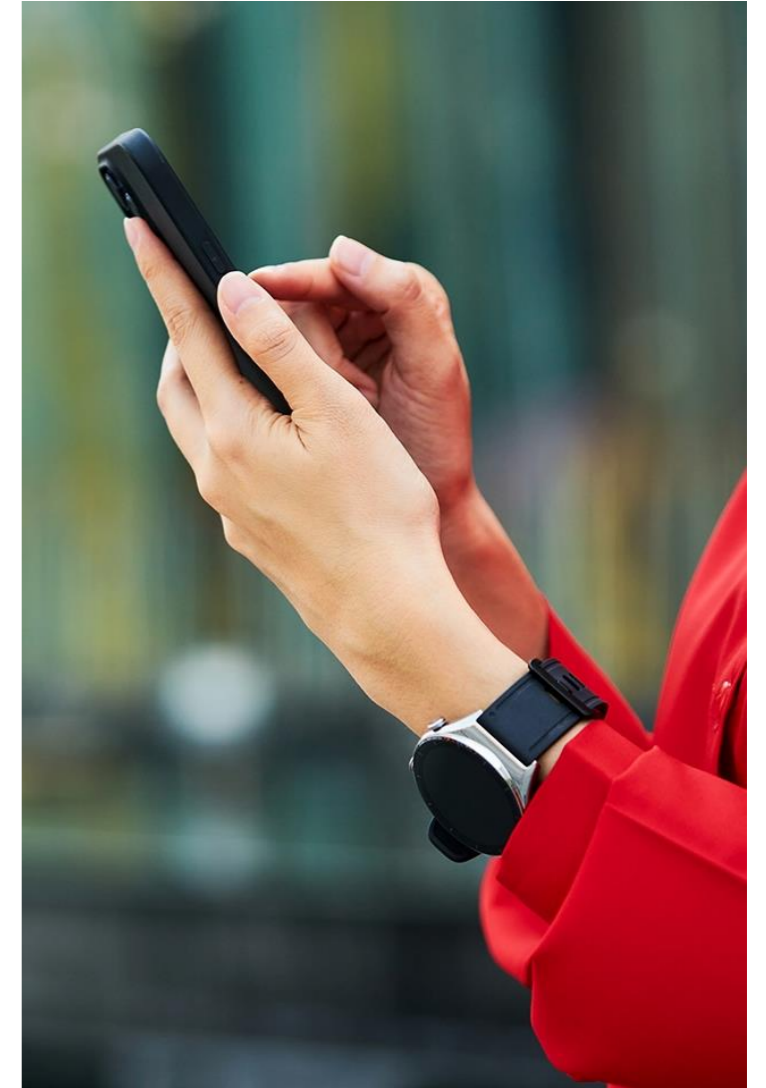
- ◆ **Déconnectez les appareils concernés** d'Internet pour empêcher la propagation de logiciels malveillants ou d'autres accès non autorisés.
- ◆ **Modifiez les mots de passe** de tous les comptes concernés, y compris les comptes de messagerie, le réseau et de tout autre compte qui a pu être compromis.
- ◆ Faites appel à un cabinet de sécurité réputé pour **réaliser une vérification complète de vos systèmes** afin d'identifier toute autre vulnérabilité ou violation.
- ◆ **Prévenez toutes les personnes concernées** comme vos employés et clients, et fournissez-leur toutes les informations nécessaires.
- ◆ **Déterminez la source** de l'attaque et prenez les mesures appropriées pour éviter qu'une attaque similaire ne se reproduise à l'avenir.
- ◆ **Saisissez les autorités réglementaires** en leur fournissant le maximum d'éléments de preuve.





## Fraude aux paiements : étapes suivantes

Scannez ce code QR pour explorer HSBC Fraud DigiRoom et accéder à des ressources utiles, notamment notre formation sur la fraude au paiement.



# Disclaimer

This document has been prepared by HSBC Continental Europe (including, where relevant, its group undertakings and affiliates, "HSBC") for the purpose of providing information solely to the addressee. This document is for the exclusive use of the person to whom it is provided by HSBC in connection with exploring HSBC business in Europe. The recipient agrees to keep confidential at all times this document and any information contained in it or made available by HSBC in connection with it. It should be read in its entirety and shall not be photocopied, reproduced, distributed or disclosed in whole or in part to any other person without the prior written consent of HSBC, nor should any other person act on it. This document is proprietary to HSBC and the recipient agrees on request to return or to destroy this document and all other materials received from HSBC relating to the information contained herein.

The information contained in this document has not been verified, approved or endorsed, or independently verified, by any independent third party. No responsibility or liability is accepted by HSBC or by any of its directors, officers, employees or agents in relation to the accuracy, completeness or sufficiency of any information contained herein or any other written or oral information made available by HSBC in connection therewith or any data which any such information generates, or for any loss whatsoever arising from or in connection with the use of, or reliance on, this document and any such liability is expressly disclaimed. Nothing in this document should be relied upon as a promise or representation as to the future. HSBC gives no undertaking, and is under no obligation, to provide the recipient with access to any additional information or to update this document or to correct any inaccuracies in it which may become apparent, and it reserves the right, without giving reasons, at any time and in any respect to amend or terminate discussions relating to the situation described herein.

This document is for information purposes only and does not constitute or form any part of any (i) invitation or inducement to engage in investment activity, (ii) offer, solicitation or invitation by HSBC or any of its directors, officers, employees or agents for the sale or purchase of any securities or other investments or (iii) commitment to underwrite, purchase or subscribe for any securities.

HSBC Continental Europe is based in Paris, is authorized and supervised by the European Central Bank (ECB), as part of the Single Supervisory Mechanism (SSM), the French Prudential Supervisory and Resolution Authority (l'Autorité de Contrôle Prudentiel et de Résolution) (ACPR) as the French National Competent Authority. It is also supervised by the French Financial Markets Authority (l'Autorité des Marchés Financiers (AMF) for the activities carried out over financial instruments or in financial markets.

© Copyright HSBC Continental Europe 2025 ALL RIGHTS RESERVED.

