PROTÉGEZ VOTRE ORGANISATION

Guide de prévention contre la fraude

ARKEA BANQUE
Entreprises & Institutionnels

CONTEXTE

25%

de PME-ETI victimes de fraude [1]

1.2 Md€

de préjudices cumulés en France [1]

Quels risques pour les organisations?

- **Pertes financières: 55K€ en moyenne [2]**
- **Perturbation organisationnelle**
- **Atteinte réputationnelle**

Dans un environnement économique de plus en plus digitalisé, les PME et ETI font face à des **menaces de fraude toujours plus sophistiquées**. L'essor des nouvelles technologies, notamment de l'intelligence artificielle et des deepfakes, rend les attaques plus difficiles à détecter et plus rapides à exécuter.

L'instantanéité des échanges, la multiplication des outils numériques et la complexité des chaînes de décision exposent **les organisations à des risques accrus**. Les fraudeurs tirent parti de ces évolutions pour viser des structures parfois moins outillées en matière de cybersécurité.

Face à cette réalité, la vigilance ne suffit plus : comprendre les mécanismes de fraude et **mettre en place des réflexes de prévention adaptés** devient essentiel pour **protéger l'activité, les collaborateurs et la réputation de l'entreprise.**

[1] source : Observatoire de la sécurité des moyens de paiements 2023
[2] source : Enquête 2024 publiée par l'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG) et Memo Bank

SOMMAIRE

LES DIFFÉRENTS TYPES DE FRAUDES

LA FRAUDE AU PRÉSIDENT

Le fraudeur usurpe l'identité d'un des dirigeants de l'entreprise pour **obtenir d'un collaborateur des informations stratégiques** ou l'émission d'un virement **urgent et confidentiel**, en prétextant une acquisition, la validation d'un contrat ou encore le règlement d'une dette.

Dans certains cas, si la tentative échoue, le fraudeur pourra retenter sa chance en se faisant passer pour la police.

CE QUI DOIT VOUS ALERTER

- L'interlocuteur fait preuve d'autorité, d'assurance, de flatterie et/ou d'intimidation.
- Le virement demandé est inhabituel et/ou à destination de l'étranger.
- La demande est urgente et intervient tardivement dans la journée ou la veille d'un jour de congés.
- La demande déroge aux procédures en place dans l'entreprise.
- La demande est hautement confidentielle.

LA FRAUDE AUX FAUSSES COORDONNÉES BANCAIRES

Le fraudeur **simule le changement de coordonnées bancaires** d'un fournisseur habituel de votre entreprise. Il utilise l'ensemble des canaux à disposition : e-mail, fax, messagerie instantanée (type WhatsApp) ou téléphone.

Ce dernier est très bien renseigné. Il utilise **la charte graphique** de votre fournisseur dans ses courriers et e-mails, afin de vous demander d'utiliser un nouvel IBAN pour effectuer les paiements courants. Pour justifier cette demande, le fraudeur **prétexte un changement de banque ou la mise en place d'un contrat d'affacturage.**

CE QUI DOIT VOUS ALERTER

- Le demandeur n'est pas l'interlocuteur habituel de la société.
- Les coordonnées bancaires fournies peuvent être à l'étranger alors que le fournisseur n'y est pas domicilié.
- Le numéro de téléphone, de fax ou l'adresse e-mail ne correspondent pas avec les coordonnées habituelles de la société.
- L'éventuelle facture a un objet peu explicite.

LA FRAUDE AU FAUX CONSEILLER BANCAIRE

Pourtant méconnue, **l'usurpation d'un tiers de confiance** comme la banque fait partie des cas fréquents de fraude.

Cette fraude peut entraîner des conséquences importantes au sein des organisations. Le fraudeur va prendre contact avec la comptabilité, la direction financière voire le dirigeant en prétextant :

- **Une activité inhabituelle sur les comptes**
- **Une opération suspecte**
- **Une mise à jour**
- **Un incident**

Dans un contexte de climat de confiance préétabli avec la banque, le fraudeur va réussir à manipuler son interlocuteur, sous couvert de l'urgence de la situation, pour que ce dernier:

- lui communique ses identifiants de connexion, pour ensuite les modifier,

ou

- lui donne accès à son système d'information, avec les conséquences que cela implique.

CE QUI DOIT VOUS ALERTER

- Votre interlocuteur vous demande vos identifiants et mots de passe. Jamais votre banque ne vous demandera ces éléments. Ils sont personnels et confidentiels.
- Le conseiller fraudeur vous met la pression et insiste sur l'urgence de la situation.
- Le conseiller fraudeur prétexte une mise à jour et vous adresse un lien cliquable .

LA FRAUDE AU FAUX TECHNICIEN

Le fraudeur usurpe l'identité d'un technicien informatique (de la banque, d'un éditeur de logiciel par exemple) pour effectuer de faux tests. Son objectif est de **soutirer des identifiants de connexion ou de provoquer des virements frauduleux.** Il peut également procéder à l'installation de logiciels malveillants.

Le fraudeur, s'il a réussi à obtenir les identifiants et mots de passe, peut également réaliser lui-même des opérations.

CE QUI DOIT VOUS ALERTER

- Vous n'avez pas sollicité d'aide informatique.
- L'interlocuteur demande à prendre la main sur votre poste.
- Un technicien qui vous demande de cliquer sur un lien envoyé par e-mail. Jamais un correctif n'est adressé dans un lien.

LA FRAUDE AU FAUX SALARIÉ

En protégeant vos salariés, vous protégez votre organisation

Le fraudeur usurpe l'identité d'un salarié pour contacter son employeur afin de demander un **changement de coordonnées bancaires.** En modifiant l'IBAN, le fraudeur s'assure que le montant du salaire est viré sur un compte qu'il contrôle, ce qui lui permet de retirer rapidement les fonds avant que la fraude ne soit détectée.

Il est donc primordial de réaliser systématiquement des contre-appels en utilisant les coordonnées usuelles pour valider la demande de changement d'IBAN.

CE QUI DOIT VOUS ALERTER

- Demandes de changement de coordonnées bancaires inhabituelles
- Incohérences dans les informations fournies
- Pression pour agir rapidement

D'AUTRES TYPES DE FRAUDES

Les nouvelles technologies ouvrent de nouvelles possibilités de fraudes de plus en plus difficiles à détecter.

MAIL-PHISHING

Vous recevez un e-mail, dans lequel on vous demande de « mettre à jour » ou de « confirmer suite à un incident technique » des données, notamment bancaires. Cette demande peut transiter par une invitation à se connecter en ligne par le biais d'un lien hypertexte sur un site falsifié ou un formulaire de saisie copie « conforme » du site original.

MALWARE, SPYWARE, RANSOMWARE

Un logiciel malveillant s'installe à l'insu de l'utilisateur sur un ordinateur non protégé (ou mal protégé), lors de l'ouverture d'un e-mail frauduleux ou par téléchargement lors de la visite d'un site web. Ce virus permet au fraudeur d'avoir connaissance de (presque) tout ce qui se passe sur l'ordinateur contaminé et de prendre en otage les données dans le cas d'un ransomware.

MISE À JOUR DE PROTOCOLE EBICS

Sous le prétexte d'une mise à jour du paramétrage des nouveaux protocoles européens, un fraudeur se faisant passer pour un informaticien parvient à vous convaincre de vous connecter sur un site dédié dont la page d'accueil affiche le logo de la société ciblée. Cette opération permet de prendre le contrôle de l'ordinateur à distance et d' émettre des virements.

Ces types de fraudes constituent un **danger croissant** car la **qualité et la précision de ces contenus** tendent à s'améliorer significativement : moins de fautes d'orthographe, une syntaxe qui progresse, des arnaques plus pertinentes, une imitation de la communication des sociétés de plus en plus crédible.

L'INTELLIGENCE ARTIFICIELLE, UNE TECHNOLOGIE AU SERVICE DES HACKERS

LE DEEPFAKE

Les"deepfake" sont une nouvelle technologie présentant un risque accru de fraude pour les organisations.
Associés à d'autres types de fraudes (faux président, faux technicien, faux salarié etc.), leur utilisation renforce la complexité de ces escroqueries et rend leur détection encore plus difficile et tardive.

Concrètement, le deepfake utilise l'intelligence artificielle et l'apprentissage automatique pour créer des contenus audio et visuels trompeurs. En combinant des images, des vidéos et des enregistrements audio existants, le deepfake permet de générer des représentations réalistes de personnes demandant l'exécution d'un virement frauduleux.

Quelques astuces pour repérer une fraude deepfake :

1. Effectuer un contre appel systématique auprès de votre interlocuteur habituel pour vérifier la demande
2. Utiliser une méthode de vérification au cours de la discussion en vérifiant son identité via des questions personnalisées
3. Utiliser des outils d'authentification

CE QUI DOIT VOUS ALERTER

- Anomalies dans les mouvements des yeux
- Incohérences dans la morphologie du corps et expression faciale non naturelle
- Problème d'éclairage et dégradation des couleurs

ARKEA BANQUE ENTREPRISES ET INSTITUTIONNELS S'ENGAGE DANS LA LUTTE CONTRE LA FRAUDE

L'ensemble des collaborateurs des collaborateurs d'Arkéa Banque EGI est **formé et sensibilisé** aux problématiques de fraudes.

Notre priorité : vous proposer des solutions pour limiter le risque de fraude

- **La solution EBICS TS** permet de faciliter et sécuriser les flux bancaires. Le protocole EBICS TS permet la signature de fichiers via un certificat électronique, avec la possibilité de mettre des droits de signatures complexes.

/!\ Il est de la responsabilité de l'entreprise de s'assurer de la fiabilité des données transmises dans le fichier communiqué à l'établissement bancaire.

- **Le service de validation d'ordres**, compatible sur l'Espace Client et sur Ebics TS, permet à l'administrateur de paramétrer les règles en matière de signatures (plafonds, habilitations, type de signature : simple ou double). Ce service permet de vous accompagner dans la lutte contre la fraude grâce aux paramétrages, à la segmentation des tâches et à une confirmation dématérialisée de l'ordre.

- **Grâce à notre partenaire SIS ID**, il est possible de payer vos fournisseurs en toute sécurité. La solution SIS ID vous permet de contrôler les coordonnées bancaires de vos fournisseurs en s'appuyant sur un réseau collaboratif de données financières sécurisées et anonymes.

Pour plus de renseignements sur ces offres, n'hésitez pas à vous rapprocher de votre responsable de clientèle.

QUELQUES BONNES PRATIQUES À ADOPTER

1. Communiquez régulièrement, auprès de vos collaborateurs, sur les risques de fraude.

2. Vérifiez l'identité de la personne qui vous contacte en contrôlant **son authenticité auprès de vos interlocuteurs habituels**. Demandez confirmation des ordres de virement reçus ou modification de coordonnées bancaires auprès de vos contacts habituels.

3. Utilisez **les coordonnées habituelles** de votre répertoire (e-mail, fax, téléphone) et ne répondez pas directement aux mails reçus.

4. Ne cliquez pas sur les liens internet contenus dans un courriel douteux.

5. Vérifiez que vous êtes bien sur un **site sécurisé** « https ».

6. Ne divulguez jamais **vos identifiants ou vos mots de passe**. Un technicien informatique de votre banque, des services de la direction générale des finances ou de tout autre organisme officiel n'aura jamais besoin de demander un mot de passe par courriel ou par téléphone.

7. Ne communiquez pas les noms et coordonnées des collaborateurs disposant de pouvoirs et de signatures sur les comptes.

8. Ne transmettez pas de **données sensibles** (solde de compte, mise à jour de données administratives, vérification des moyens de paiements, déblocage de carte).

9. Au moindre doute, **contactez votre interlocuteur habituel** au sein d'Arkéa Banque Entreprises et Institutionnels.

10. Ne dérogez pas aux process habituels et n'hésitez pas à **demander des documents justificatifs**.

NOS CONSEILS EN CAS DE FRAUDE

Contactez immédiatement votre banque
Déposez plainte

Même en cas de tentative non réussie :

- Relevez les numéros et heures d'appel du fraudeur, gardez les e-mails frauduleux, conservez les enregistrements des appels s'ils existent, demandez l'extraction de la source (en-tête) de ces e-mails et déposez plainte.
- Prévenez votre banque.

Nous vous invitons également :

- À réaliser, par vos services informatiques ou votre prestataire habituel, un audit de votre système d'information,
- À modifier régulièrement vos mots de passe.

ARKEA BANQUE
Entreprises & Institutionnels

www.arkea-banque-ei.com

AVERTISSEMENT

Le présent document est un document établi uniquement à titre d'information et de sensibilisation aux risques de fraude. Ce document ne prétend en aucun cas à l'exhaustivité. Les scenarii décrits dans ce document ne constituent pas l'ensemble des risques auxquels sont exposées les entreprises. Les méthodes et moyens de prévention des risques présentés dans ce document (i) ne suffisent pas à eux seuls à une prévention efficace de l'ensemble des risques, (ii) ne représentent pas l'ensemble des moyens pouvant être mis en place et, (iii) en tout état de cause ne remplacent pas les procédures de contrôle et de sensibilisation que chaque entreprise se doit de développer en interne. Chaque société reste responsable de l'élaboration de sa propre cartographie des risques et d'identification des risques de fraude propres à son activité, ainsi que de la mise en place de ses procédures de prévention des risques de fraude.

Société anonyme à Directoire et Conseil de surveillance, banque et courtage d'assurances
(N° ORIAS : 07 026 594) RCS BREST 378 398 911.
Siège social : Allée Louis Lichou - 29480 Le Relecq-Kerhuon.
Adresse postale : Arkea Banque E&I, Bâtiment Altair - 3 Avenue d'Alphasis - 35760 Saint Grégoire