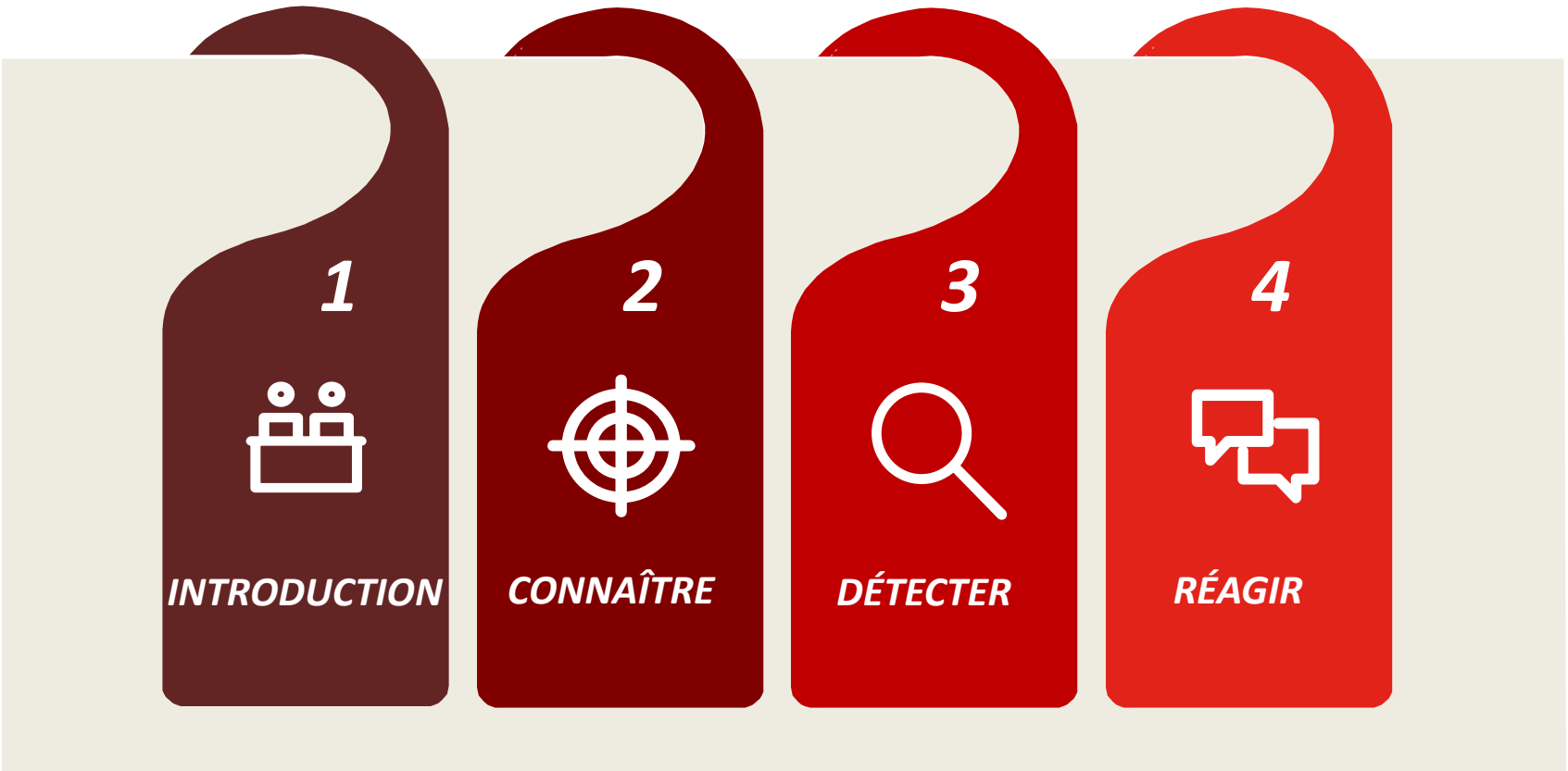

SENSIBILISATION AUX
RISQUES DE FRAUDE
AMRAE AURA 15.10.20

Intervenants

Marie-Pierre BOSSARD
Risk Manager Group
GL events

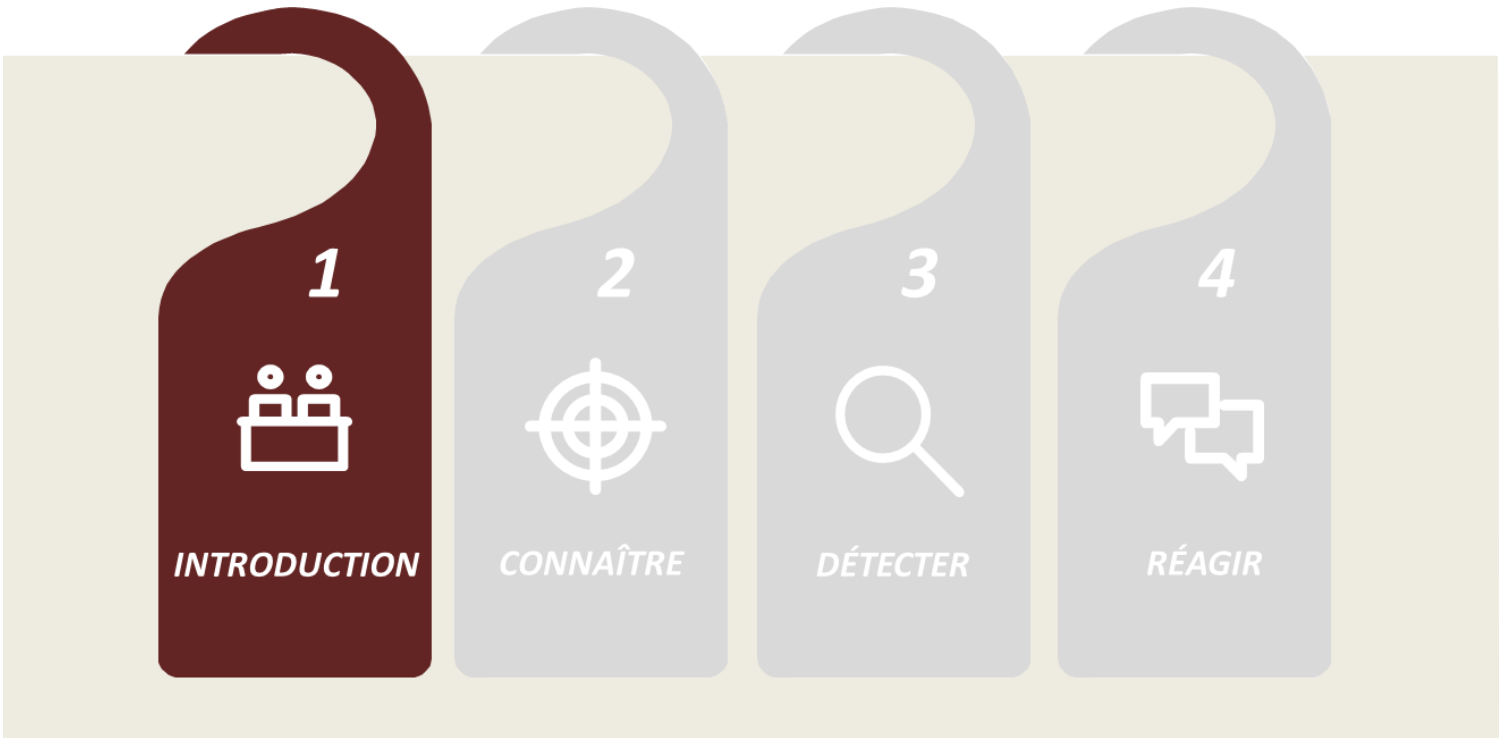
Baptiste HELBERT
CHUBB

Sommaire



Introduction

Mise en contexte et présentation des enjeux de la formation



La fraude, un sujet d'actualité


ouest france

Que recherchez-vous ?

Abonnez-vous

Réservé aux abonnés

Bretagne. Des entreprises escroquées de centaines de milliers d'euros

Six personnes comparaissent, de jeudi 13 à vendredi 15 novembre, pour association de malfaiteurs devant le tribunal correctionnel de Rennes. Elles sont suspectées d'avoir participé à un réseau qui a escroqué ou tenté d'escroquer une dizaine d'entreprises françaises, dont trois en Bretagne.


france bleu

Haute-Savoie Changer

Infos Sports Culture Vie quotidienne

Escroqueries : plusieurs entreprises de Haute-Savoie victimes d'arnaques aux faux ordres de virement

Mardi 5 novembre 2019 à 22:01 - Par Richard Vivion, France Bleu Pays de Savoie, France Bleu

Dans le Chablais (Haute-Savoie), deux entreprises viennent de perdre plusieurs milliers d'euros suite à l'arnaque dite des "faux ordres de virement" (FOVI). Le commissariat de Thonon-les-Bains lance un appel à la vigilance.


LE BERRY RÉPUBLICAIN

À LA UNE | VIE LOCALE | SPORTS | LOISIRS | ENTREPRENDRE

Faits divers

Les laiteries Triballat touchées par une cyberattaque

Publié le 05/11/2019 à 07h05

RIANS FAITS DIVERS

LIRE LE JOURNAL


Hirson

Vervins Étreux-Ménehould Épernay Sézanne Vitry-le-François

Une comptable de la mairie de Vervins suspendue pour soupçons de fraude


RTL

INFO RADIO VIDÉO PODCAST

En Direct

La curiosité est un vilain

Cybersécurité

1 min de lecture

Ticket Restaurant : la maison-mère victime d'une cyberattaque

Edenred, propriétaire de Ticket Restaurant, a subi une cyberattaque ce jeudi 21 novembre. La société qui "analyse actuellement l'étendue de l'attaque".

EDF Entreprises

Devenons l'énergie


Les Echos.fr

POLITIQUE ÉCONOMIE BOURSE MONDE TECH-MÉDIAS INDUSTRIE-SERVICES FINANCE - MARCHÉS RÉGIONS IDÉES I.A. VIDÉOS START-UP EXECUTIVES PATRIMOINE WEEK-END

Fraude 3.0 : quand l'IA imite la voix du PDG

ABONNEZ-VOUS

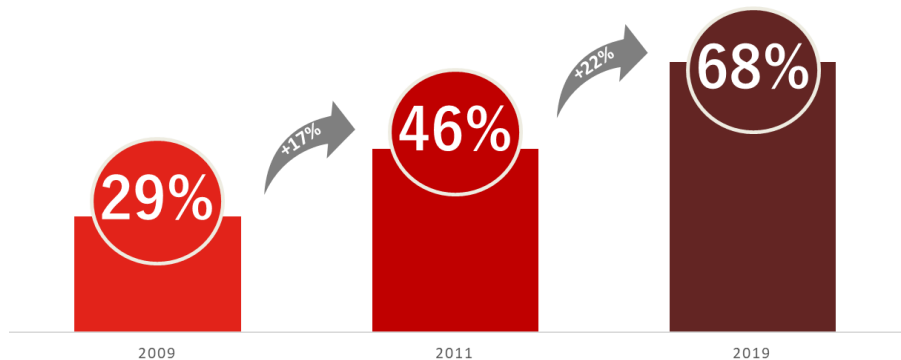
Fraude 3.0 : quand l'IA imite la voix du PDG

15/11/2019

La fraude, un danger toujours plus proche

70%

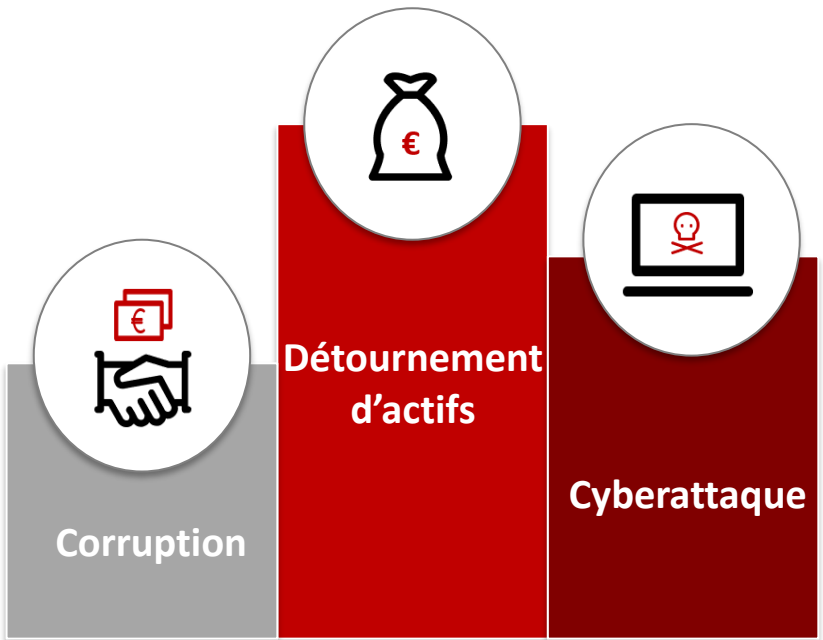
Des entreprises ont été **au moins une fois victime d'une tentative de fraude**



La fraude est un phénomène **en constante évolution**, avec une progression de **+40%** en dix ans

Source : PwC – Global Economic Crime Survey

Concrètement dans le monde



Toutes les entreprises sont touchées par la fraude, peu importe :

- La localisation
- Le secteur d'activité
- La taille

Top 3 des fraudes reportées dans le monde

Source : PwC – Global Economic Crime Survey (2016)

Concrètement chez GL events depuis le début de l'année

25 hameçonnages

3 détournements d'actifs

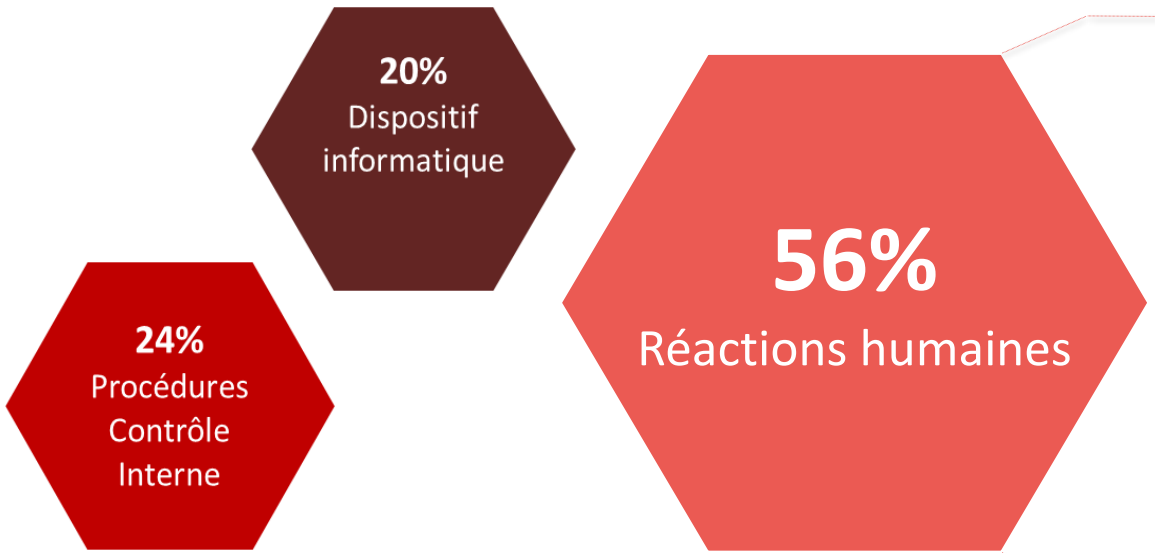
2 fraudes au président

1 tentative de fraude au faux fournisseur

Fraudes et tentatives de fraudes non-connues et/ou non-identifiées

Comment ces fraudes sont-elles détectées ?

Dispositifs ayant permis de détecter la fraude



- **Vigilance** des collaborateurs dans leur quotidien
- **Bonnes pratiques** à adopter en cas de suspicion de fraude
- **Bon sens** face à des situations inhabituelles / incohérentes

L'HUMAIN, LE MEILLEUR DISPOSITIF ANTIFRAUDE

Source : Euler Hermès (2018)

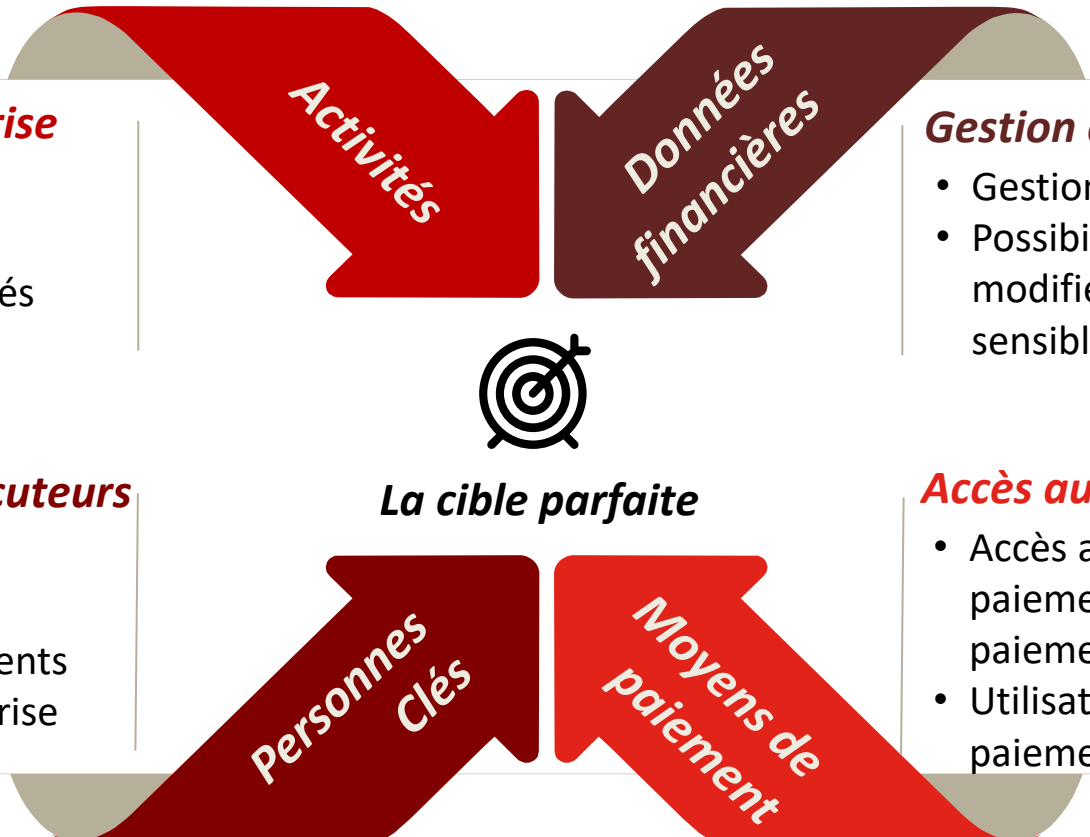
Pourquoi être sensibilisé aux risques de fraude?

Connaissance de l'entreprise

- Au cœur de l'activité de l'entreprise
- Retranscription des activités en données financières

Gestion de la donnée financière

- Gestion des comptes
- Possibilité de créer et/ou de modifier des données sensibles



Connaissance des interlocuteurs

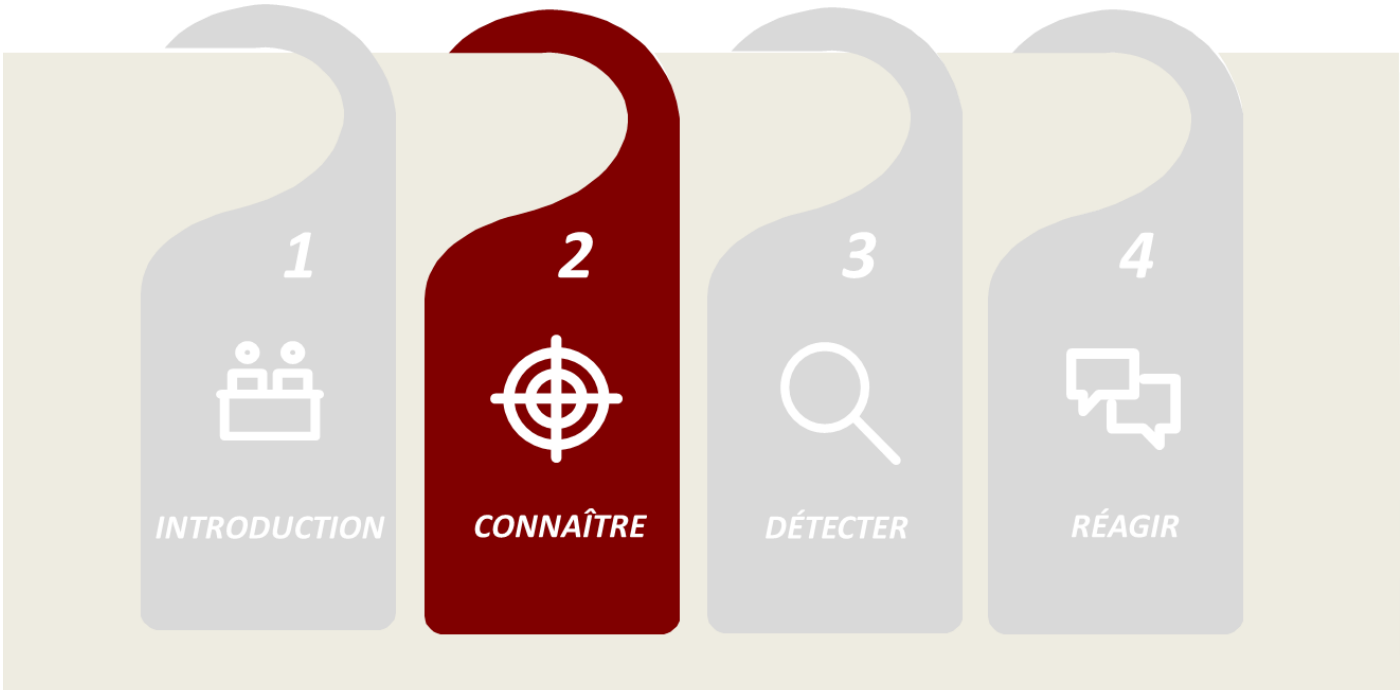
- Accès aux informations fournisseurs
- Accès aux informations clients
- Personnes clés de l'entreprise

Accès aux moyens de paiement

- Accès aux informations de paiement : batchs / lots de paiement
- Utilisation des moyens de paiement du groupe

Connaître la fraude

Comprendre la notion de fraude, son origine, ses conséquences et les différentes formes qu'elle peut prendre



Comprendre le risque de fraude et les différentes formes qu'il peut prendre

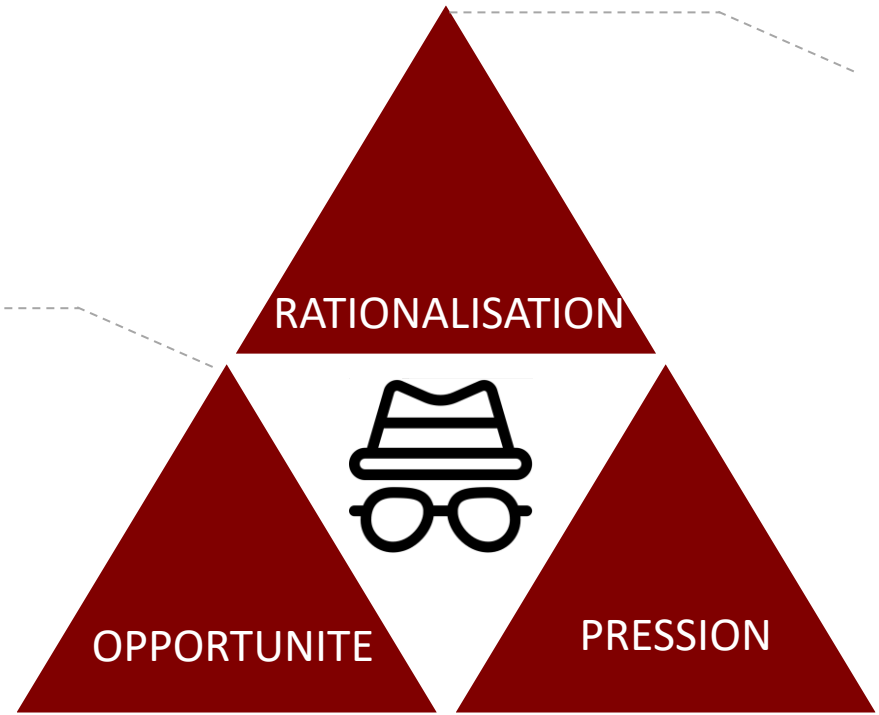
Avoir connaissance et **conscience** de l'existence de ce risque dans votre environnement de travail

La fraude, KESAKO?

*« Tout comportement, toute **dissimulation** ou toute **manipulation** d'un collaborateur ou d'un tiers qui irait volontairement à **l'encontre des valeurs de GL events**, des législations et/ou des procédures au préjudice à l'entreprise »*

Source : EY

La fraude, une combinaison de trois leviers

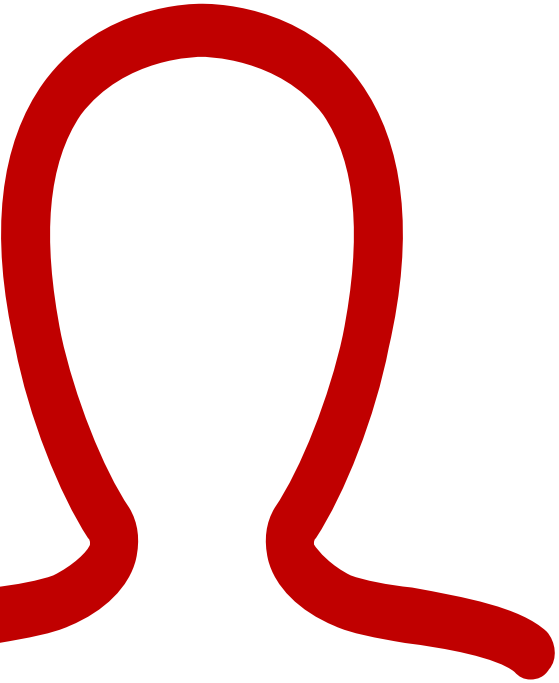


Rationalisation de l'acte frauduleux comme étant un dû

Circonstances qui donnent l'opportunité de commettre la fraude

Environnement managérial, économique, ou personnel favorisant la fraude

Le profil type du collaborateur - fraudeur



- Un **homme**
- Agé de **31 à 40 ans**
- Ayant un **diplôme universitaire**
- Occupant une **fonction Cadre**
- Avec plus de **6 ans d'ancienneté**

Apprécié par tous ses collaborateurs

Source : PwC – Global Economic Crime Survey

Les typologies de fraude

Fraude au faux fournisseur

Fraude au faux fournisseur

« Se faire passer pour un fournisseur afin de se faire remettre frauduleusement des fonds ou de la marchandise »

Informations sur :
- L'entreprise
- Les fournisseurs
- Les salariés

- Paiement
- Marchandise

RECOLTER → **CONTACTER** → **RECLAMER**

Un changement de:
- Contact
- Coordonnées bancaires
- Adresse de livraison

Exemples de fraude au faux fournisseur

ACTUALITES

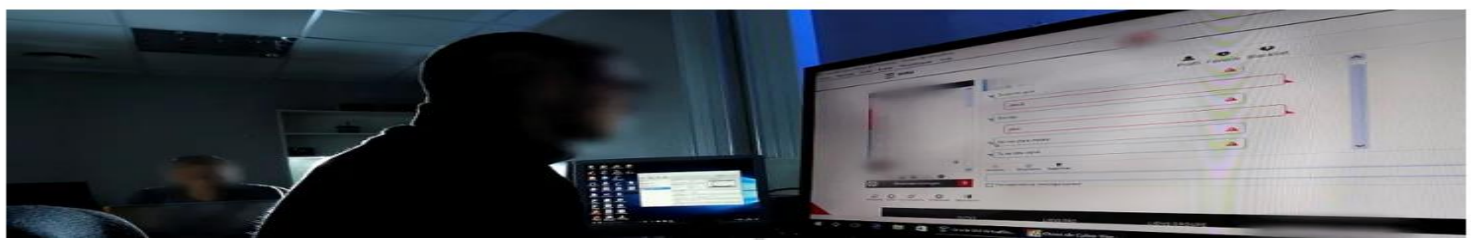
france bleu | Haute-Savoie Changer

Infos Sports Culture Vie quotidienne

Escroqueries : plusieurs entreprises de Haute-Savoie victimes d'arnaques aux faux ordres de virement

Mardi 5 novembre 2019 à 22:01 - Par Richard Vivion, France Bleu Pays de Savoie, France Bleu

Dans le Chablais (Haute-Savoie), deux entreprises viennent de perdre plusieurs milliers d'euros suite à l'arnaque dite des "faux ordres de virement" (FOVI). Le commissariat de Thonon-les-Bains lance un appel à la vigilance.



Fraude au président

Fraude au Président

« Se faire passer pour un dirigeant afin d'ordonner la réalisation d'un ou plusieurs virements bancaires en urgence »

Informations sur:
- L'entreprise
- Le président
- Les collaborateurs
- Leurs habitudes

Virement bancaire :
- Confidentiel
- Urgent

RECOLTER → **TENTER** → **RECLAMER**

Plusieurs tentatives sont faites avant de réussir à atteindre la victime

Exemples de fraude au président

ACTUALITES

Les Echos.fr — Fraude 3.0 : quand l'IA imite la voix du PDG — ABONNEZ-VOUS

POLITIQUE | ÉCONOMIE | BOURSE | MONDE | TECH-MÉDIAS | INDUSTRIE-SERVICES | FINANCE - MARCHÉS | RÉGIONS | IDÉES | I.A. | VIDÉOS | START-UP | EXECUTIVES | PATRIMOINE | WEEK-END

Fraude 3.0 : quand l'IA imite la voix du PDG

| 15/11/2019 |

Détournement d'actifs

Détournement d'Actifs

« Transfert illégal d'un bien de l'entreprise à un salarié, un tiers ou une autre entreprise »

- Faille dans le processus
- Faille de sécurité
- Défaillance de contrôle

- Actifs financiers
- Actifs non financiers

IDENTIFIER → **RATIONALISER** → **PASSER A L'ACTION**

Légitimer son acte

Source : PwC – Global Economic Crime Survey

Exemples de détournement d'actifs

ACTUALITES

Souscription

Fraude ? Cyber ? Vol ?

Différence avec un contrat Cyber:

- Frontière au niveau de la garantie "Acte de Malveillance Informatique"
- **Cyber Fraude** = contrat Fraude alors que **Cyber Criminalité** = contrat Cyber.
- un **randsomware** s'apparente à de l'extorsion et n'est pas couvert par un contrat fraude

Différence avec un vol :

- Pas de notion d'effraction dans une fraude
- Pas de schéma de tromperie dans un vol

Différence avec un acte de malveillance :

- Intention de nuire sans profit illicite

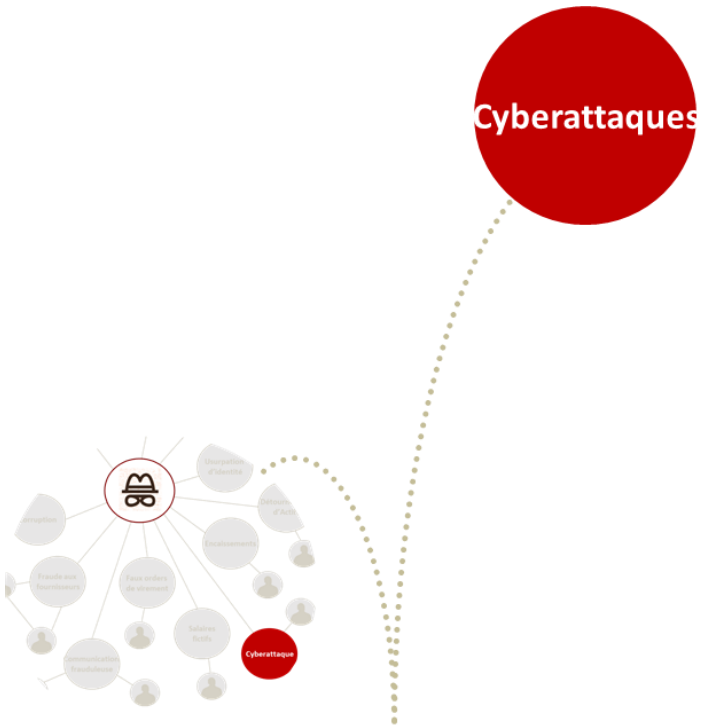
Souscription

Les garanties

Pertes Pécuniaires Directes	Pertes Pécuniaires Indirectes	Malveillance Informatique	Principales exclusions
• Somme d'argent détournée • Valeur des biens détournés	• Frais de consultant • Frais supplémentaires d'exploitation • Frais de procédure • Frais de protection d'image • Intérêts débiteurs/créditeurs • Frais de décontamination et de reconstitution de l'information	• Attaque ciblée contre la société	• Propriété Intellectuelle/Secrets commerciaux • Opérations de marché • Collusion • Fraude commise par les dirigeants de la maison mère

CHUBB

Cyberattaques



« Atteinte aux systèmes informatisés de l'entreprise dans un but malveillant »

- **Phishing** : « est une approche détournée pour pousser la victime à révéler des informations personnelles (mot de passe, codes bancaires, autres etc.**»**
- **Spear Phishing** : « variante du phishing, qui consiste à cibler une personne spécifique, ou les employés d'une entreprise spécifique »
- **Malware** : « tous les programmes ou codes malveillants qui peuvent être nocifs pour les systèmes »
- **Scam** : « il prend généralement la forme d'un e-mail dont l'objectif est d'abuser de la confiance du destinataire pour obtenir de l'argent »

Source : 1min30.com

Exemples de cyberattaques

ACTUALITES


RTL INFO RADIO VIDÉO PODCAST En Direct La curiosité est un vilain

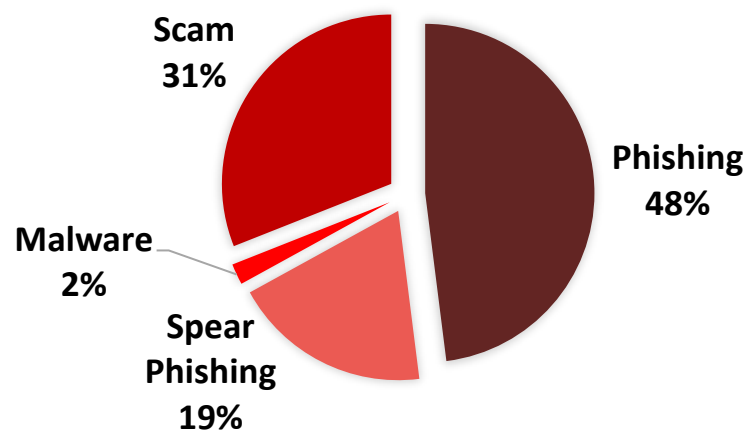
Cybersécurité 1 min de lecture

Ticket Restaurant : la maison-mère victime d'une cyberattaque

Edenred, propriétaire de Ticket Restaurant, a subi une cyberattaque ce jeudi 21 novembre. La société qui "analyse actuellement l'étendue de l'attaque".

EDF Entreprises Devenons l'énergie

En moyenne, la DSI relève 6697 tentatives de cyberattaques par mois dont:



Les impacts de la fraude

FINANCIER

- Pertes financières directes
- Cours de la bourse

IMAGE

- Réputation entachée
- Effet médiatique boule de neige
- Marque employeur

CONFIANCE

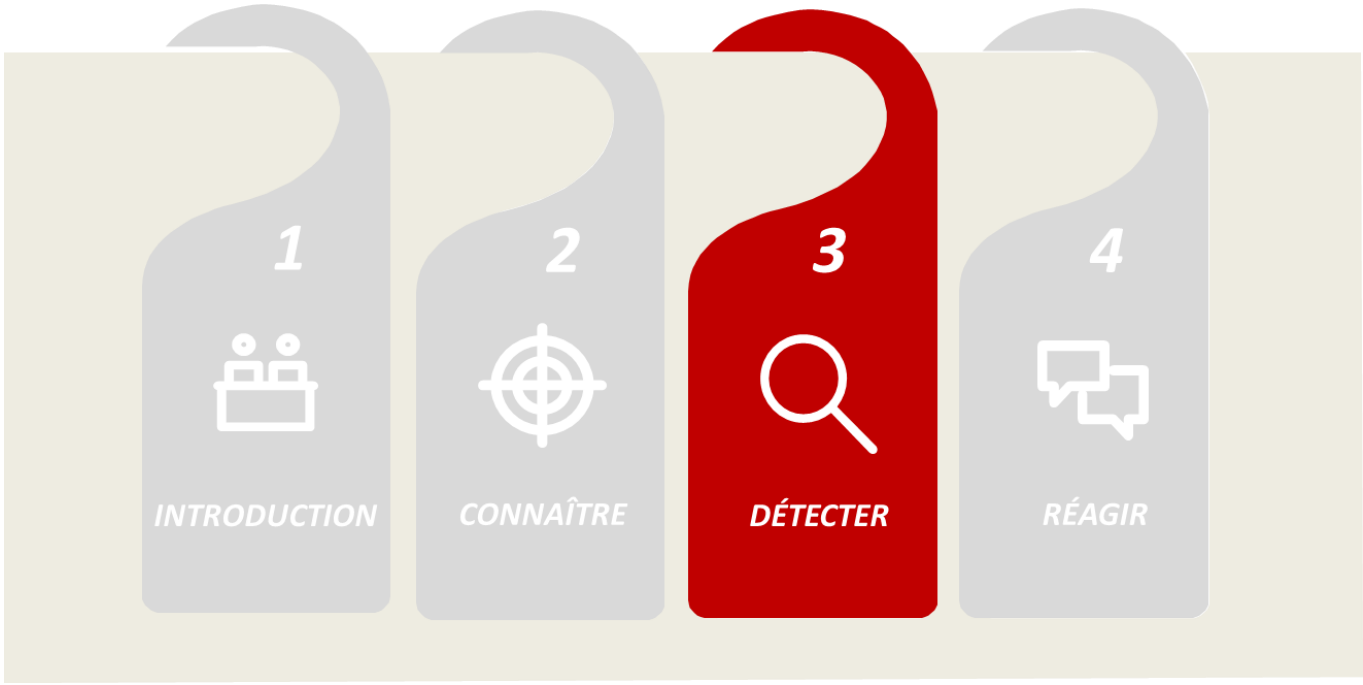
- Perte de confiance des parties prenantes , des collaborateurs et du grand public

PSYCHOLOGIQUE

- Séquelles pour la victime, l'entourage personnel et professionnel

Détecter la fraude

Savoir identifier les situations à risque et connaître la démarche à adopter en cas de suspicion de fraude ou de fraude avérée



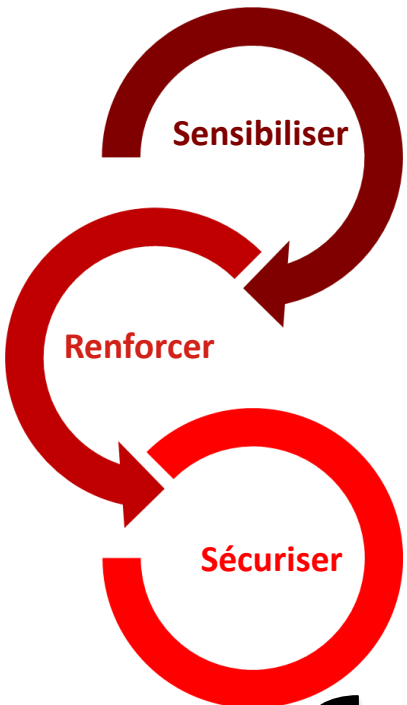
Détecter les signes et situations à risque qui doivent alerter

Devenir acteur de la préservation des actifs du Groupe

Savoir comment se comporter en cas de risque potentiel / avéré

Prévenir pour lutter contre la fraude

Sensibiliser, renforcer et sécuriser : des dispositifs déployés au sein de l'entreprise pour lutter contre la fraude



- Sensibilisation des équipes
- Formations internes
- Communication de la direction et des services supports

- Déploiement de procédures
- Renforcement du contrôle interne

- Audit
- Sécurité, sureté des systèmes d'information

L'Humain, le meilleur dispositif antifraude

Prévention

Les éléments pris en compte par les assureurs

- L'existence d'une procédure d'alerte en cas de suspicion ou détection de fraude
- La double validation des paiements
- La relation avec les partenaires bancaires (mise en place d'une procédure d'alerte en cas de virement inhabituel)
- La ségrégation des tâches, au niveau financier et gestion des stocks
- Stratégie de cash-pooling
- Procédure de contre-appel systématique en cas de demande de modification de coordonnées bancaires d'un tiers
- Sensibilisation du personnel au risque de fraude
- Le niveau de décentralisation du groupe et l'harmonisation des procédures au sein du groupe et des filiales
- L'effectif, et la présence à l'international
- L'activité (exposition au risque de détournement des stocks)
- L'existence d'un département d'audit et de contrôle interne et l'intégration dans ses missions du risque de fraude

Les enjeux

L'assureur entreprend une démarche d'auditeur pour évaluer le risque, et peut-être amené à donner des recommandations pour en améliorer la qualité

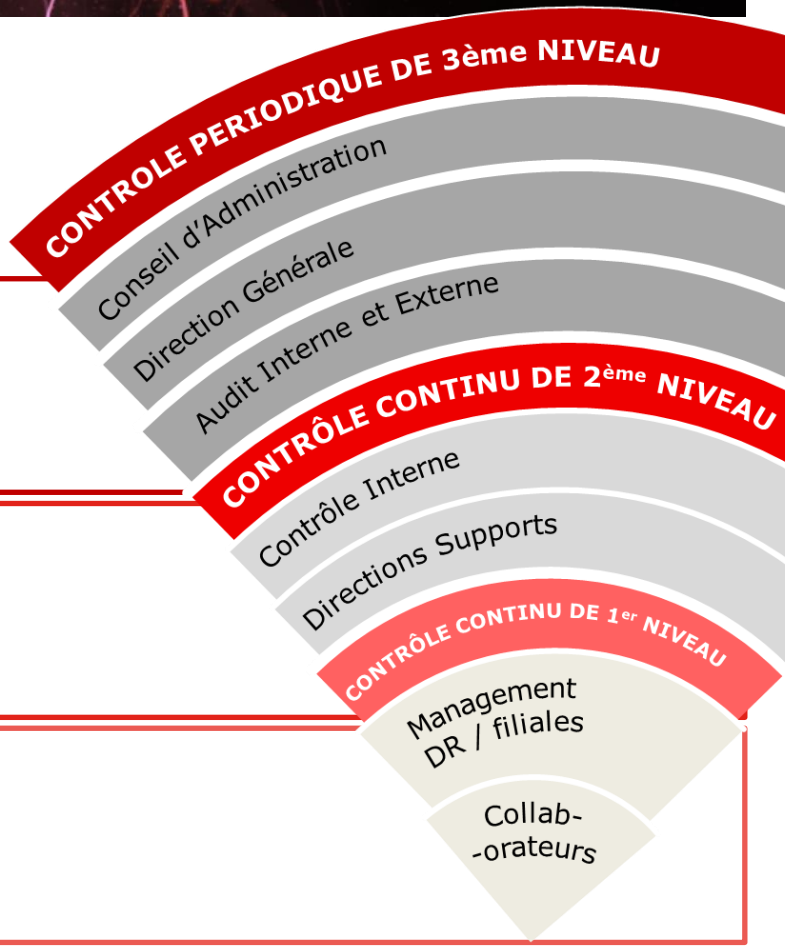
La vigilance, l'affaire de tous

Afin de garantir la maîtrise des activités et de fournir un appui efficient aux opérations, les dispositifs de contrôle interne doivent être exécutés par tous. Celui-ci peut s'établir selon **trois niveaux de vigilance**:

NIVEAU 3 Assuré par la Direction Générale qui fixe les grands principes et **l'Audit** qui évalue périodiquement le fonctionnement du dispositif et contribue à son amélioration à travers la proposition de plans d'actions.

NIVEAU 2 Assuré par les Directions Supports (contrôle de gestion, juridique …) dans leur domaine de compétence. Définissent les politiques / normes transversales. Assistent les directions dans la mise en œuvre.
Le Contrôle Interne coordonne les actions de maîtrise des activités entre les fonctions.

NIVEAU 1 Assuré par chaque collaborateur et par sa hiérarchie dans l'exercice quotidien des activités. Le management est sponsor du dispositif.
Il est responsable du bon fonctionnement du dispositif dans son périmètre.



Identifier les situations à risque

Tout changement **Situation à risque**

IDENTIFICATION

- Contact
- Adresse de livraison
- Coordonnées bancaires

MODE OPERATOIRE

- Demande inhabituelle
- Demande illogique
- Demande contraire aux procédures
- Interlocuteur suspect

FRAUDE

AUTRES SIGNES

- Demande confidentielle
- Caractère urgent de la demande
- Périodes propices
- Activités anormales sur mon ordinateur

FORME

- Objet de l'e-mail
- Adresse e-mail
- Expression, ton employé
- Majuscules, fautes d'orthographe, police de caractères

Période creuse **Situation à risque**

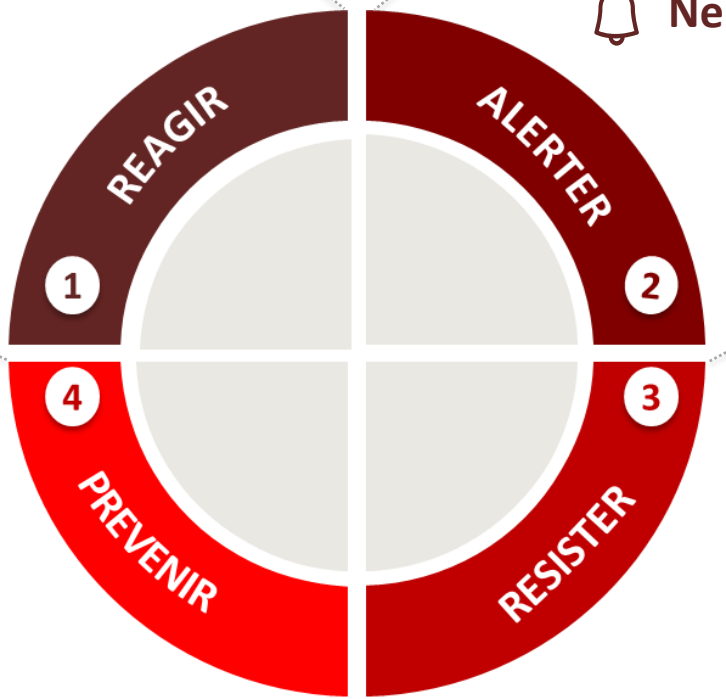
En cas de suspicion de fraude : Réagissez!

Avant toute démarche

- Vérifier avant d'exécuter toute demande
- Faire preuve de bon sens
- Effectuer un contre-appel sur le numéro habituellement utilisé

Ne pas s'isoler face à un doute

- En parler autour de vous
- Alerter son manager ou son directeur en son absence
- **WHISPLI** en cas de fraude interne



Prévenir les personnes concernées

- DSI
- Finance
- Trésorerie
- Juridique (dépôt de plainte)

Combattre la fraude

- Résister à la pression
- Suivre les instructions formulées par votre management et interlocuteur(s) privilégié(s)

Gestion du sinistre

Comment gère-t-on ?

Préalables :

- Déposer plainte
- Prendre toutes les mesures pour stopper la fraude si encore en cours

Désignation d'un consultant (varie selon la typologie du sinistre)

Missions : démontrer le schéma frauduleux et **établir le montant des pertes**

Un gestionnaire sinistre spécialisé vous accompagne dans toutes les étapes du sinistre

Paiement du montant détourné (Pertes directes)

Prise en charge des **Frais Annexes** (Pertes indirectes) :

- **Frais de consultant**
- **Frais supplémentaires d'exploitation**
- **Intérêts débiteurs**

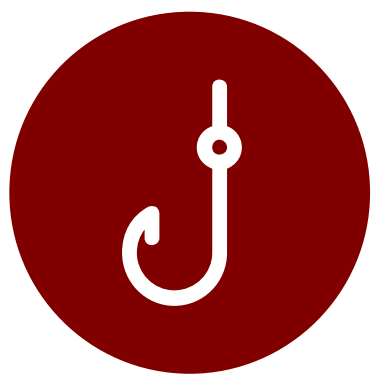
Prévenir la fraude et éviter les piratages

- Verrouiller vos ordinateurs
- Changer tous vos mots de passe régulièrement
- Ne pas divulguer vos mots de passe
- Ne pas partager vos droits d'accès
- Stocker les mots de passe intelligemment
- MiUTy78P Utiliser un mot de passe complexe

POUR EVITER TOUT PIRATAGE

Fiabiliser vos données afin d'éviter les piratages

- Ne pas transférer vos fichiers sur des plateformes publiques
- Être attentif aux exports de fichiers et envois de mails
- Ne pas ouvrir de pièce-jointe inconnue ou questionnable
- Veiller à vos données personnelles et professionnelles sur internet



En résumé

À RETENIR …

- Être vigilant
- Faire preuve de bon sens
- Ne pas se précipiter
- Ne pas s’isoler
- En parler

Penser à former ses équipes