

Bienvenue !

Le webinar va bientôt commencer

Cybersécurité et lutte contre la fraude

Phishing, ingénierie sociale, ransomware...
quelles mesures pour sensibiliser et accompagner les entreprises

Rappel des bonnes pratiques pour la tenue des réunions à distance



Coupez votre micro (sur votre ordinateur et/ou téléphone) pour éviter les bruits parasites



Utilisez la fonction « Chat » pendant la session pour partager vos remarques et poser vos questions. Elles seront ensuite reprises par le modérateur et transmises aux intervenants



En fin de présentation, lorsque la session questions/réponses sera ouverte, vous pourrez rouvrir vos micros. Annoncez votre prénom et nom lorsque vous intervenez

Présentation des intervenants



Ilker YILDIZ
Consultant Senior cash
management & flux
AZZANA CONSULTING



Pauline MENDIELA
Consultante Senior
Chef de projet Risques IT
99 ADVISORY



Nadia SAHTOUT
Team Manager – Moyens de paiement
AZZANA CONSULTING



Johanne ULLOA
Director Solutions Consulting
LEXISNEXIS RISK SOLUTIONS



Bertrand PINEAU
Conseil & Veille e/m-commerce,
logistique, paiements / monétique
FEVAD

Présentation des sociétés



Spécialiste du conseil dans les métiers liés au Transaction Banking et Corporate Treasury en France et à l'étranger, Azzana Consulting accompagne les entreprises, les banques et les acteurs de la fintech dans leurs projets de monétique, cash management et gestion de trésorerie.



Depuis plus de 10 ans, 99 Advisory accompagne les décideurs dans leurs projets de :

- Transformation
- Organisation
- Conformité

Au plus près des établissements de la Place ainsi que des régulateurs, 99 Advisory prépare ses clients à construire un écosystème plus sûr.

1. Cybersécurité et paiement : contexte et enjeux



Ilker YILDIZ
Consultant Senior cash
management & flux
AZZANA CONSULTING



Pauline MENDIELA
Consultante Senior
Chef de projet Risques IT
99 ADVISORY



Nadia SAHTOUT
Team Manager – Moyens de paiement
AZZANA CONSULTING

CYBERSÉCURITÉ ET LUTTE CONTRE LA FRAUDE AUX PAIEMENTS

Contexte et enjeux

I. DÉFINITION DE LA CYBERSÉCURITÉ ET FRAUDE AUX PAIEMENTS

- **Cybersécurité - Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI)**
- **Fraude aux moyens de paiement**

II. CONTEXTE ET ENJEUX DE LA CYBERSÉCURITÉ ET DE LA LUTTE CONTRE LA FRAUDE AUX PAIEMENTS

- **La fraude aux paiements = une véritable menace pour tous**
- **Digitalisation de la société et des moyens de paiements**
- **Crise sanitaire**
- **Contexte géopolitique**



CONTEXTE ET ENJEUX

Panorama de la menace 2021 en France

TOP 3 DES ATTAQUES INFORMATIQUES

PHISHING



LES CYBER ATTAQUES N'ARRIVENT PAS QU'AUX AUTRES...

1 PME SUR 3 
Victime d'un ransomware en 2021

34% des victimes de ransomware sont des TPE, PME et ETI

LES ENJEUX CYBER EN FRANCE

L'HUMAIN...
MAILLON VULNERABLE
DE LA CYBER SÉCURITÉ

8 PME SUR 10

ont proposé aucune formation ou sensibilisation aux risques de la cybercriminalité durant l'année 2021

DES PERTES FINANCIÈRES

27% du CA 

52%

D'attaques réussies dans secteur de la vente en ligne



Sources : ANSSI et CESIN

CONTEXTE ET ENJEUX

Quelques perspectives pour 2022

MENACES IT /
CYBER 2022

Ingénierie sociale et augmentation des surfaces d'attaques (travail sur site distant, multi-device...)



Renforcement des attaques ransomware et attaque via les chaînes de confiance



Détection et traitement des failles 0-Day sur le long terme



Espionnage et manipulation à l'approche d'événements majeurs

UNE NATION ET DES ENTREPRISES MENACÉES MAIS DE PLUS EN PLUS
CONSCIENTES ET PRÉPARÉESUn plan à 1 milliard d'euros pour
renforcer la cybersécurité

- Renforcement du cadre réglementaire
- Création d'un réseau régional de CSIRT (*computer security incident response team*) pour être au plus prêt de chaque entreprise
- Recrutement de 1100 cyber-combattants d'ici 2025
- Développement la souveraineté numérique de la France se positionnant par rapport à la concurrence internationale (licornes + création emploi)
- Diffusion d'une véritable culture de la cybersécurité dans les entreprises

La Sécurité est la préoccupation de tous

60% des DSI estiment que la sécurité sera essentielle en 2022 du fait des changements liés à la pandémie

L'automatisation est une priorité tant sur les process IT que Business des organisations

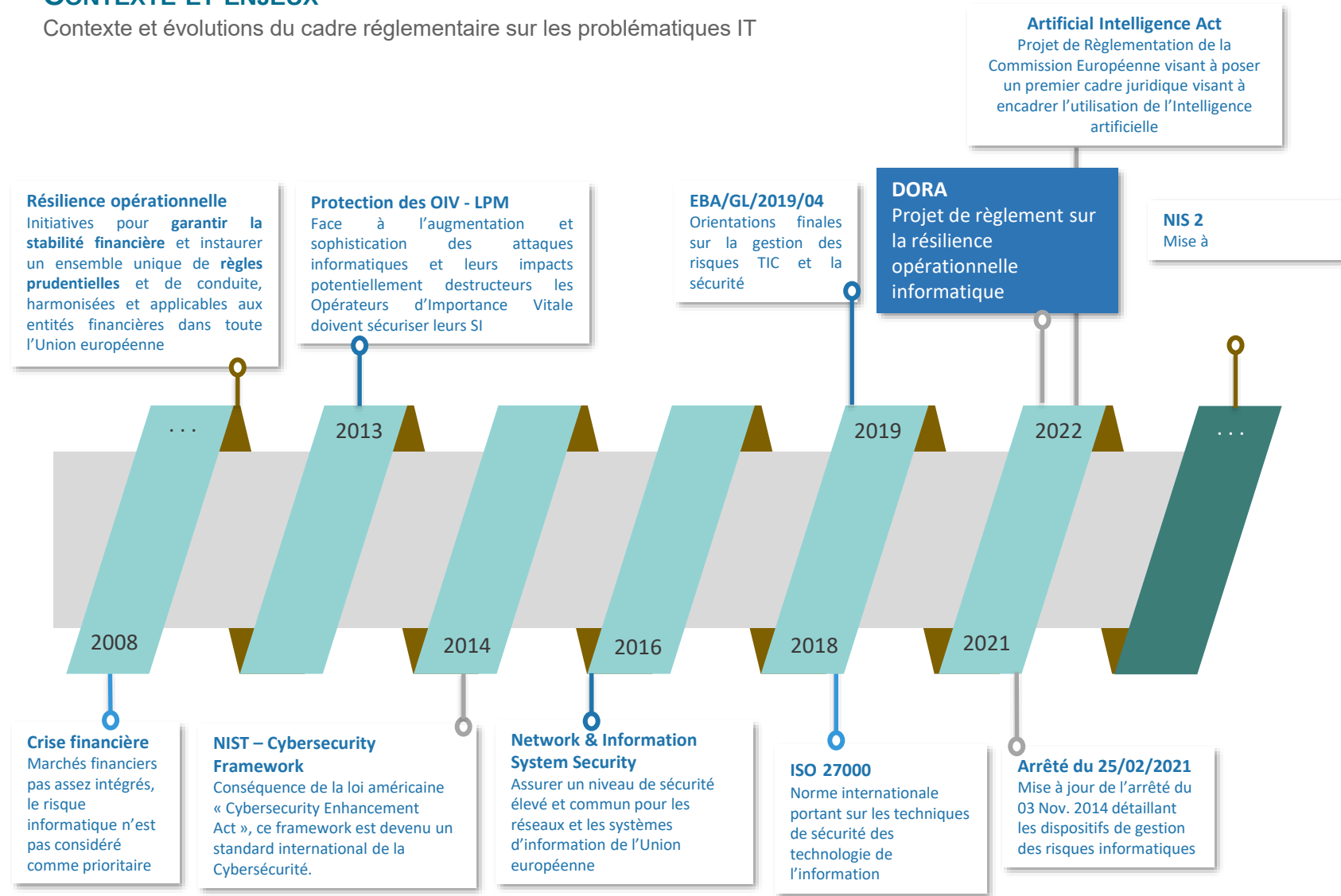
Les scans et les tests de sécurité sont perçus comme prioritaires là où ils étaient inexistants en 2020.

Le "Future of Work" sera un poste
d'investissement majeur

80% des organisations en France prévoient des changements liés à l'organisation du travail et une sur six se déclare très proactive sur le sujet

CONTEXTE ET ENJEUX

Contexte et évolutions du cadre réglementaire sur les problématiques IT



PAIEMENT ET FRAUDE

En quelques chiffres

- Modification des habitudes d'achat et de paiement des consommateurs
- Préférence pour le paiement par carte depuis la crise sanitaire
- Services de livraison et Click and Collect de plus en plus proposés par les commerçants
- Paiement sans contact privilégié dans le paiement de proximité



+ 80%

entre 2019-2020 de paiements par carte



+ 20%

pour les paiements en ligne



+ 50%

pour le paiement sans contact



- 4%

pour les retraits d'espèces



PAIEMENT ET FRAUDE

En quelques chiffres

Hausse significative de la fraude entre

2019 – 2020 :

+ **8,4%** en valeur (euros)

+ **4,2 %** en volume (nbre de transactions)



7,8 Millions de transactions

1,28 Milliards d'euros

Disparité de la fraude



538 M€



473 M€



267 M€

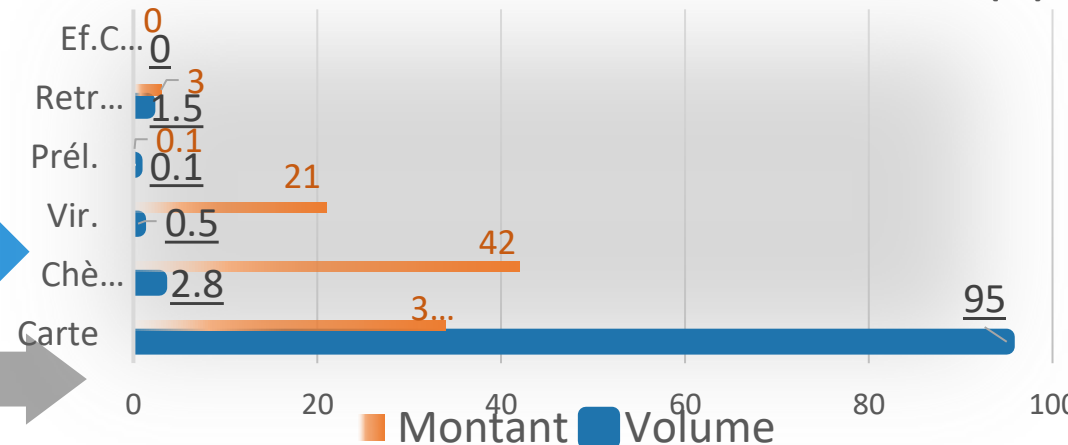


2 M€



fraudé pour

LA FRAUDE PAR MOYEN DE PAIEMENT (%)

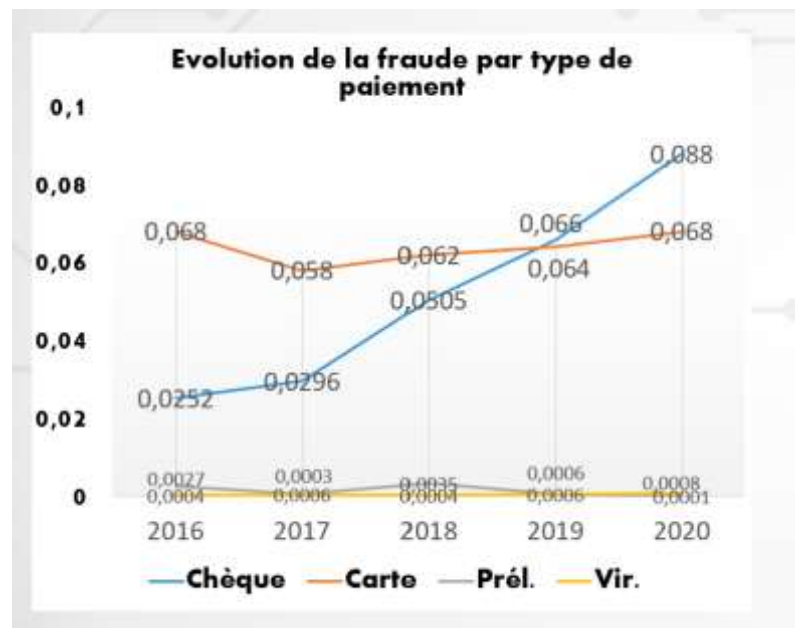


- **1 100 euros de paiement par** 
- **1 500 euros de paiement par carte** 
- **120 000 euros de paiement par virement** 
- **1 million d'euros de paiement par prélèvement** 

Les données chiffrées proviennent de la Banque de France (2020)

PAIEMENT ET FRAUDE

Tendances d'évolution



1

Hausse sensible pour le chèque

2

Maîtrise des taux de fraude sur les opérations par carte sous l'effet de l'authentification forte pour les paiements à distance

= **Équipement de 97 % des porteurs de carte**. Le taux de fraude sur les paiements à distance baisse sensiblement à 0,149 % contre 0,174 %

3

Baisse importante de la fraude au prélèvement ramenée de 11 millions à 2 millions d'euros en 2020. (- 82% en valeur par rapport à 2019)

PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques



Phishing
(hameçonnage)



Skimming



Spoofing



Fraude au président



Ransomware



Fraude à la mule



Piratage des comptes

53 % DES ENTREPRISES FRANÇAISES VICTIMES D'AU MOINS UN INCIDENT DE FRAUDE

DES DISPOSITIFS DE LUTTE CONTRE LA FRAUDE AUX PAIEMENTS



Sensibilisation et Formation interne



Le meilleur réflexe pour garder un coup d'avance sur les fraudeurs !



Dispositifs réglementaires



Outils LCLF



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques



Technique d'approche du fraudeur qui se fait passer pour un tiers de confiance (opérateur téléphonie, banque...) dans le but d'obtenir des informations sensibles (mot de passe, numéro de carte bancaire...) pour les utiliser à des fins frauduleuses. Cette technique peut se matérialiser sous la forme d'un appel téléphonique, un SMS ou un e-mail.



Bons réflexes :

Ne pas cliquer sur une pièce jointe ou un lien contenu dans un mail qui semble suspect.

Se rendre toujours sur un site sécurisé pour régler un achat. L'adresse d'un site web sécurisé doit commencer par « https ».

Ne communiquez jamais d'informations confidentielles par mail. Aucun site web fiable ne vous le demandera

Vérifiez que votre antivirus est à jour

Utilisez le filtre contre le filoutage du navigateur internet : la plupart des navigateurs existants proposent une fonctionnalité d'avertissement contre le filoutage.

Utilisez un logiciel de filtre anti-pourriel ou les fonctionnalités de classement automatique en tant que spam de votre boîte de réception : même si ces filtrages ne sont pas exhaustifs, ils permettent de réduire le nombre de ces courriels.



Le hameçonnage ou phishing



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques



Il s'agit d'une technique frauduleuse de clonage avec utilisation de faux lecteurs permettant de dupliquer les données de la piste magnétique d'une carte bancaire et potentiellement le code secret de la carte moyennant un faux clavier numérique ou une caméra.

Le skimming peut s'opérer sur un automate de retrait, un distributeur de carburant, un terminal de paiement ou sur le web (cacher leur logiciel de skimming dans les métadonnées de certaines images présentes sur des sites marchand).



Bons réflexes :

**Toujours bien cacher son code secret lorsqu'on le compose lors d'un retrait DAB ou pour régler par carte bleue n'importe où.
Ne vous laissez jamais distraire lors de l'utilisation de votre carte bancaire à n'importe quel endroit, surveillez-la attentivement.**

Vérifiez bien l'état du lecteur de carte du distributeur, Si celui-ci vous semble suspect (moins neuf que la machine ou affichant des traces de brûlure...), changez aussitôt de distributeur. En même temps, songez à avertir rapidement la banque si vous êtes sûr que la machine a été piratée.

Avoir toujours à jour les logiciels et systèmes de sécurité. Ces mises à jour peuvent aider à se protéger contre une tentative de harponnage, et contre d'autres types d'attaques grâce aux nouvelles fonctionnalités qu'elles peuvent offrir.



Skimming



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques



“
Nouvelle technique de fraude qui consiste à usurper l'identité de la banque du particulier en déguisant une communication provenant d'une source inconnue en une communication provenant d'une source connue et fiable. Un mail, un sms ou un appel téléphonique est effectué auprès de l'individu en lui faisant croire qu'il a été victime d'une escroquerie. L'objectif étant de lui demander son identifiant et mot de passe de la banque en ligne. L'escroc possède des informations personnelles comme une adresse postale pour mettre en confiance la victime. Les individus qui obtempèrent se voient détournés leur argent



Bons réflexes :

Prendre ou renouveler chaque année son abonnement à un service de filtre anti-spam.

Désignation d'une personne afférente (interne ou externe) pour la surveillance et l'administration du système d'e-mail, y compris le service de filtrage du spam. Les nouvelles menaces évoluent constamment et les adresses électroniques évoluent fréquemment en raison des changements de personnel.

Sensibiliser et former le personnel à l'usurpation d'adresse électronique et aux autres techniques utilisées par les spammers et les cybercriminels.



Spoofing



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques



“ Le fraudeur, qui s’appuie notamment sur sa connaissance de l’entreprise, se fait passer pour le président ou le dirigeant de l’entreprise pour obtenir de l’argent à travers la demande d’exécution d’un virement exceptionnel et confidentiel faite à un personnel de l’entreprise, qui malgré lui deviendra le complice lors de ce scénario.



Bons réflexes :

Rappeler à l’ensemble des collaborateurs l’importance de ne pas divulguer d’informations concernant le fonctionnement de l’entreprise sur les réseaux sociaux privés et professionnels.

Informez le personnel et les nouveaux arrivants, stagiaires, sur cette technique d’escroquerie.

Instaurer des procédures de vérifications et de signatures multiples pour les paiements internationaux.

Accentuer la vigilance sur les périodes de congés scolaires, les jours fériés, les vendredis soir et les week-ends.



La fraude au président



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques



“ Cette technique de fraude consiste à encaisser pour le compte d’une personne tierce appelée « Mule », complice ou dupée, de faux chèques ou des chèques falsifiés. Cette personne tierce qui encaisse le chèque a soit été attirée par l’appât du gain, en postant à une annonce sur internet promettant de toucher une commission sur les chèques encaissés, soit victime d’un chantage affectif, le fraudeur prétextant des difficultés financières pour demander à la personne tierce de l’aider.

Le fraudeur demande ensuite à la personne qui a encaissé les chèques de transférer cet argent sur le compte du fraudeur ou de lui restituer les fonds en espèces.



Bons réflexes :

Il est impératif pour éviter ce type de fraude d’être catégorique dans son refus d’encaisser des chèques pour le compte d’autrui. En plus d’être dangereux, ceci est totalement illégal. Vous vous rendez à votre insu complice d’une fraude, dont vous vous serez très probablement piégé et en difficulté financière.



La fraude à la mule



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques

“ Cette technique de fraude consiste à encaisser pour le compte d’une personne tierce appelée « Mule », complice ou dupée, de faux chèques ou des chèques falsifiés. Cette personne tierce qui encaisse le chèque a soit été attirée par l’appât du gain, en postant à une annonce sur internet promettant de toucher une commission sur les chèques encaissés, soit victime d’un chantage affectif, le fraudeur prétextant des difficultés financières pour demander à la personne tierce de l’aider.

Le fraudeur demande ensuite à la personne qui a encaissé les chèques de transférer cet argent sur le compte du fraudeur ou de lui restituer les fonds en espèces.



Bons réflexes :

Alerter votre banque (directement par téléphone) et faire opposition sur vos moyens de paiement si ceux-ci s’avèrent perdus ou volés.

Solliciter un remboursement par votre banque en adressant un courrier en recommandé avec accusé de réception. Le délai de contestation est de 13 mois pour les opérations réalisées à l’intérieur de l’Union européenne (UE) et de 70 à 120 jours maximum pour les opérations hors UE.

Garder à disposition tous les éléments nécessaires à l’instruction de votre dossier (circonstances de l’incident par exemple).



Piratage des comptes



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques

- Réception d'appels téléphoniques de faux commerciaux vous incitant à investir dans la cryptomonnaie et vous promettant d'importants rendements.
- Orientation vers des sites internet conçus par les fraudeurs des fois utilisant google pub ou des contenus sponsorisés laissant croire l'investisseur qu'il est sur un vrai site. Le fraudeur en profite pour dérober l'identifiant et mot de passe et détourne la somme investie.



Bons réflexes :

Se méfier des offres trop alléchantes.

Toujours vérifier l'identité de la personne qui appelle



Les appels et fausses pub/Promesse de faux cadeaux



PAIEMENT ET FRAUDE

Quelques techniques de fraude et bonnes pratiques

- Faux forums et faux sites internet avec des témoignages et commentaires positifs sur des taux de rendements alléchants sur ces forums frauduleux référencés "crypto-actifs".
- Cadeaux ou réduction pour toute souscription en ligne avec des rendements alléchants pour tout investissement sur un site de cryptomonnaies. Généralement, il s'agit de faux site permettant aux fraudeurs de récupérer les sommes investies.



Bons réflexes :

Il est important de vérifier les données des plateformes grâce au site de l'AMF (Autorité des Marchés Financiers) qui certifie les plateformes. Aussi, il est important de faire attention aux offres trop alléchantes, celles-ci cachent souvent des arnaques aux utilisateurs.



Les fausses plateformes et promesse de faux cadeaux

PAIEMENT ET FRAUDE Les bonnes pratiques (1)

1

2

3

4

5

6

7

8

Conseils pour éviter les arnaques ou la fraude

LA FAILLE
HUMAINE : AU
CŒUR DE TOUTE
FRAUDE ET
CYBERATTAQUE
RÉUSSIE

Formation et sensibilisation à la politique de sécurité

Bien choisir les informations à publier sur l'entreprise et son personnel

Mise en place de procédures claires pour les fonctionnalités sensibles

Sécuriser les postes de travail

Mise à jour régulière de correctifs sécuritaires

Utilisation de mots de passe forts et différents entre applications

Utilisation de mots de passe forts et différents entre applications

Renouvellement régulier des mots de passe

PAIEMENT ET FRAUDE

Les bonnes pratiques (2)



1

2

3

4

Conseils pour éviter les arnaques ou la fraude

Sécuriser son réseau

Utilisation d'un VPN pour la connexion à distance

Formation et partage des techniques de fraude
connus

Audit et tests d'intrusion pour vérifier son SI

PAIEMENT ET FRAUDE

Les bonnes pratiques (2)

1

2

3

4

5

Conseils pratiques pour investir en cryptomonnaies selon l'AMF

Vérifier les listes noires de l'AMF avant d'investir

*pour consulter la liste
noire cliquez ici*



Passez par un prestataire enregistré auprès de
l'AMF

*pour consulter la liste
blanche cliquez ici*



Sécurisez la conservation de vos crypto-actifs

Ne perdez et ne communiquez jamais votre clé
privée

Vérifiez toujours l'exactitude d'une adresse
publique

2. Cybersécurité et paiements : les différents types de fraude en ligne



Johanne ULLOA
Director Solutions Consulting
LEXISNEXIS RISK SOLUTIONS

LEXISNEXIS® RISK SOLUTIONS FAIT PARTIE DU GROUPE RELX

RELX est spécialisé dans la production de données et d'outils d'analyse

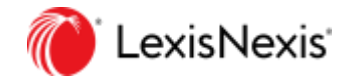
Coté à la Bourse de Londres, Amsterdam et New York, le Groupe sert des clients dans plus de 180 pays et possède des bureaux dans environ 40 pays.

Pour en savoir plus www.relx.com

RELX



Risk & Business Analytics



Legal



ELSEVIER

Scientific, Technical & Medical



Exhibitions

CONFORMITÉ EN MATIÈRE DE CRIMINALITÉ FINANCIÈRE



Customer Identification Program (CIP)



Customer Due Diligence (CDD)



Know Your Customer (KYC)



Customer and Vendor Risk Assessment



Third-Party Vetting



Watchlist Screening



Trade Compliance



Ongoing Monitoring and Financial Crime Risk Management

FRAUDE ET IDENTITÉ

LexisNexis® ThreatMetrix®

Solution leader de l'identité numérique et de l'intelligence comportementale



Leader de la gestion de la fraude et de l'identité, permettant aux clients de gérer les risques, de développer leur activité et d'améliorer l'expérience client

LexisNexis® Emailage®

Solution leader de l'évaluation des risques de fraude basée sur des informations numériques liées à l'adresse e-mail.



Analysis from The LexisNexis® Risk Solutions Cybercrime Report



July to December 2021

Balancing Risk & Reward: Highlights



Human Initiated Attack rates **grew** for the first time since **2019**



Automated Bot Attacks **increased** across eCommerce and Communications, Mobile, Media



The Mobile channel accounted for **75%** of transactions in H2 2021



Password Reset has become a new frontier for fraud, with **1 in 8** resets being attacks

Global Transaction Patterns in Numbers

Mobile Accounts for 75% of all Events, as Login Volumes Explode

- Accelerated digitalization, fuelled by the pandemic, continues across multiple demographics and geographies
- Shift to building brand loyalty after peaks of new consumer relationships during the early phases of the pandemic
- Digital payments continue to grow as consumer behavior has fundamentally changed

TRANSACTIONS PROCESSED JULY-DECEMBER 2021

35.5B Growth YOY **+44%** ▲

TRANSACTIONS BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



TRANSACTIONS BY USE CASE

		Growth YOY
	New Account Creations	516M +4% ▲
	Logins	25.7B +51% ▲
	Payments	5.9B +35% ▲

Uncovering Regional Networked Fraud Reveals the Close Links Between Financial and Telco Attacks



53,000 Events

Associated with fraudulent Digital Identities



387,000 Events

Recorded at other organisations that were associated with the Digital Identities involved in the original fraudulent events



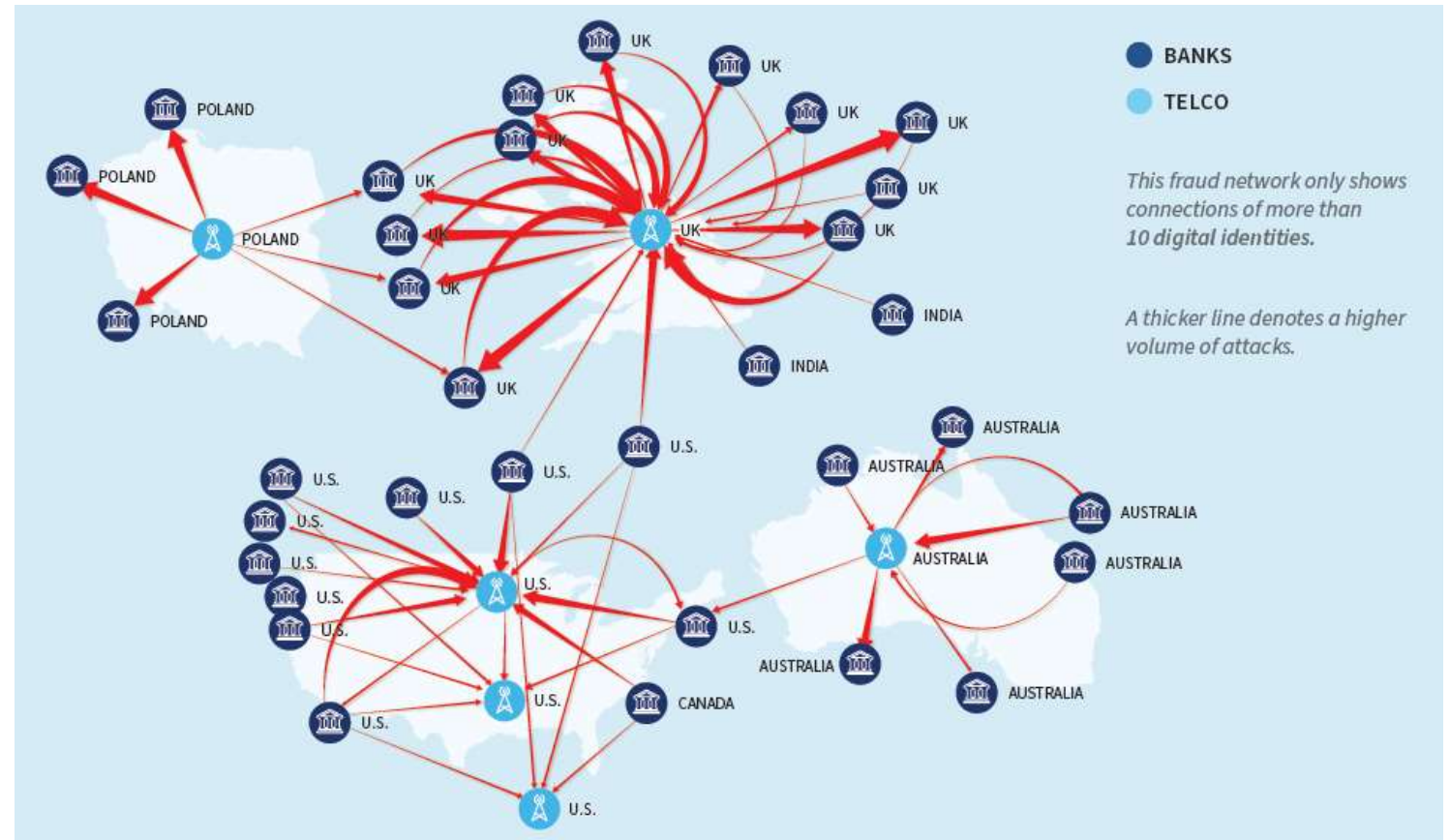
At least \$2.4M

In fraud value blocked

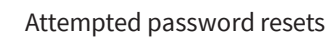


At least \$10.3M

Exposed to fraud across network



Fraud Attacks Across the Network from a Single Digital Identity





Analysis from The LexisNexis® Risk Solutions Cybercrime Report

July to December 2021

lexisnexis risk solutions cybercrime report

Tous Actualités Images Maps Shopping Plus Outils

Environ 22 300 résultats (0,48 secondes)

Conseil : Recherchez des résultats uniquement en **français**. Vous pouvez indiquer votre langue de recherche sur la page Préférences.

Annonce • <https://risk.lexisnexis.com/french>

LexisNexis Risk Solutions - Gestion des risques

Nous éclairons l'information et facilitons les décisions opérationnelles. Alliance de technologies de pointe, de données hors pair et d'outils d'analyse avancée.

<https://risk.lexisnexis.com> > research > Traduire cette page

LexisNexis® Risk Solutions Cybercrime Report

The **LexisNexis® Risk Solutions Cybercrime Report** is based on **cybercrime** attacks detected by the Digital Identity Network® from July-December 2021, during near ...

Vidéos

LexisNexis® Risk Solutions Cybercrime Report

YouTube · lexisnexisnetwork
6 avr. 2022

LexisNexis® Risk Solutions Cybercrime Report - condensed

YouTube · lexisnexisnetwork
7 avr. 2022

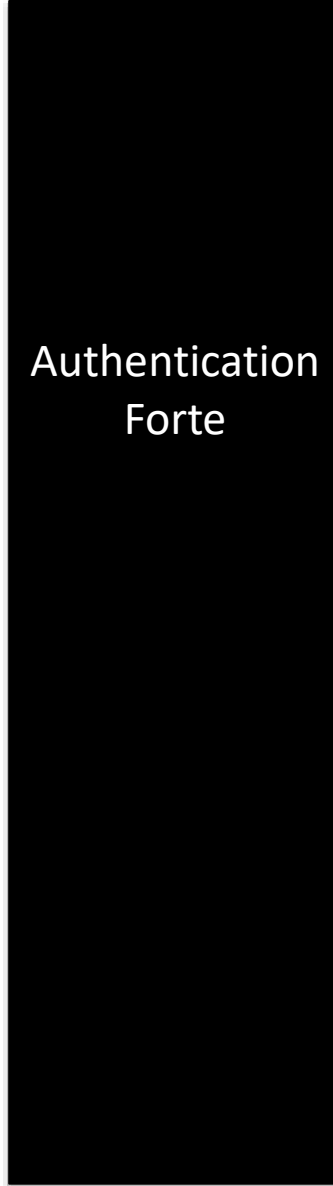
Tout afficher →

L'authentification forte : un challenge pour les fraudeurs

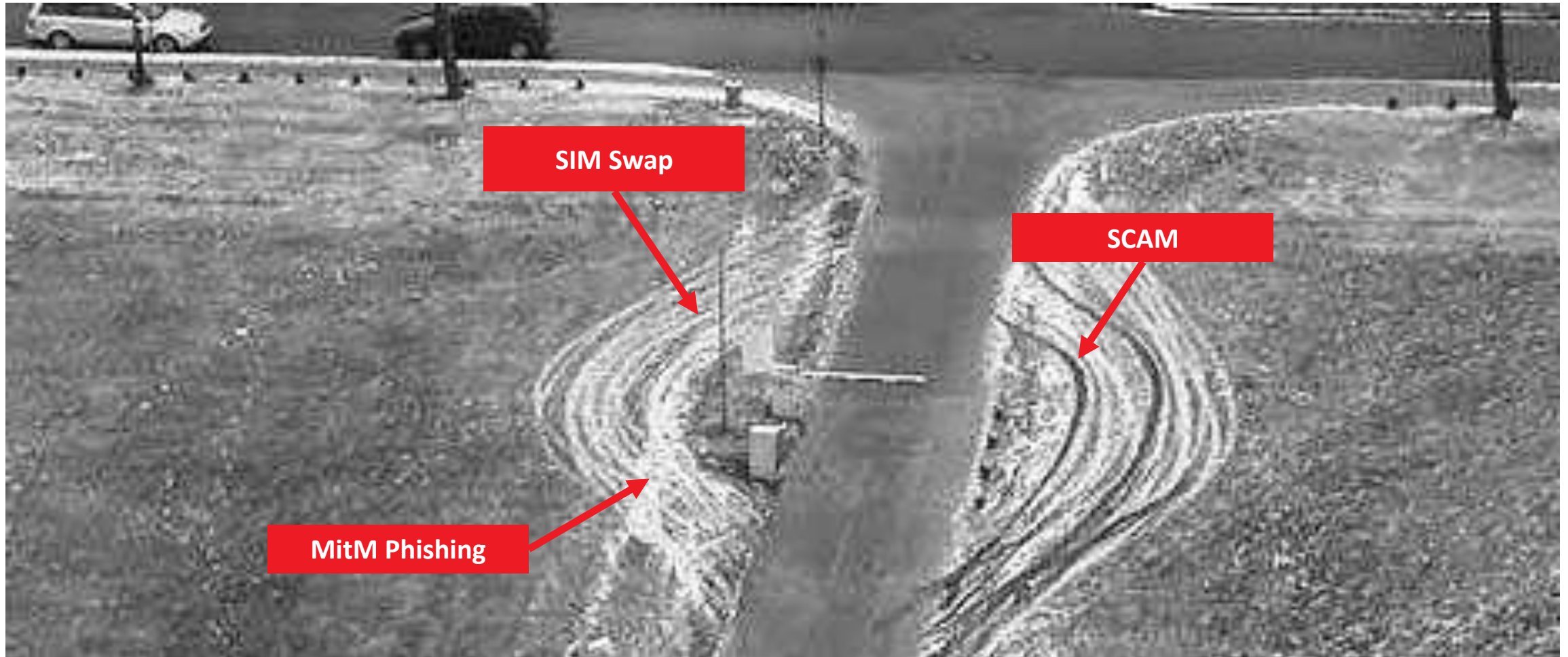
Fraudeur



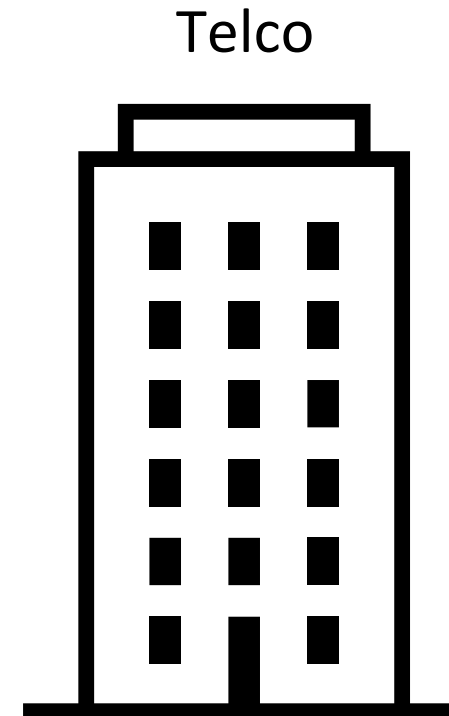
Authentication
Forte



Contournement de l'authentification forte



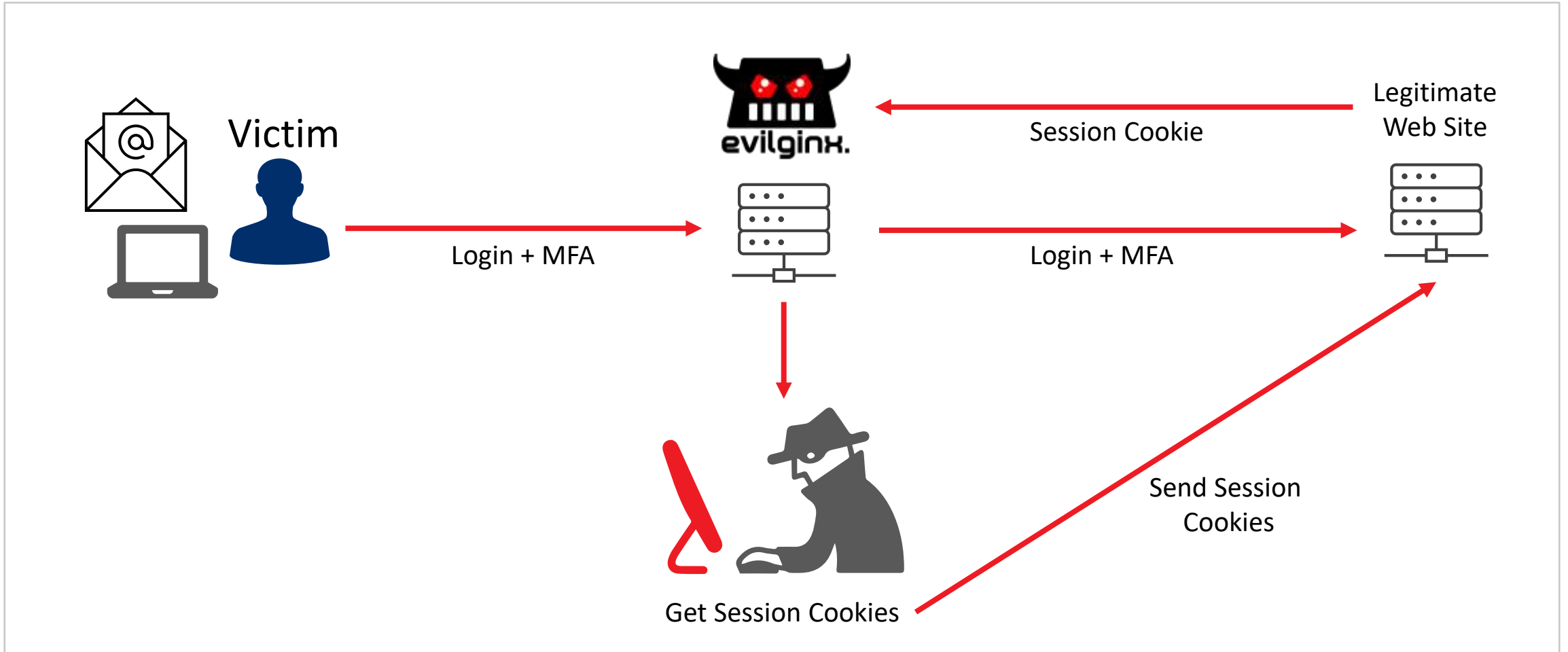
SIM SWAP



Man in the Middle PHISHING



PHISHING MITM



SCAM ?



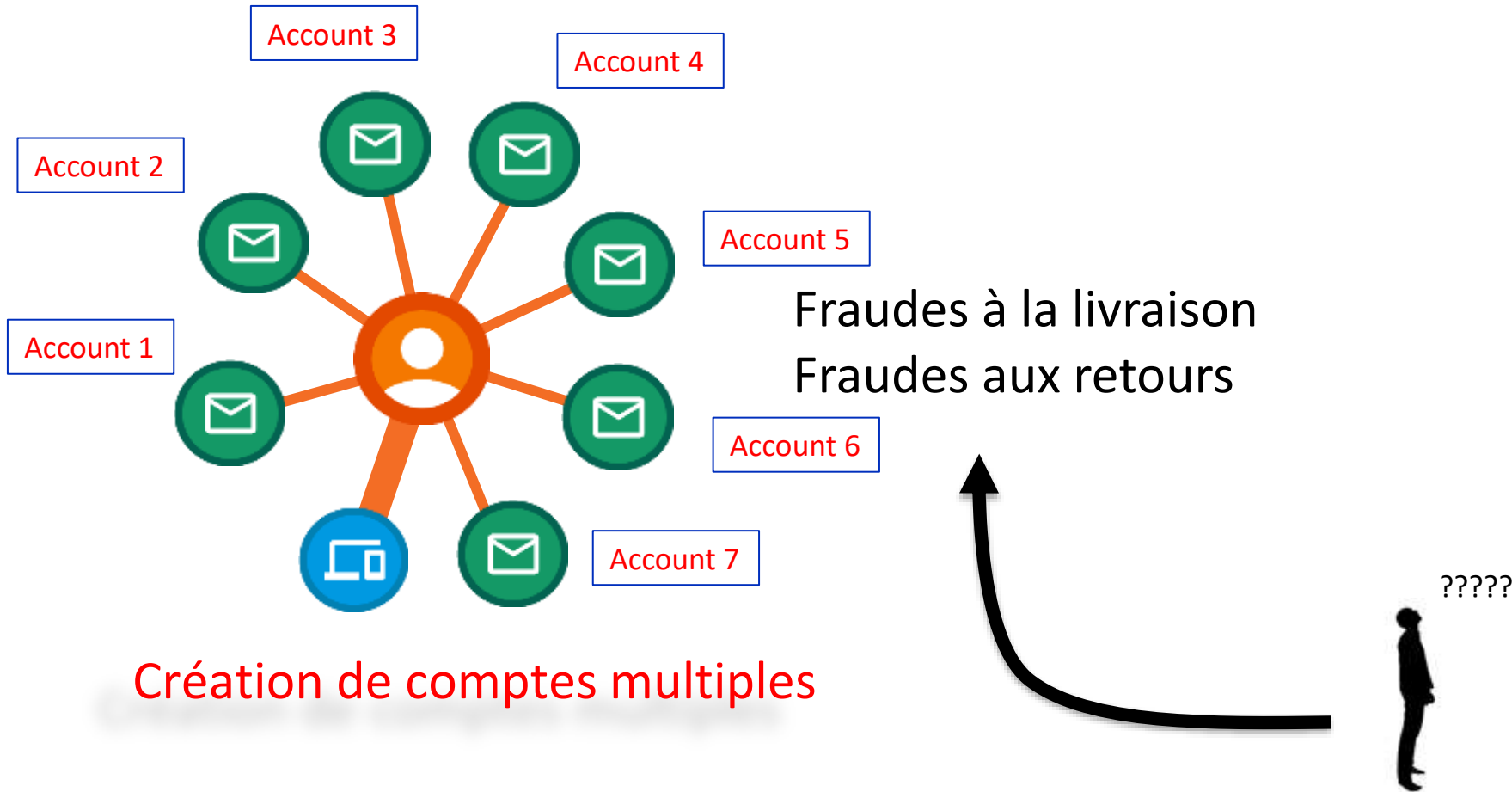
Vous êtes bien Mr. x ?

Votre numéro de compte est bien le xxx ?

Je fais partie de la cellule de lutte contre la fraude
de votre banque

Votre compte a été compromis

Les abus en forte augmentation



Comment limiter les
risques ?



4 PILIERS



**Création
de données**



**Réseau d'identité
numérique**



**Analyses
de données**



**Services
Professionnels**

CRÉATION DE DONNÉES

LexID Digital



IDENTIFIANTS MACHINE



DONNÉES LIÉES À LA LOCALISATION



ANALYSE COMPORTEMENTALE GESTUELLE



Clavier: Vitesse de frappe? Copier/coller?
Temps de remplissage ?



Gyroscope Le téléphone est-il tenu en mode portrait ou paysage ? Gestuelle montrant un appel lors de la transaction ?



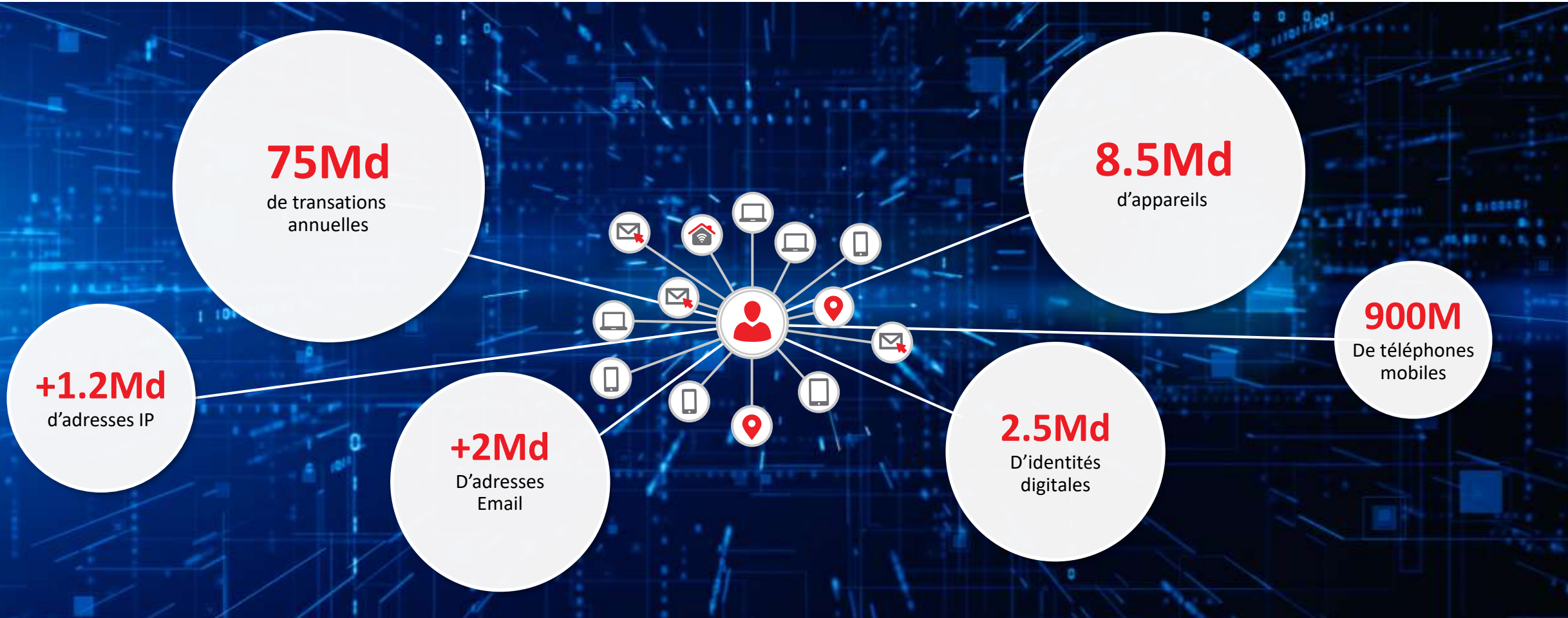
Souris: Distance? Courbes? Vitesse? Souris sortie de la page?



Toucher: Fréquence ? Vitesse de swipe ?



DONNÉES “CROWD SOURCE” POUR UNE MEILLEURE PRISE DE DÉCISION



ANALYSES DES DONNÉES



Moteur de règles

- Flexible
- Puissant
- Transparent
- Des centaines de variables
- Règles avec seuil dynamique (basé sur des variables)



Machine Learning

- Générer des modèles
- Créer de nouvelles règles
- Mesurer les ajustement à apporter
- Mesurer les performances

SERVICES PROFESSIONNELS



Expertise

Nous combinons plus de 100 ans d'expérience en matière de fraude et de risque avec une connaissance approfondie des produits pour garantir que le client dispose de la bonne solution pour répondre à des besoins en constante évolution.



Configuration Robuste

Nous veillons à ce que les clients disposent de la meilleure configuration possible et d'un accès à des plates-formes et solutions en constante expansion. C'est le fondement de votre réussite à long terme.



Optimisation des solutions et Engagements

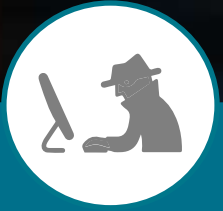
Nous optimisons la solution pour cibler efficacement et précisément les points faibles des clients et fournissons un soutien stratégique pour nous assurer que la solution évolue avec le client.



Des clients satisfaits

Vos clients ont une solution qui répond à leurs exigences, sont plus engagés et plus susceptibles de renouveler leurs interactions.

TYPES OF FRAUD



Account
Takeover



Scam
Detection



RAT
Detection



BOT
Attacks



Account
Opening



Malware
Defence

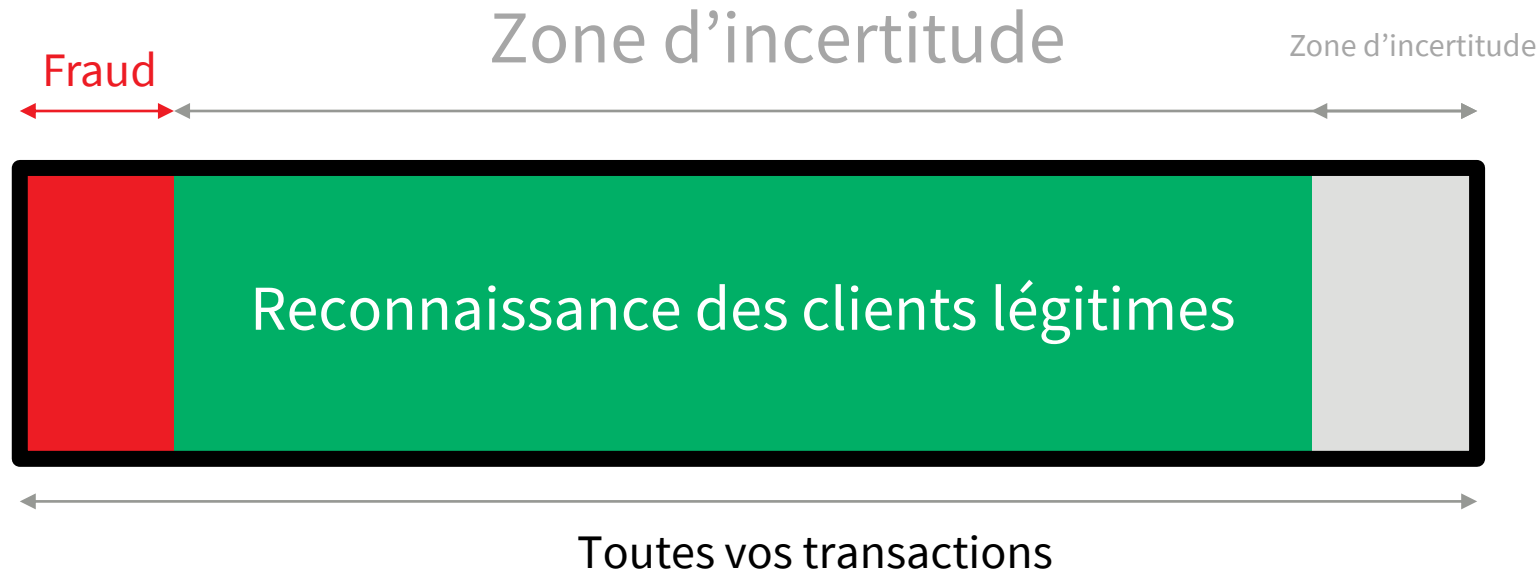


Card Not Present
Fraud



Abuses

RECONNAISSANCE DES CLIENTS LÉGITIMES



Moins de faux
positifs

Moins de SCA

Moins de revues
manuelles