

# RISQUES CYBER & LUTTE CONTRE LA FRAUDE

L'affaire de tous !



PARTENAIRE PREMIUM



**CAISSE  
D'ÉPARGNE**  
Rhône *Alpes*  
*Vous être utile.*

# SOMMAIRE

## Sensibilisation à la Cybersécurité

### Intervention :

- ❑ Karl RALLIS, *Directeur Centre Expertise Offres et Solutions CERA*

## Les différents types de fraude, sensibilisation et bons réflexes à adopter

### Intervention :

- ❑ Patrick MICHEL, *Directeur Filière Flux CERA*

## Présentation du logiciel de communication bancaire PULCEO

### Intervention :

- ❑ Karl RALLIS, *Directeur Centre Expertise Offres et Solutions CERA*

# Sensibilisation à la Cybersécurité



# CONTEXTE DE LA CYBERSECURITE

## Quelques chiffres

Une explosion des cyberattaques

**+30%**

Augmentation des attaques par rançongiciel par rapport à 2022

Source : ANSSI

**80%**

Des cyberattaques exploitent la technique du Phishing

Source : Club des Experts de la Sécurité de l'Information et du Numérique

Les sociétés sont des cibles régulières des cyberattaquants

**53%**

des sociétés françaises ont été la cible d'une cyber-attaque en 2023

Source : Hiscox

**34%**

Des victimes de rançongiciels en 2023 sont représentées par des TPE/PME/ETI  
24% sont des Collectivités et 10% des sociétés stratégiques

Source : ANSSI

Les sociétés ne sont actuellement pas suffisamment protégées

**90%**

des failles impliquent une erreur humaine

Source : IBM

**2/3**

des sociétés ne disposent pas de solution de protection de leurs applications WEB

Source : Visiativ

Des conséquences lourdes pour les victimes

Une attaque de phishing ou ransomware coûte en moyenne **100 à 250 k€** pour une société

# CYBERATTQUES : ENJEUX ET ÉLÉMENTS DE RÉPONSE

## Des solutions clés en main

À l'ère du digital, les points d'entrée des attaques se multiplient, **les risques sont réels et les conséquences**, en particulier pour les TPE/PME, **sont lourdes et parfois même désastreuses** : fraude bancaire, rançon, perte d'exploitation, perte de sauvegardes, pression des hackers de publier les données volées, impact en termes d'image, etc.

**Le besoin de cybersécurité est devenu un impératif** pour toutes les entreprises, quelle que soit leur taille.

Pour jouer pleinement notre rôle de Partenaire stratégique et être force de proposition, nous avons noué 3 partenariats solides permettant de couvrir l'ensemble de vos besoins en matière de Cybersécurité :



« Avant c'est trop cher, après c'est trop tard ! »

# Les différents types de fraude et modes opératoires

Sensibilisation et bons réflexes à adopter



PARTENAIRE PREMIUM



**CAISSE  
D'ÉPARGNE**  
Rhône *A*lpes  
*Vous être utile.*

# MODE OPÉRATOIRE : COMPROMISSION DES SYSTÈMES INFORMATIQUES

## Scénario

- Des emails semblant venir d'une institution (banque, fournisseur, client, ...) sont envoyés avec un lien ou une pièce jointe
- Des logiciels malveillants sont installés sur votre ordinateur à votre insu (malware)
- De fausses pages s'ouvrent et vous demandent des informations confidentielles (phishing, hameçonnage)

## Ce qui doit vous alerter

- Une pièce jointe à un courriel ou un support sur clé USB
- Une sollicitation ou un objet inattendu

## Les bons réflexes

- ✓ Vérifiez les emails (adresse, objet alarmiste, orthographe, le nom de domaine après le « @ » ...)
- ✓ Réalisez un contre-appel à l'expéditeur vers un numéro de confiance  
*Nb : la boîte mail de votre interlocuteur a pu être piratée, mais aussi la vôtre*
- ✓ Vérifier les liens (si sécurisé https, URL affiché en passant la souris...)
- ✓ Ne renseignez aucune information
- ✓ Veillez à la mise à jour de vos anti-virus
- ✓ Restreignez les possibilités d'installation de logiciels sur vos postes

# MODE OPÉRATOIRE : COMPROMISSION DES SYSTÈMES INFORMATIQUES

## Exemples

### SMS

Message  
sam. 7 mai à 04:47

AMELI : info samedi : Veuillez suivre la procédure de renouvellement de votre carte vitale via le lien suivant : <http://fr.redirection-infos-client.com>

impots.gouv  
Direction générale des Finances pu... OUVRIR  
INSTALLÉE

**l'Assurance Maladie**  
Agir ensemble, protéger chacun

Assurance Maladie / Mise à jour carte vitale

### Mettre à jour votre carte vitale

La mise à jour de la carte vitale doit se faire annuellement par ses bénéficiaire. Cette opération actualise les droits et garantit une prise en charge efficace des dépenses de santé plus rapidement.

Pour une façon pratique, facile et sécurisée de présenter une demande de votre nouvelle carte avec de nombreux avantages, veuillez suivre les étapes suivantes :

Nom  Prénom

Date de naissance  
Jour  Mois   
Annee

AA fr.redirection-infos-client.com

### Emails

Bonjour,

Vous avez modifié votre adresse mail depuis votre espace sécurisé caisse d'épargne En ligne de notre site internet

Nous vous confirmons que votre demande a bien été enregistrée..

Si vous n'êtes pas à l'origine de cette opération, [cliquez ici](#)

Merci de votre confiance,  
La Caisse d'Epargne

Suite à l'analyse de votre espace personnel, nous avons constaté avec regret que vos dispositifs sécuritaires sont obsolètes à la nouvelle mise à jour.

Nous vous prions donc d'actualiser vos données afin de vous mettre à l'abri.

Pour activer ce service, cliquez sur le bouton ci-dessous :

Mon Compte

# FRAUDE AU PRÉSIDENT

## Scénario

- Un escroc se fait passer pour le dirigeant de l'entreprise et demande un virement "inhabituel"

## Ce qui doit vous alerter

- Un mail ou un appel indiquant qu'une opération d'envergure va avoir lieu
- L'urgence et le secret de la situation, l'intimidation, la flatterie
- Les périodes comme les vacances ou veilles de week-end
- L'appel par un tiers (avocat, expert-comptable, auditeur, ...)

## Les bons réflexes

- ✓ Ne décidez rien seul et parlez-en à votre hiérarchie
- ✓ Vérifiez l'adresse mail si l'ordre est transmis par cette voie
- ✓ Vérifiez l'identité de votre interlocuteur en le recontactant sur un numéro sûr (appel sortant), et jamais par mail



A cause de  
vous l'affaire va  
capoter !



Je vous ai choisi  
car je vous  
connais pour  
votre discrétion



Je suis l'avocat  
de Monsieur...

# FRAUDE AU PRÉSIDENT

## Exemple

**De:** [redacted]  
**Envoyé:** [redacted]  
**À:** [redacted]  
**Objet:** [redacted]

Parfait,

Voici l'OPA en cours, nous effectuons en ce moment une opération financière concernant une fusion/acquisition de société basée en Europe.

Ce dossier doit rester strictement confidentiel, personne d'autre ne doit être au courant pour le moment.

L'annonce publique de cette opération aura lieu le [redacted] dans nos locaux avec la présence de toute l'administration.

Merci de prendre contact de suite avec notre cabinet KPMG à l'attention de Maître [redacted] pour la remise des coordonnées bancaires afin d'effectuer le virement dans l'immédiat.

Contact : [\[redacted\].kpmg@\[redacted\].com](mailto:[redacted].kpmg@[redacted].com)

Ps : par mesure de sécurité, merci de dialoguer uniquement sur mon mail sécurisé ([redacted]@[redacted].fr) pour cette opération confidentielle où nous pourrions discuter sans risque de divulgation afin de respecter les normes de ce dossier.

Merci de ne me faire aucune allusion sur ce dossier de vive voix, ni même par téléphone, uniquement sur mon mail personnel selon la procédure imposée par l'AMF (Autorité des Marchés Financiers).

Cordialement,

# FRAUDE AU FAUX FOURNISSEUR

## Scénario

- Des fraudeurs se font passer pour un créancier. Ils contactent un opérationnel de l'entreprise (comptable, trésorier), en lui rappelant le montant de la somme due, sa date d'échéance et en indiquant un changement d'IBAN (français ou étranger).

## Ce qui doit vous alerter

- Un IBAN atypique
- La nature de la demande
- Une facture inhabituelle sur le fond et la forme
- L'adresse mail de l'expéditeur

## Les bons réflexes

- ✓ Vérifiez l'adresse mail mais ne pas s'en contenter
- ✓ Vérifiez systématiquement un changement de RIB (contre-appel sortant)
- ✓ Mettez en place dans l'entreprise une procédure pour tout changement de RIB (par exemple contre-appel systématique),
- ✓ Désignez une personne responsable validant les nouveaux RIB

# FRAUDE AU FAUX FOURNISSEUR

## Exemple mail reçu

Account Receivable Urgent Memo



LA A <[redacted]@l.a.d.e>

Hello,

Please be informed that, we are undergoing our annual bank reconciliation and auditing on our account(s). We are going through auditing of all our unpaid invoices in the next 60 days with our auditors, we therefore need some clarifications;

- 1). How much is the outstanding/open invoices and the exact payment date?**
- 2). Can you please send a list of the open invoices and outstanding payments according to what your records show?**

If you have not paid yet, kindly hold on with the payment, so that we can make available our new alternative payment instructions to process payment, as our main account is under-going auditing and will not be able to receive funds at the moment.

Thank you in anticipation for your quick response.

Best Regards,

  
Managing Director

# FRAUDE AU FAUX TECHNICIEN

## Scénario

- Des fraudeurs se font passer pour un service d'assistance technique. Ils contactent un opérationnel du client (comptable, trésorier, assistant...). Ils peuvent aussi se faire passer pour le service fraude de la banque, de Visa...

## Ce qui doit vous alerter

- Des questions sur vos logiciels, vos services bancaires ou sur des informations personnelles (code, id)
- Une demande de prise en main à distance de votre PC, un lien internet que vous ne connaissez pas
- Une demande d'une personne que vous ne connaissez pas

## Les bons réflexes

- ✓ Restez toujours vigilant sur les appels entrants même si le numéro est connu. On parle alors de « spoofing »
- ✓ Rappelez / contactez toujours votre interlocuteur au numéro habituel
- ✓ Ne communiquez jamais aucun code
- ✓ Soyez vigilants sur les prises en main à distance

# FRAUDE AU FAUX TECHNICIEN

## Exemple de message d'alerte sur notre application bancaire illustré d'un cas concret

**Pour votre information**

**ⓘ SOYEZ VIGILANT !**  
Des fraudeurs peuvent vous contacter PAR TÉLÉPHONE ou EMAIL en se faisant passer pour votre conseiller, les services fraude ou opposition carte... en affichant parfois même nos numéros de téléphone.

Nous ne vous demanderons JAMAIS de COMMUNIQUER vos données bancaires (identifiant, mot de passe, code reçu par sms, code Sécur'Pass...), pour CONFIRMER ou ANNULER une opération (ajout de compte bénéficiaire, virement, paiement par carte, validation Sécur'Pass...).

Toute démarche contraire relève d'une tentative de fraude.

De manière générale, ne vous laissez pas impressionner par le caractère d'urgence de l'appel. En cas de doute, rapprochez-vous de votre agence au plus tôt.

**J'ai compris**

**Ne plus afficher**



**CAISSE  
D'ÉPARGNE**

---

**Objet : Action requise : Confirmation des informations de compte et réactivation du service de sécurité**

Cher(e) Client(e),

Afin de garantir la sécurité de votre compte et de maintenir des standards élevés en matière de protection des données, nous vous prions de bien vouloir confirmer et mettre à jour les informations associées à votre compte.

Par ailleurs, nous vous encourageons à réactiver immédiatement votre service de sécurité, Sécur'Pass, pour assurer une protection optimale de votre compte.

Sans action de votre part, votre compte sera mis en restriction temporaire et toute opération sera donc impossible à réaliser.

**Je confirme mes informations ici**

Merci pour votre coopération continue.  
Cordialement,  
Votre gestionnaire

## CE QU'IL FAUT RETENIR

**1**

Les escrocs  
renouvellent régulièrement  
leurs modes opératoires

+

**2**

Ils continuent leurs  
tentatives en cas d'échec et  
peuvent utiliser plusieurs  
méthodes

+

**3**

Les conséquences peuvent  
être dommageables pour  
votre entreprise

## LES BONS RÉFLEXES

Que faire quand vous êtes confronté(e) à une fraude (tentative ou fraude avérée)

- **Réactivité** : en cas de doute sur une opération, contactez immédiatement votre conseiller sur ses coordonnées habituelles
- **Déposez plainte** auprès d'un Commissariat de Police ou de la Gendarmerie
- **Recherchez activement la source** de la compromission, en s'adjoignant, le cas échéant les services d'une société spécialisée telles que celles qualifiées par l'ANSSI ([Lien ANSSI](#))

En amont

- **Formez et informez** vos collaborateurs sur tous les types de fraude en renouvelant leurs connaissances régulièrement
- **Mettez en place des procédures** internes pour les validations opérations sensibles
- **Vérifiez** régulièrement la **sécurité** de vos systèmes d'informations (serveurs, pare feu...)
- **Challengez** régulièrement vos collaborateurs (tests intrusion par exemple)
- **Adaptez les délégations dans votre logiciel de communication bancaire**

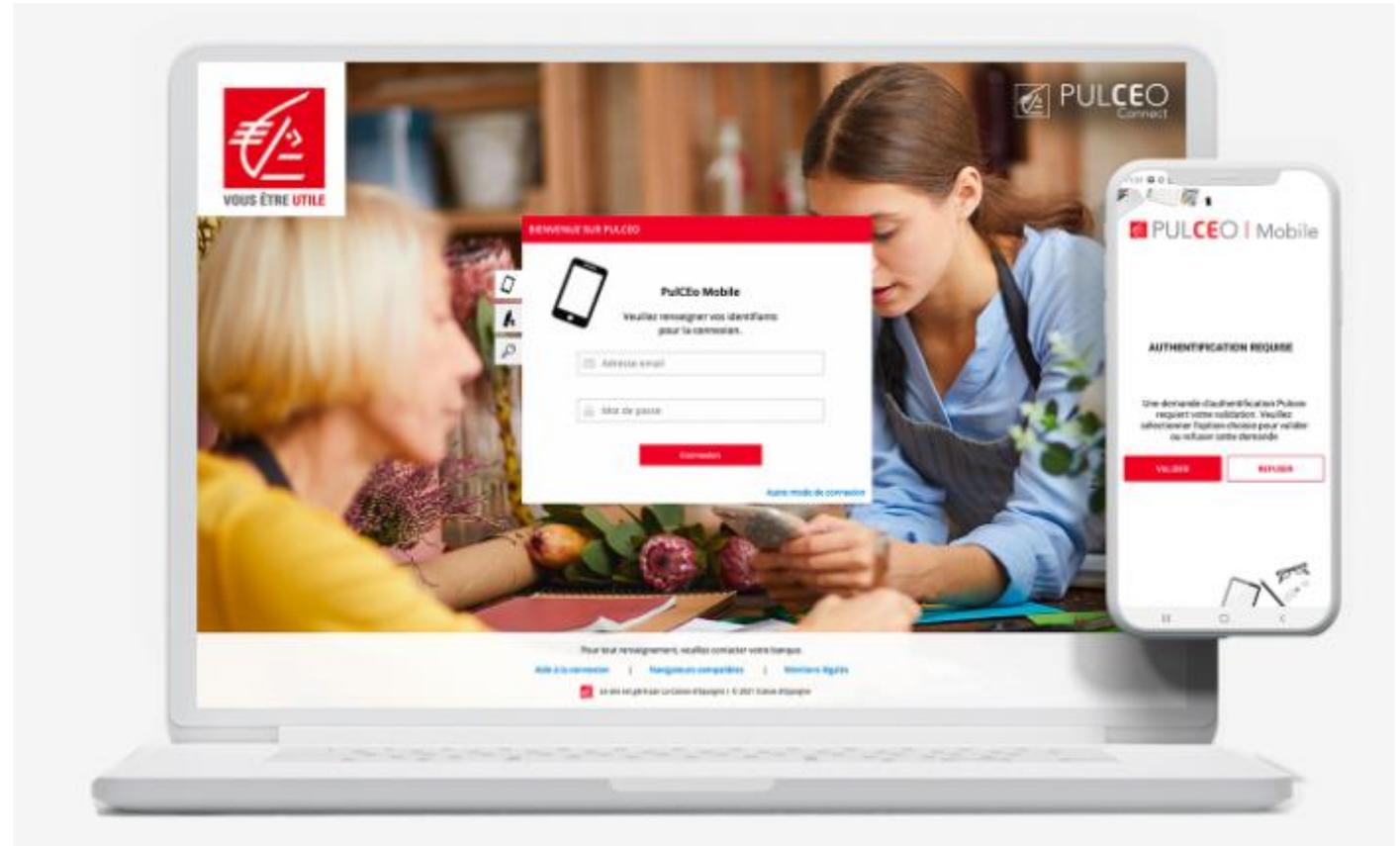
# Les solutions bancaires

Un bon moyen de limiter les risques de fraude



# PULCEO.COM : PLATEFORME DE GESTION DE FLUX ZOOM LUTTE CONTRE LA FRAUDE

**PulCEo** une plateforme multi-banque en mode SaaS (Software as a Service) utilisant le protocole EBICS TS



# PULCEO.COM : PLATEFORME DE GESTION DE FLUX

## ZOOM LUTTE CONTRE LA FRAUDE

Gérer les habilitations des utilisateurs : niveau comptes et types d'opérations

### Comptes

#### Modifier utilisateur

Étape 1 - Infos | **Étape 2 - Droits** | Étape 3 - Authentification

Comptes bancaires  Aucune restriction de comptes

16 COMPTES AUTORISÉS

Actions autorisées

<input type="checkbox"/> Nom société	Comptes autorisés	
<input checked="" type="checkbox"/> JUPITER	tous	<a href="#">cacher comptes</a> v
<input checked="" type="checkbox"/> Amalthée		
<input checked="" type="checkbox"/> Callisto		
<input checked="" type="checkbox"/> Compte Courant CE GEE 1		
<input checked="" type="checkbox"/> Compte Courant CE GEE 2		
<input checked="" type="checkbox"/> Compte Courant CE GEE 3		
<input checked="" type="checkbox"/> Europe		
<input checked="" type="checkbox"/> Ganymède		
<input checked="" type="checkbox"/> Io		
<input checked="" type="checkbox"/> MARS	tous	<a href="#">montrer comptes</a> <
<input checked="" type="checkbox"/> NEPTUNE	tous	<a href="#">montrer comptes</a> <
<input checked="" type="checkbox"/> PLUTON	tous	<a href="#">montrer comptes</a> <
<input checked="" type="checkbox"/> SATURNE	tous	<a href="#">montrer comptes</a> <

Modules

Précédent Enregistrer & suivre

### Types d'opérations

#### Modifier utilisateur

Étape 1 - Infos | **Étape 2 - Droits** | Étape 3 - Authentification

Comptes bancaires  Aucune restriction de comptes

16 COMPTES AUTORISÉS

Actions autorisées

TOUTE ACTION AUTORISÉE

Modules

- Portefeuille
- Relevés
- Virement SEPA
- Virement International
- Prélèvement SEPA
- Transmission
- Sepamail Diamond

Précédent Enregistrer & suivre

# PULCEO.COM : PLATEFORME DE GESTION DE FLUX

## ZOOM LUTTE CONTRE LA FRAUDE

Un système d'alerte vous prévient par mail dès qu'une opération que vous jugez exceptionnelle passe sur un de vos comptes bancaires.

Paramétrage > Général

▼ Rapports de sécurité

OUI Envoyer un mail pour chaque opération critique ?

Envoyer le rapport des opérations critiques  ?

Destinataires des rapports de sécurité : 1 utilisateur [modifier la liste](#)



- Création/modification des utilisateurs
- Activation/création/modification des bénéficiaires
- Modification des valideurs
- Modification de la liste de pays autorisés

Paramétrage > Alertes

OUI Activer Alertes

Utilisateur	Opé débit (à partir de)	Opé crédit (à partir de)	Solde Compte (inférieur à)	Fichiers en erreur	Fichier à signer	Fichier non envoyé	Notification
Elodie	Aucune alerte	Aucune alerte	Aucune alerte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Fabrice	Aucune alerte	Aucune alerte	Aucune alerte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Isabelle	Aucune alerte	Aucune alerte	Aucune alerte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sarah	Aucune alerte	Aucune alerte	Aucune alerte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

# **PULCEO.COM : PLATEFORME DE GESTION DE FLUX ZOOM LUTTE CONTRE LA FRAUDE**

**Parce que vous ne travaillez pas avec tous les pays**

**Afin de limiter toujours plus la fraude vers les pays étrangers :**

- Mise en place d'une liste de pays autorisés pour l'émission de vos virements
- Plafonds personnalisables par pays



# PULCEO.COM : PLATEFORME DE GESTION DE FLUX

## ZOOM LUTTE CONTRE LA FRAUDE

Contrôler systématiquement vos nouveaux IBAN (vos flux seront bloqués tant qu'une personne habilitée n'aura pas activé les nouveaux IBAN)

Virement SEPA > Bénéficiaires

Afficher les bénéficiaires issus de l'import de fichiers

 Société :

<input type="checkbox"/> Activé	Nom ou raison sociale	Pays	Société	Compte
<input type="checkbox"/>	 BEY KERIM	FR	Pluton	CRCAM FRANCHE COMTE
<input type="checkbox"/>	 DERVAL DOMINO	FR	Pluton	LYONNAISE DE BANQUE LB
<input type="checkbox"/>	 DRAXX INDUSTRIES_2	FR	Pluton	TRESOR PUBLIC
<input type="checkbox"/>	 GOLDFINGER AURIC	FR	Pluton	AXA BANQUE
<input type="checkbox"/>	 Liam Lefebvre SA	FR	Pluton	CAISSE D EPARGNE GRAND EST EUROPE
<input type="checkbox"/>	 Louis Morel SA	FR	Pluton	CAISSE D EPARGNE ILE DE FRANCE
<input type="checkbox"/>	 Nathan Martin SA	FR	Pluton	BANQUE POPULAIRE BOURGOGNE FRANCHE COMTE
<input type="checkbox"/>	 Pascal Bernard SA	FR	Pluton	BANQUE POPULAIRE ALSACE LORRAINE CHAMPAG
<input type="checkbox"/>	 SKRATOY JORG	BG 	Pluton	UNITED BULGARIAN BANK AD

# PULCEO.COM : PLATEFORME DE GESTION DE FLUX ZOOM LUTTE CONTRE LA FRAUDE

Vérifiez les coordonnées bancaires de vos partenaires commerciaux



**SEPA MAIL DIAMOND** permet de

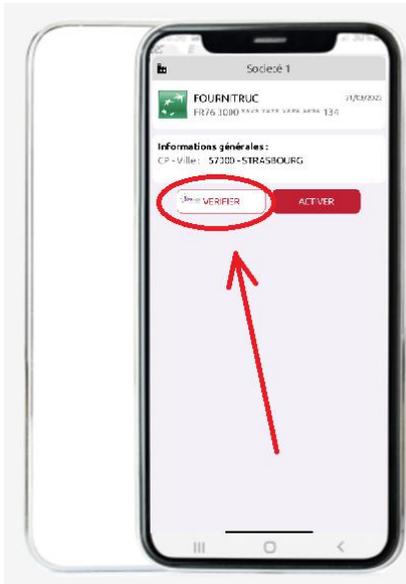
- Détecter si l'IBAN existe vraiment, s'il correspond à un compte ouvert
- Vérifier si l'IBAN correspond au titulaire présumé du compte

**2 possibilités de contrôle :**

PulCEo Mobile

ou

le logiciel PulCEo



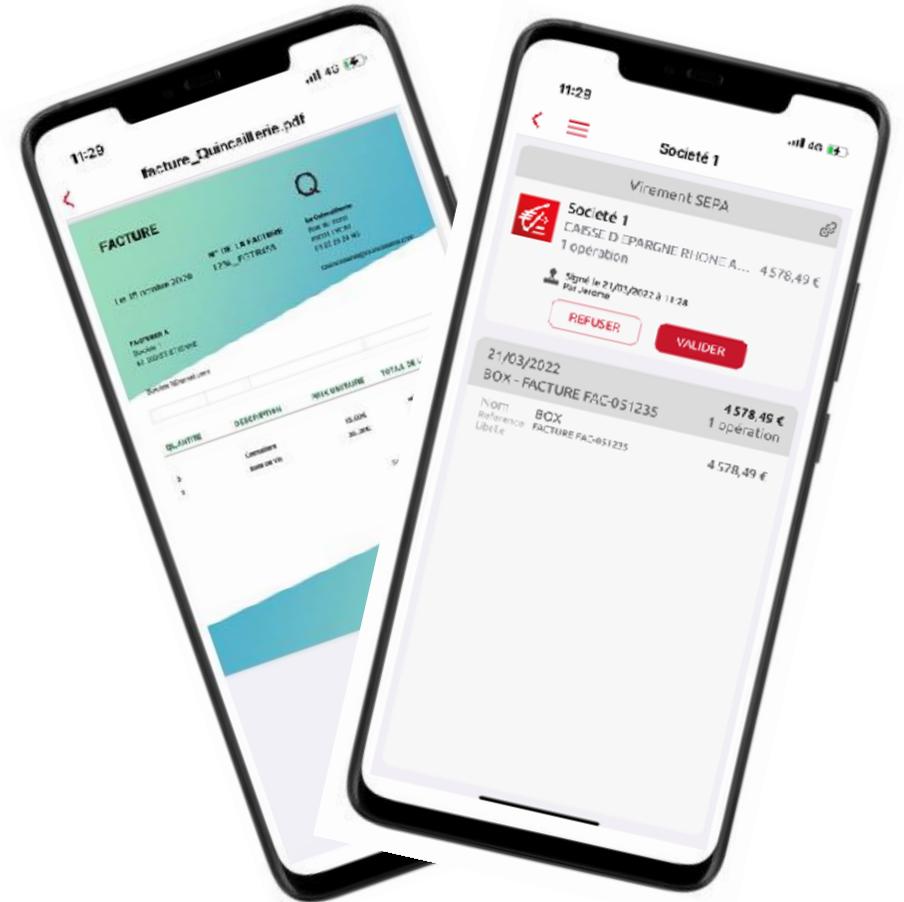
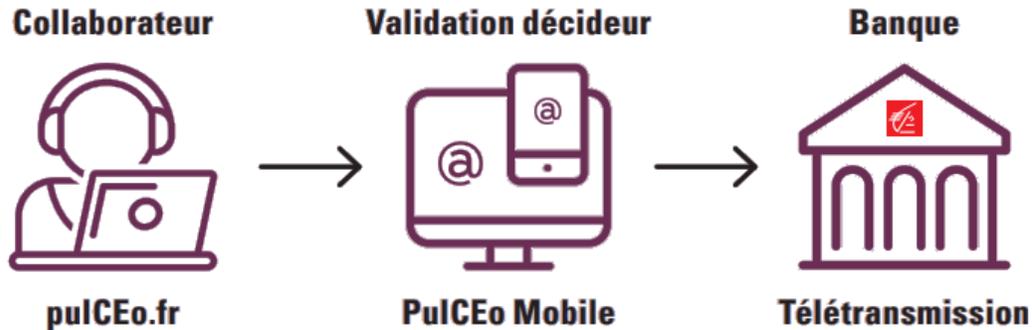
État	Score	Résultat	Informations du détenteur	Numéro de compte	Détails
<input type="checkbox"/>	0		Peter Parker	FR76 1005 7000 0153 7146 6441 831	Compte clos Score : 0 (Données incorrectes)
<input type="checkbox"/>	400		SA TARTEMPION	FR76 1213 5454 5847 1547 1472 143	IBAN valide et connu Type client correct (particulier/entreprise)
<input type="checkbox"/>	400		STADIUM PLACE	FR76 1333 5171 3500 0165 4177 477	IBAN valide et connu Type client correct (particulier/entreprise)
<input type="checkbox"/>	400		BOX	FR76 1382 5445 4548 0210 0000 271	IBAN valide et connu Type client correct (particulier/entreprise)

# PULCEO.COM : PLATEFORME DE GESTION DE FLUX ZOOM LUTTE CONTRE LA FRAUDE

Validez depuis votre smartphone les flux préparés par vos collaborateurs

PulCEo Mobile offre aux décideurs de l'entreprise de valider les flux avant envoi en banque

- Opération au débit et/ou au crédit du compte
- Possibilité de joindre une facture
- Plafond personnalisable par valideur



## — SYNTHÈSE PULCEO

- Sécurisez vos flux grâce au protocole EBICS TS
- Connectez-vous et signez vos opérations avec authentification forte
- Gérez les habilitations de vos utilisateurs
- Recevez des alertes sur des personnes de confiance
- Maîtrisez les pays avec lesquels vous faites des opérations
- Gérez le référentiel de vos bénéficiaires de virements
- Maîtrisez la destination de vos virements
- Validez et suivez vos opérations à distance

# Réponses à vos questions



## POUR ALLER PLUS LOIN

- **Le site national d'assistance et de prévention du risque numérique**  
<https://www.cybermalveillance.gouv.fr/>
- **Guide édité par l'ANSSI (Agence nationale de la sécurité des systèmes d'information)**  
<https://cyber.gouv.fr/bonnes-pratiques-protégez-vous>
- **Les clés de la Banque – Ordre de virement des entreprises - 9 réflexes sécurité**  
<https://www.lesclesdelabanque.com/entreprise/ordres-de-virement-des-entreprises-9-reflexes-securite/>
- **Retrouvez nos conseils et nos solutions en matière de sécurité**  
<https://www.caisse-epargne.fr/rhone-alpes/votre-banque/securite/>
- **PULCEO : informations clés ainsi que la vidéo disponible en cliquant sur ce lien [Pulcéo](#)**



PARTENAIRE PREMIUM

