L'IBAN : une information sensible disponible dans tous les dossiers

Résumé du document :

L'**IBAN** est visible en clair dans notre base de données (fiches de paie) alors qu'il n'est **pas nécessaire** pour constituer un dossier locatif.

Contrairement aux idées reçues, un simple IBAN suffit **pour prélever un compte sans autorisation**, sans validation bancaire, grâce au **SEPA Direct Debit**.

Avec un IBAN, un attaquant peut :

1. **Faire des dons** au nom de la victime jusqu'à vider son compte
2. **Débiter des comptes** à plus grande échelle **s'il jouit d'un ICS via Stripe** (par exemple)

💡 **Suggestions de solutions pour Dossier Facile** :
- **Sensibiliser les utilisateurs** à masquer leur IBAN.
- **Automatiser le caviardage** des IBAN sur les fiches de paie.

🚨 I. Constats

- L’IBAN apparaît en clair sur certains bulletins de paie stockés dans notre base de données.
- Avec les autres infos présentes dans les dossiers, il est facile de reconstituer un RIB complet… (ce n’est même pas nécessaire d’aller jusque-là pour faire des dégâts.)
- Ce n'est en aucun cas une information nécessaire dans la constitution d’un dossier de location.

I. Le vol d’IBAN, un sport à la mode

Prenons un exemple récent : le **piratage massif des données des données des utilisateurs Free**. Des milliers d’IBAN bientôt dans la nature. (Pour le moment la base de données n’a été vendue que 2 fois sur Breach Forums mais elle se retrouvera tôt ou tard en accès libre.)

Une réaction médiatique rassurante mais trompeuse

Suite à cela, les médias ont tenu à **rassurer** :
https://www.bfmtv.com/tech/vie-numerique/piratage-de-sfr-que-risquez-vous-si-votre-rib-ou-votre-iban-a-ete-derobe_AV-202409200533.html

"Le RIB ou l'IBAN ne sont pas des moyens de paiement. On ne peut rien décaisser sans l'autorisation du propriétaire du compte", souligne Guillaume Almeras, fondateur et animateur du blog spécialisé en banque-finance Score Advisor."

II. Le risque est réel et identifié

L’administration reconnaît le risque :

Un site gouvernemental explique les manipulations à effectuer en cas de prélèvement SEPA non autorisé cela sous entend donc que c’est quelque chose de possible

II.1 On en parle

Quelques autres articles mentionnants des prélèvements bancaires non autorisés :

- **Yahoo : ‘Attention, des Français ont eu la mauvaise surprise de découvrir des prélèvements non autorisés sur leur compte bancaire ces derniers jours.**

- **Service public : témoignages de prélèvements injustifiés**

- **https://www.rtl.fr/actu/sciences-tech/une-nouvelle-arnaque-aux-prelevements-non-autorises-en-cours-a-travers-la-france-7900259053**

- **https://www.rtl.fr/actu/economie-consommation/arnaque-aux-prelevements-non-autorises-en-france-comment-se-proteger-7900265652?utm_**

II.2 Un raisonnement bancal (à mon sens)

“On ne peut rien décaisser sans l'autorisation du propriétaire du compte”

C’est faux, faire un don à une association permet de s’en rendre compte. Justifier de son identité n’est pas nécessaire, donner une autorisation depuis son espace bancaire non plus.

Les journalistes confondent souvent **"vider un compte"** et **"récupérer l’argent"**, alors que ce sont **deux choses différentes**.
👉 **Vider un compte** = énorme pouvoir de nuisance, même si l’attaquant ne peut pas récupérer les fonds.
👉 **Récupérer l’argent** = autre problématique, mais solutionnable à des niveaux de “filouteries” pas si élevés que cela (voir suite - méthode 2)

Les banques remboursent-elles systématiquement ?

Ils insistent sur un point :

"Les banques remboursent toujours en cas d’arnaque au mandat de prélèvement SEPA."

C’est tout à fait vrai, mais pourquoi ?

Tout simplement parce que **les banques ne vérifient plus les mandats de prélèvement SEPA** depuis la mise en place du **SEPA Direct Debit* (SDD) en 2010-2014**.

Le **SEPA Direct Debit (SDD) est un système de prélèvement automatique européen qui permet à un créancier de débiter un compte en euros dans la zone SEPA, sans validation bancaire préalable, en s’appuyant uniquement sur un mandat de prélèvement.*

Auparavant, les banques contrôlaient les mandats, mais aujourd’hui, **c’est le créancier (celui qui fait le prélèvement) qui est chargé de s’en occuper**. La banque, elle, se charge d'accréditer les créanciers en leur donnant un identifiant unique dit numéro ICS mais on y reviendra plus tard.

https://www.banquepopulaire.fr/entreprises/activite-international/paiement-sepa

Donc oui, en cas de fraude : **Le banque rembourse systématiquement** (faut-il encore s’en rendre compte et porter réclamation)

Mais ça ne veut pas dire qu’il n’y a aucun problème !

Même si la banque est toujours en tort et **doit rembourser** (jusqu’à 13 mois après l’opération frauduleuse selon sa nature), ça ne veut pas dire que c’est anodin :

1️⃣ **un compte peut être vidé.** Il faut ensuite effectuer des démarches pour obtenir un remboursement + aller déposer plainte

2️⃣ **Ça attire les attaquants** Une base de données avec autant d’IBAN + toutes les autres infos persos associées est une vraie pépite.

III. Démonstrations - Vider un compte

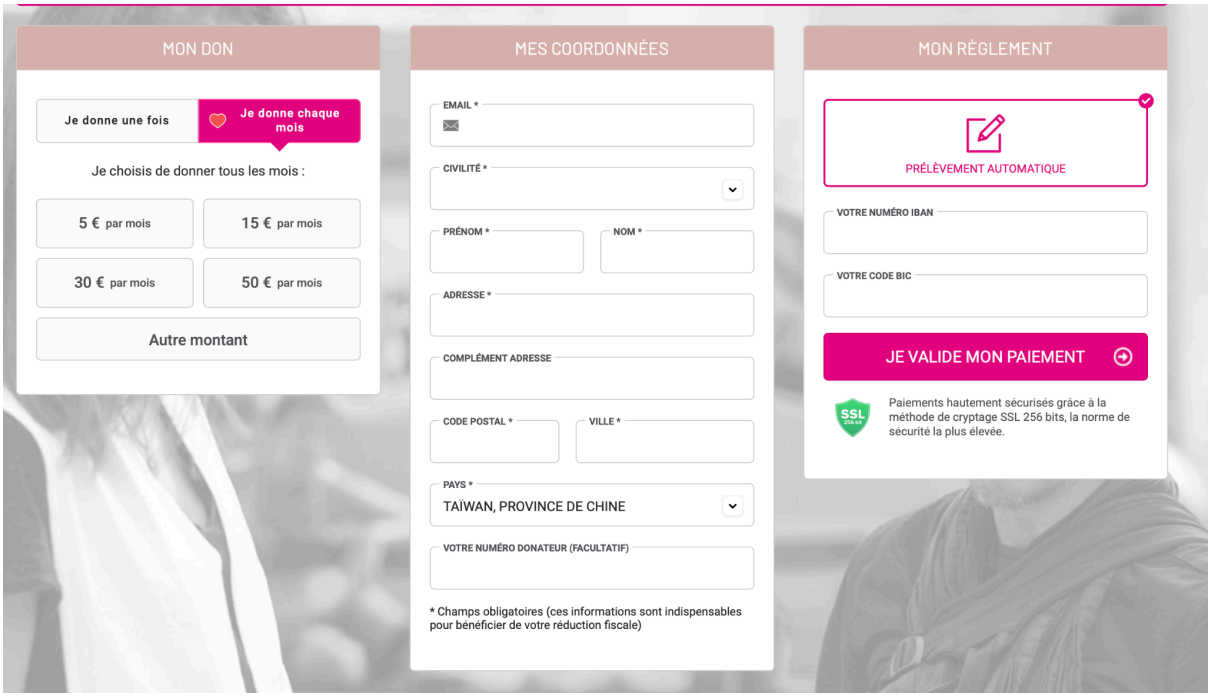
Maintenant, une petite démo pour bien mesurer le **niveau de criticité**, je vais vous montrer **deux méthodes pour prélever un compte bancaire** en ne disposant que d’un IBAN.

⚠️ **Disclaimer** : **Cette démarche a pour unique but de sensibiliser et de souligner l’importance du sujet. Cela ne saurait être interprété comme une incitation, une intention malveillante ou une tentative de fraude.**

III.1 - Les dons aux associations

En effet un IBAN est suffisant pour faire des dons à des associations (le malfaiteur ne récupère pas l'argent mais l'argent est bel et bien débité sur le compte de la personne attaquée):

Les restos du coeur : https://dons.restosducoeur.org/particulier/~mon-don
Option : "Je donne chaque mois"

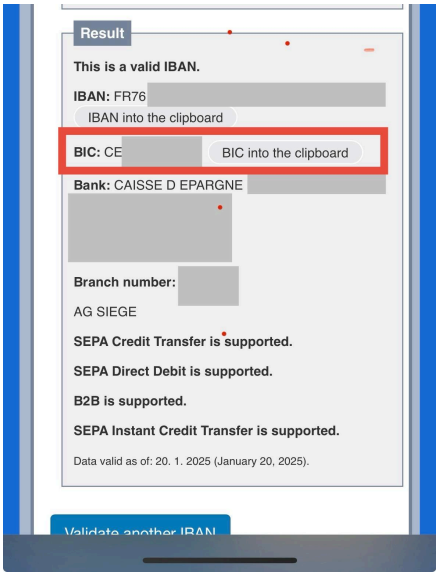


Uniquement 2 informations sont demandées :

- L'IBAN (dispo sur nos fiches de paie donc)
- Le BIC aussi appelé le code SWIFT (calculable)

Ici, le BIC est demandé (ce n'est pas toujours le cas) mais celui-ci est facile à déterminer à partir de l'IBAN. Je ne rentre pas dans les détails mais toutes les séquences dans un IBAN et un BIC ont une signification (à l'instar du début du numéro de sécurité sociale par exemple). Les derniers caractères (chiffres) d'un BIC représentent l'agence précise dans laquelle est domiciliée votre compte, mais cette info est souvent remplacée par "XXX" car ce n'est pas une information nécessaire pour la plupart des opérations. Le code BIC est parfois commun pour une région entière.

Il est très facile de trouver le BIC à partir d'un IBAN, divers sites le font très bien:



https://www.ibancalculator.com/iban_validieren.html
Pour la science j'ai testé sur ce site (le faites pas, je ne sais pas si il s'agit d'un site très fiable) et le BIC renvoyé est correct juste à partir de mon IBAN.

Le site https://www.iban.com/ propose aussi un calculateur de BIC qui semble bien plus sûr pour vos données (mais son usage est payant).

Cette solution est vraiment simple à mettre en place pourtant le pouvoir de nuisance est réel. Le risque pour le malfaiteur est absolument nul.

PS: Mes banques (Crédit Agricole et Caisse d'épargne) ne m'ont jamais informé explicitement que j'avais accordé des mandats de prélèvement à diverses associations.

III.2 - Prélèvements non autorisés hors associations

Débiter des comptes sans aucun accord préalable **ET** récupérer l'argent est tout à fait possible en ne disposant que d'un IBAN et de quelques connaissances.

Informations en préambule **rédigées par chat GPT** pour mieux comprendre la manip à suivre et comment ça se fait que ce soit si facile :

"Le fonctionnement des ICS dans le cadre des mandats de prélèvement SEPA

L'Identifiant Créancier SEPA (ICS) est un numéro unique attribué à une entreprise ou un organisme qui souhaite initier des prélèvements SEPA. Il permet d'identifier le créancier lors de chaque transaction et est obligatoire pour tout prélèvement SEPA.

Comment fonctionne un ICS ?

- ***Obtention de l'ICS** : Une entreprise doit demander un ICS auprès de sa banque ou de l'organisme compétent de son pays.*
- ***Enregistrement des mandats** : Le créancier (l'entreprise qui prélève) doit faire "signer" un mandat SEPA par le débiteur (le client).*

- ***Archivage et gestion*** *: Contrairement à avant, les banques ne vérifient plus les mandats, c'est le créancier qui est responsable de leur conservation et de leur validité.*
- ***Exécution des prélèvements*** *: Lorsqu'un prélèvement est initié, l'ICS est inclus dans la transaction pour identifier l'entité qui effectue le prélèvement.*

En clair : L'ICS est une baguette magique vous permettant de prélever absolument n'importe quel compte bancaire présent dans la zone SEPA sans avoir à vous justifier en amont.

On dit merci qui ?

STRIPE (ou un autre processeur de paiement)

Stripe est l'un des plus gros processeurs de paiement en ligne qui permet aux entreprises d'accepter des paiements via carte bancaire, prélèvement SEPA et autres moyens de paiement électroniques.

L'accès à l'ICS de Stripe après vérification

Plutôt que d'exiger de ses utilisateurs qu'ils obtiennent leur propre ICS, Stripe met à disposition son propre Identifiant Créancier SEPA pour faciliter les prélèvements automatiques.

Mais avant de pouvoir utiliser cet ICS, Stripe impose une vérification d'identité de l'entreprise.

Cette vérification peut inclure :

- *La fourniture de documents légaux sur l'entreprise (SIRET, statut juridique, etc.).*
- *Une validation des bénéficiaires effectifs de l'entreprise.*
- *Une analyse des risques liés à l'activité de l'entreprise.*

Une fois la vérification terminée, l'entreprise ou l'individu peut initier des prélèvements SEPA en utilisant l'ICS de Stripe sans avoir à en demander un auprès de sa propre banque."

A noter en supplément que Stripe limite à 10 000€ par semaine les prélèvements effectués par des comptes récemment créés et vérifiés. C'est pas énorme et c'est donc une sécurité supplémentaire mais ça laisse quand même de la marge.

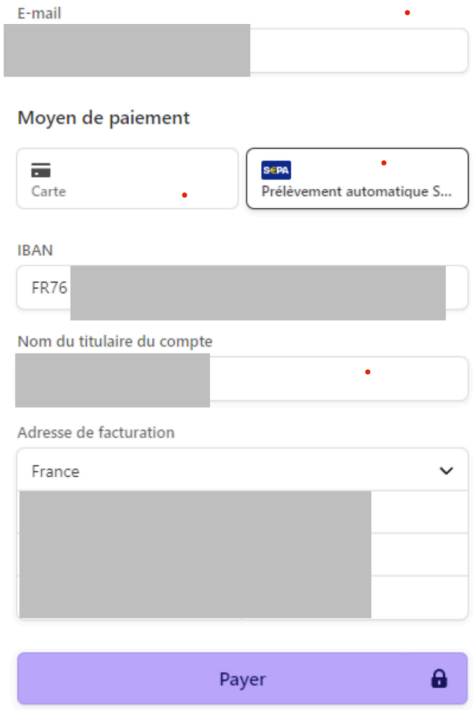
Pour commencer notre petite entreprise malveillante 2 solutions s'offrent à nous pour bénéficier de l'ICS de Stripe :

1- Créer une société bidon et l'enregistrer en France (ou dans n'importe quel pays européen). C'est gratuit, rapide et les vérifications sont très faibles
2- Utiliser les documents d'une autre société. Les documents demandés pour une entreprise française sont Carte d'identité et K-BIS (plutôt très facile à se procurer)

Se servir des documents issus de l'une de ses solutions pour s'authentifier auprès de Stripe et commencer à jouir de l'utilisation de leur ICS.

Je ne détaille pas davantage ici mais c'est étrangement assez facile.

Une fois les mandats de prélèvement SEPA mis en place il suffit de créer une page web et d'y insérer une interface de paiement. Voici comment cela se présente concrètement pour remplir le mandat afin de débiter un compte :



L'unique information importante demandée est l'IBAN. Le prélèvement sera effectif même si toutes les autres informations sont fausses (nom inclus).

(Le nom du titulaire du compte est évidemment un jeu d'enfant à trouver mais ce n'est en réalité même pas important. Comme expliqué précédemment les banques n'effectuent AUCUN contrôle systématique de cohérence. C'est évidemment aussi le cas pour l'adresse.)

Et voilà, c'est déjà fini en fait. L'argent est débité du compte sous quelques jours, rarement plus d'une semaine. Tandis que Stripe libère les fonds en général sous 3 semaines. Tout cela laisse des traces quand l'assaillant est un amateur mais à un niveau intermédiaire il est très facile de faire sortir l'argent d'europe.

Certaines banques notifient le fait qu'un mandat de prélèvement SEPA a été initié. Mais cela n'est pas systématique (je ne sais pas pourquoi).

LIMITES DE LA MÉTHODE :

- Stripe est connu pour être assez tatillon. Si une victime avertie suspend le mandat et le conteste rapidement alors Stripe aura le temps de bloquer le compte du malfaiteur pour mener une investigation plus précise comprenant une vérification d'identité plus poussée.

Propositions de solutions que nous pourrions mettre en place pour limiter ce problème :

- inciter les utilisateurs à caviarder eux même leur IBAN (et numéro SS aussi tant qu'à faire). Et donc rajouter une page de documentation pour expliquer la bonne manière pour caviarder un document.
- Utilisation d'un outil qui permettrait automatiquement de détecter l'IBAN sur les fiches de paie puis de le caviarder ?
- Donner la possibilité technique à l'équipe d'opération de caviarder manuellement ?

BONUS : Les bonnes pratiques pour éviter ces problèmes si votre IBAN a fuité :

- créer une liste blanche pour les mandats de prélèvement directement depuis votre espace bancaire
- changer de compte en banque en cas de fraude constatée (pour avoir un nouvel IBAN)
- utiliser 2 comptes bancaires. L'un sert pour recevoir son salaire ou autre et dispose de l'IBAN que l'on partage à des tiers. Mais il ne stocke jamais l'argent trop longtemps et

renvoie systématiquement tout versement entrant vers un second compte vous appartenant. (Vous ne partagez évidemment JAMAIS l'IBAN du second compte).