



Au cours de ces derniers mois, la FSMA a, dans le cadre de fraudes à l'investissement, observé un grand nombre de cas d'usurpation d'identité de sociétés autorisées (« cloned firm »). Dans ce cadre, les escrocs usurpent l'identité d'une société autorisée afin de faire croire aux consommateurs qu'ils sont en droit de leur offrir des services d'investissement, alors que ce n'est pas le cas. Leur offre relève de la pure escroquerie. La FSMA met dès lors les consommateurs en garde.

Comment les escrocs procèdent-ils ?

Afin de vous convaincre de donner suite à leur offre d'investissement, les escrocs vous font croire qu'ils agissent pour des sociétés qui disposent des autorisations requises pour offrir de tels services et qui sont inscrites dans les registres de la FSMA ou d'une autre autorité.

À cette fin, ils utilisent, de manière usurpatrice, les noms et autres informations légales de prestataires régulés et renvoient par exemple les consommateurs sur le site web officiel de la FSMA pour tenter de convaincre qu'ils sont bien autorisés. Les consommateurs sont ainsi trompés, pensant avoir affaire à un acteur régulé, alors que l'identité de ce dernier est tout simplement usurpée.

Dans certains cas, les escrocs renvoient également au site web de l'Autorité de contrôle prudentiel et de résolution (ACPR), autorité française, et plus particulièrement au registre des agents financiers (REGAFI) publié sur celui-ci.

Les consommateurs témoignent:

« La première chose qu'ils vous disent quand on les contacte de Belgique est de taper sur votre moteur de recherches le nom de cette société. »

« Pour me mettre en confiance et me prouver leur bonne foi, [l'interlocutrice] m'a invitée à aller sur le site internet français dépendant de la Banque de France qui répertorie le registre des agents financiers sur le territoire français (www.regafi.fr). Après recherche de ma part sur ce site, je tombe sur ce lien : (...). Etant convaincu de leur bonne foi, j'ai donc ouvert un compte sur leur site ».

« L'interlocutrice, 'chargée de clientèle', m'a conduite sur le site REGAFI pour me montrer que la société était enregistrée sous le n° XXX. Ma question : cet enregistrement a-t-il de la valeur ? »

Dans quel contexte peut-on rencontrer cette pratique ?

Ces usurpations d'identité peuvent se rencontrer dans n'importe quel type de fraude à l'investissement.

La FSMA vous invite cependant à être particulièrement méfiant dans le contexte des fraudes aux cryptomonnaies, où cette pratique semble extrêmement courante.

En effet, la FSMA a récemment mis en garde contre un grand nombre de ces plateformes qui proposent des investissements « miracles » très simples et très lucratifs basés sur les cryptomonnaies, mais qui ne sont en réalité que des escroqueries (voyez notre dernier [communiqué](#) du 26 octobre 2018). Il semble qu'une partie importante de ces sites web usurpent l'identité de sociétés autorisées à offrir des services financiers en Belgique, en renvoyant à leur autorisation sur le site web de la FSMA (voire sur le registre des agents financiers de l'ACPR – REGAFI).

Comment éviter le piège ?

Cette pratique frauduleuse peut être difficile à repérer et à contrer. Nous vous invitons par conséquent à effectuer les démarches suivantes pour vous assurer que votre interlocuteur est bien celui qu'il prétend être :

- Vérifiez que les **coordonnées de contact** reprises sur le site de la FSMA concernant cette société et celles notées sur le site web de votre interlocuteur sont bien les mêmes.

Attention ! Il est toutefois fréquent que les escrocs usurpent également l'adresse postale de la société agréée. Le fait que la bonne adresse postale soit utilisée par votre interlocuteur n'est donc pas suffisant pour vous assurer de son identité !

- Utilisez des moteurs de recherche en ligne pour vous assurer qu'il n'existe pas **un autre site web au nom de la société autorisée**.

Attention ! Il est fréquent que les escrocs utilisent une adresse internet très proche de celle du site officiel de la société dont ils usurpent l'identité (en rajoutant un tiret dans l'adresse, en utilisant une autre extension (.com à la place de .be par exemple), ...)

- Confrontez **les informations officielles avec les faits**. Par exemple, si votre interlocuteur prétend représenter une société établie en Belgique mais vous contacte avec un numéro de téléphone étranger, cela doit vous alerter. De la même façon, vous devez être méfiant si le site web de la société est uniquement en langue française ou néerlandaise alors que la société prétend être établie dans un pays étranger, dont la langue officielle est autre.
- Utilisez des outils en ligne permettant de vérifier la **date de création du site web** utilisé par vos interlocuteurs. Si le site web est très récent, il s'agit d'un indice important permettant de douter de la fiabilité de celui-ci.
- Si vous avez le moindre doute concernant l'identité de votre interlocuteur, prenez contact avec les services de la FSMA via le [formulaire de contact pour les consommateurs](#).

Source URL: <https://www.fsma.be/fr/warnings/la-fsma-met-en-garde-contre-lusurpation-didentite-de-societes-agreees>