# INGENIERIE SOCIALE & CYBERCRIMINALITE

Lutter contre la fraude est l'affaire de tous

Conférence – débat

Lundi 9 Mars 2020

# LA FRAUDE AUJOURD'HUI

Le contexte actuel

Panorama des menaces

# LE CONTEXTE ACTUEL

**Fraudeurs de mieux en mieux organisés**

**Techniques de fraude de plus en plus élaborées**

**Explosion de la fraude**

## Parmi les fraudes les plus répandues

**Entrée en relation frauduleuse**

Escroquerie sentimentale

**Faux crédits immobiliers**

Falsification de chèque

**Arnaques via les réseaux sociaux**

Phishing

Fraude Président,
Changement de coordonnées bancaires

**Opération frauduleuse carte bancaire**

Faux placements

**Malwares, Ransomwares**

# THÉMATIQUES DE LA CONFÉRENCE


**Le vol ou la perte d'informations** 5

**Les attaques cybercriminelles** 9

- Phishing / Malware / Ransomware
- Autres attaques

**L'ingénierie sociale et les F.O.V.I.** 14

- Fraude Président
- Fraude au changement de coordonnées bancaires
- Fraude à l'informatique ou au faux technicien

**Les arnaques en ligne** 18

- Faux placements
- Arnaques aux remises de chèques suite à contact via les réseaux sociaux
- Escroqueries sentimentales
- Autres arnaques

# LE VOL OU LA PERTE D'INFORMATIONS

Le point de départ de nombreuses attaques…

# QUELQUES EXEMPLES

Cible :
Tous concernés

Vol d'information

Exemple : en 2013, David Cameron oublie sa mallette dans un train **avec la clé dessus**.

Cette "red box", remise à tous les ministres du gouvernement, leur permet de ranger leurs documents importants, **voire des secrets d'Etat**.

Fuite d'information

Espionnage industriel

**Vidéo : Un faux voyant lit vos secrets…**
https://www.youtube.com/watch?v=heRelQVLya4

# LE VOL OU LA PERTE D'INFORMATION

Cible :
Tous concernés

## Les données : Une aubaine pour les fraudeurs

La collecte d'information est la **première étape** pour les fraudeurs. Ils vont chercher par tous les moyens à **récupérer des informations** sur leurs cibles.

## Des risques grandissants

Ils vont utiliser **tous les canaux et techniques** pour voler les données : vol physique, espionnage, attaque informatique…

Dans un monde **hyper connecté,** leur **surface d'attaque** est encore plus grande et les risques toujours plus importants.

## Quelles conséquences ?

Plus les fraudeurs vont réussir à récupérer des informations, plus il leur sera facile **d'usurper votre identité** ou **celle de collaborateurs d'une entreprise.**

Ils pourront ensuite réaliser plusieurs attaques frauduleuses, notamment via **ingénierie sociale,** qui pourrait engendrer **une perte financière.**

Une fuite d'information pourrait également avoir un **impact considérable** sur la **réputation** d'une entreprise.

## Votre rôle au quotidien ?

Ne **communiquez pas** d'éléments susceptibles de faciliter le travail des fraudeurs

Maitrisez la **diffusion des informations** vous concernant et sur votre entreprise

Il est essentiel de bien respecter votre **politique de protection de l'information** mise en place en interne

# NOS PRÉCONISATIONS

Cible :
Tous concernés

## Vos mots de passe

- ✓ Définissez-les avec **précaution** (différents pour chaque accès, longs & complexes)
- ✓ **Changez-les** au moindre soupçon
- ✓ Ne les **partagez jamais**
- ✓ **Changez** les mots de passe par défaut


## La sécurité informatique

- ✓ Définissez une **charte** informatique
- ✓ Limitez le **téléchargement** sur les postes de travail
- ✓ **Méfiez-vous** des supports USB
- ✓ **Verrouillez** votre poste de travail

## Vos documents « papier »

- ✓ **Labellisez-les** selon leur criticité
- ✓ Conservez-les à l'abri des **curieux**
- ✓ Limitez les **impressions**
- ✓ Ne les jetez pas : **détruisez-les** !

## La sécurité physique

- ✓ **Contrôlez** l'identité des visiteurs
- ✓ **Encadrez** le personnel non permanent
- ✓ Ne les laissez **pas accéder** aux informations stratégiques

# LES ATTAQUES CYBERCRIMINELLES

Phishing / Malware / Ransomware

Autres attaques

# PHISHING / MALWARE / RANSOMWARE

Cible :
Tous concernés

## Phishing

Un fraudeur **se fait passer par email pour une entreprise, une banque ou une organisation crédible**

### L'objectif ?

Récupérer des **informations confidentielles**

Voire diffuser un **malware bancaire** ou un **Ransomware**

## Malware

**Virus** introduit sur un ordinateur par le biais d'un **email** avec pièce jointe, ou du **téléchargement d'un document ou d'un logiciel** depuis un site internet piraté.

### L'objectif ?

Récupérer à votre insu des **données personnelles souvent confidentielles**

Vous orienter **vers un site frauduleux** lors de votre **connexion à votre banque à distance**

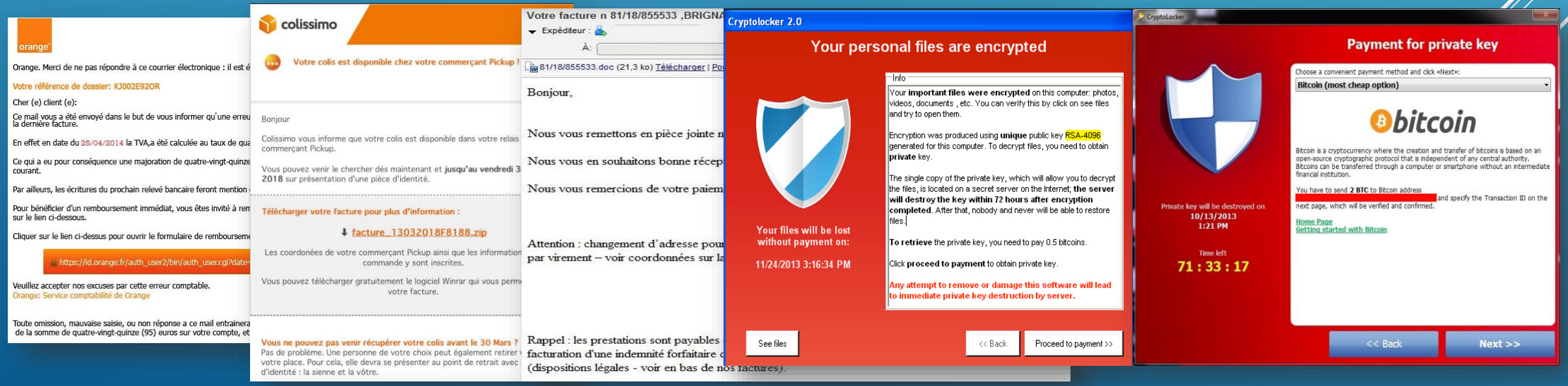
## Ransomware

**Malware** dont le but est de chiffrer des données afin de demander au propriétaire de l'ordinateur **d'envoyer une rançon en échange de la clé qui permettra de les déchiffrer**

### L'objectif ?

Récupérer une **rançon**

A noter que le paiement se fait le plus souvent en cryptomonnaie, principalement en **Bitcoin**



# QUELQUES EXEMPLES D'ATTAQUES RECENTES

Cible :
Tous concernés

## Eurofins Scientific

La Rédaction, 4 mars 2020, 13:00

RANSOMWARE SÉCURITÉ

**Eurofins Scientific, groupe de services, a révélé le coût d'une attaque de rançongiciel sur son sytème d'information en juin dernier : 69 millions € sur son chiffre d'affaires et à 75 millions € sur l'Ebitda.**

Quel est l'impact financier d'un ransomware ? Récurrente, la question trouve une multitude de réponses selon le périmètre d'activité de l'entreprise rançonnée et la période d'immobilisation du système d'information.

La publication des résultats annuels d' Eurofins Scientific, groupe de services d'analyses pour la pharmacie, l'agroalimentaire et l'environnement, donne l'occasion de chiffrer les conséquences : « l'impact de cette cyberattaque s'est élevé à 69 millions d'euros sur le chiffre d'affaires et à 75 millions d'euros sur l'Ebitda. » communique la société.

Survenue le 2 juin 2019, l'attaque au rançongiciel avait été estimée respectivement à 62 millions € et à 51,5 millions € lors de sa découverte.

### Arrêt temporaire de la production

Elle «a touché de façon sévère plusieurs laboratoires du groupe, réduisant ou arrêtant temporairement la production», a précisé Gilles Martin, le PDG du groupe, cité dans le communiqué.

## Bouygues Construction : Maze est-il le plus dangereux des ransomware ?

Clément Bohic, 6 février 2020, 17:35

RANSOMWARE SÉCURITÉ


**L'ANSSI considère Maze, qui a touché Bouygues Construction, comme le ransomware ayant le plus fort impact potentiel sur les entreprises. Pour quelles raisons ?**

Voilà bientôt une semaine que Bouygues Construction a annoncé avoir été victime d'une « attaque virale de type *ransomware* ».

Vendredi 31 janvier, le groupe français avait fait état de cet incident qu'il disait avoir détecté la veille. Il affirmait avoir mis son système d'information à l'arrêt pour éviter toute propagation.

Le dernier communiqué, daté du 5 février, ne va pas beaucoup plus loin. Message principal : la restauration du SI se poursuit, avec des mesures spécifiques pour assurer la continuité des activités. On n'en sait toutefois pas plus sur l'avancée des négociations autour de la rançon de 10 millions d'euros qui aurait été réclamée à Bouygues Construction.

À la même date, l'ANSSI a actualisé le rapport « État de la menace rançongiciel » qu'elle avait publié à l'occasion du FIC. Elle a enrichi l'annexe relative au *ransomware* qui a touché Bouygues Construction.

Sources :
https://www.silicon.fr/ransomware-75-millions-e-perdus-pour-eurofins-scientific-335439.html
https://www.silicon.fr/maze-bouygues-construction-rancongiciel-333830.html

# AUTRES ATTAQUES

Cible :
Tous concernés

## Déni de Service (DDos)

**Les principaux préjudices :**

- Pertes financières
- Paralysie de l'activité d'une entreprise
- Risques réputationnels

## Spear Phishing

## Pharming

## Clés USB et support amovibles infectés

**Liste (malheureusement) Non exhaustive…**

# NOS RECOMMANDATIONS

## Etre vigilants à la réception d'emails

- Ne jamais répondre à un email sollicitant la communication d'informations personnelles
- Ne pas ouvrir les pièces-jointes en cas de doute
- Ne pas cliquer sur les liens contenus dans un email dont ont ne connait pas l'expéditeur

## Protéger son ordinateur et le parc informatique de son entreprise

- Disposer d'un système d'exploitation, d'un antivirus et d'un pare-feu à jour
- Installer en complément un logiciel contre les malwares bancaires
- Effectuer des sauvegardes régulières des systèmes et données informatiques importantes

## A propos des applications bancaires

- Se connecter régulièrement à son application de banque à distance, vérifier la dernière date de connexion, votre relevé de compte et se déconnecter via le bouton « déconnexion »
- Ne jamais partager les identifiants de connexion (données strictement confidentielles)
- Entreprises : effectuer une ségrégation des pouvoirs

# L'INGENIERIE SOCIALE ET LES F.O.V.I.

La fraude Président

La fraude au changement de coordonnées bancaires

Autres attaques

# QUELQUES CHIFFRES SUR LES F.O.V.I. (FAUX ORDRES DE VIREMENTS INTERNATIONAUX)

Cible :
Surtout les entreprises

Préjudice unitaire de **quelques milliers d'euros** jusqu'à **plusieurs dizaines de Millions d'euros**

De 2010 à 2019 pour les entreprises françaises :

**720 Millions d'euros** de pertes cumulées

**Plus de 2 880 victimes** pour **4 260 faits**

**+ de 1,6 Milliard d'euros** de tentatives

*Source : O.C.R.G.D.F. / Octobre 2019*
*(Office Central pour la Répression de la Grande Délinquance Financière)*

# LES PRINCIPAUX TYPES D'ATTAQUES

Cible :
Surtout les entreprises

## Fraude au Président

**Appel téléphonique**, fax et/ou email

**usurpant l'identité** d'une personne influente de l'entreprise / structure

demandant avec **insistance**, à l'un des collaborateurs de cette entreprise / structure,

la réalisation d'une **transaction exceptionnelle et confidentielle**

## Fraude au changement de coordonnées bancaires

Escroc qui fait croire à un **changement de domiciliation bancaire**

d'un créancier légitime de l'entreprise / structure pour les **prochains règlements**

de loyers ou de factures

## Fraude à l'informatique ou au faux technicien

Escroc qui se fait passer pour un **technicien prestataire** de l'entreprise / structure visée

et tente d'obtenir par le collaborateur l'exécution de **« virements tests »**.

Il peut aussi demander **l'installation de logiciels**

qui permettront de **récupérer des informations** de sécurité ou de **pirater** le système informatique

## Le déroulement d'une attaque

- **Etape 1 : Collecte d'informations et élaboration d'un scénario d'attaque**
- **Etape 2 : Prise de contact**
- **Etape 3 : Demande de virement / changement de coordonnées bancaires / Test bancaire ou d'installation d'un logiciel**

# NOS RECOMMANDATIONS

**Définir et respecter les procédures**
pour l'exécution de virements bancaires mais aussi pour les contacts avec les banques / fournisseurs ainsi que leurs interlocuteurs

**Effectuer les vérifications indispensables**
(légitimité de la demande, rapprochements bancaires quotidiens)

**Limiter la communication d'informations**

**Etablir une ségrégation des pouvoirs sur les applications bancaires**
(et maintenir la liste des utilisateurs et droits à jour)

**En cas de doute ou de suspicion de fraude : communiquer !**
(contacter le fournisseur en cas d'une demande de changement de coordonnées bancaires afin d'être sûr qu'il est bien à l'origine de la demande, escalader en interne auprès de son manager, auprès de la Banque et des services de Police)

**Etre vigilant** (résister aux tentatives d'intimidation et à la pression psychologique)

**Sensibiliser les collaborateurs**
…à leur arrivée et tout au long de leur parcours
(la formation est un travail continu)

**Définir des règles de gestion des incidents/fraudes**
et réagir sans délai en cas de fraude en contactant sa banque puis en déposant plainte auprès des services de Police

# LES ARNAQUES EN LIGNE

Les faux placements

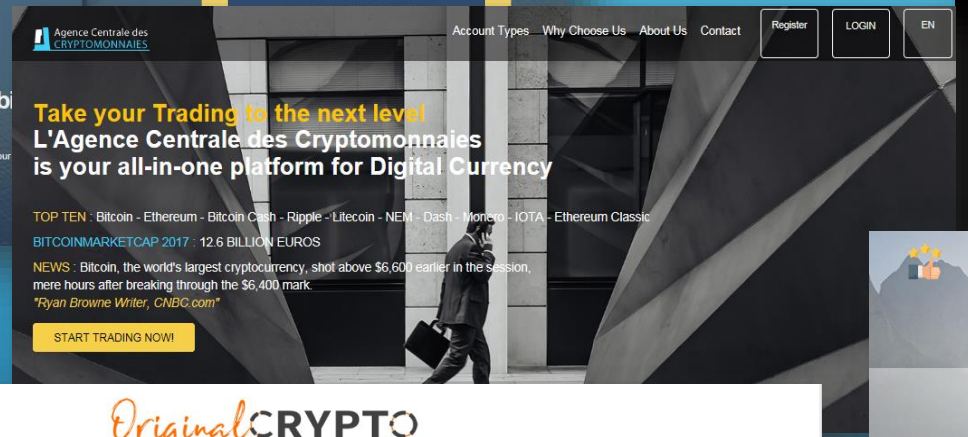
Les arnaques aux remises de chèques suite à contact via les réseaux sociaux

Les escroqueries sentimentales

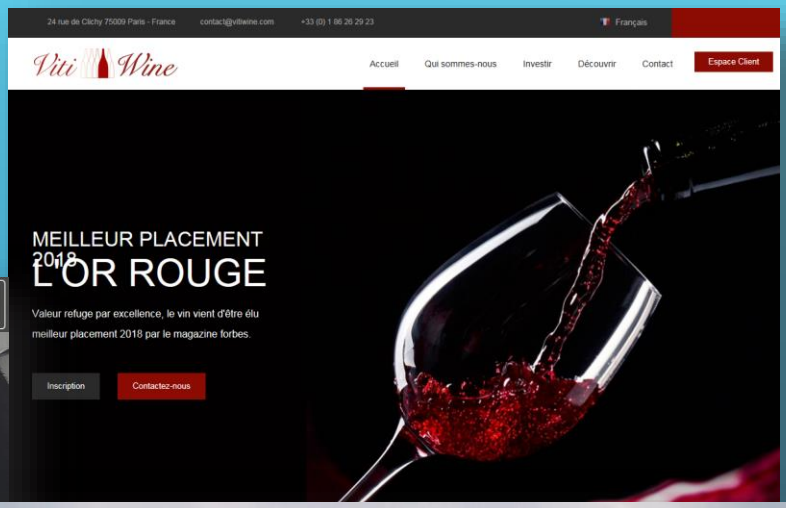
Autres arnaques

# LES FAUX PLACEMENTS

Cible :
Surtout les particuliers







1700000
vaches laitières en France

65000
exploitations réparties dans le territoire

12%
de rendement possible

**Le concept est assez simple** et bénéfique pour tout le monde: l'investisseur bénéficie d'un rendement aux alentours de 6 à 12 % par an, tandis que l'éleveur n'a pas à s'endetter pour acheter son troupeau.

## Comment ça marche ?

L'investisseur achète des vaches (1530 euros par vache)

Il s'adresse a un simple régisseur qui les loue pour lui a un éleveur sélectionné.

L'éleveur fournit le travail, les bâtiments, le matériel et les sols.

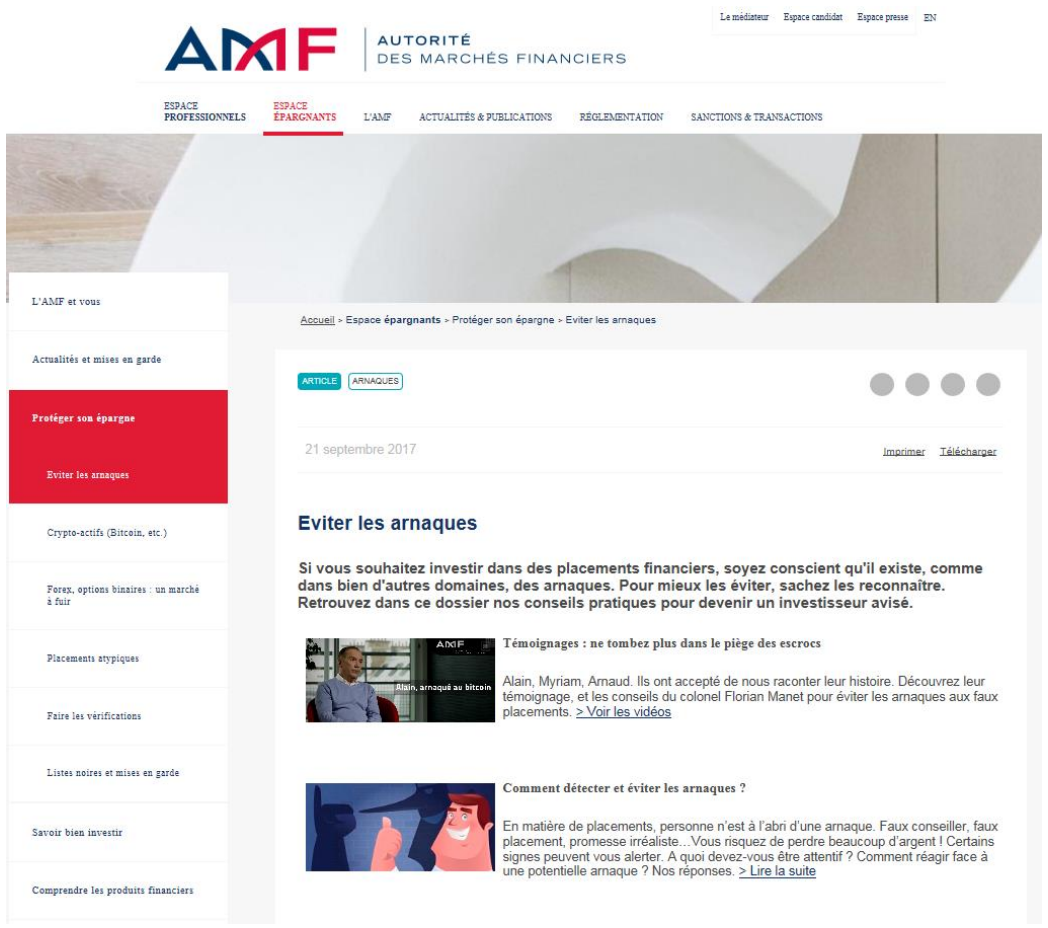
Le propriétaire perçoit chaque année environ 4 a 5% de son cheptel

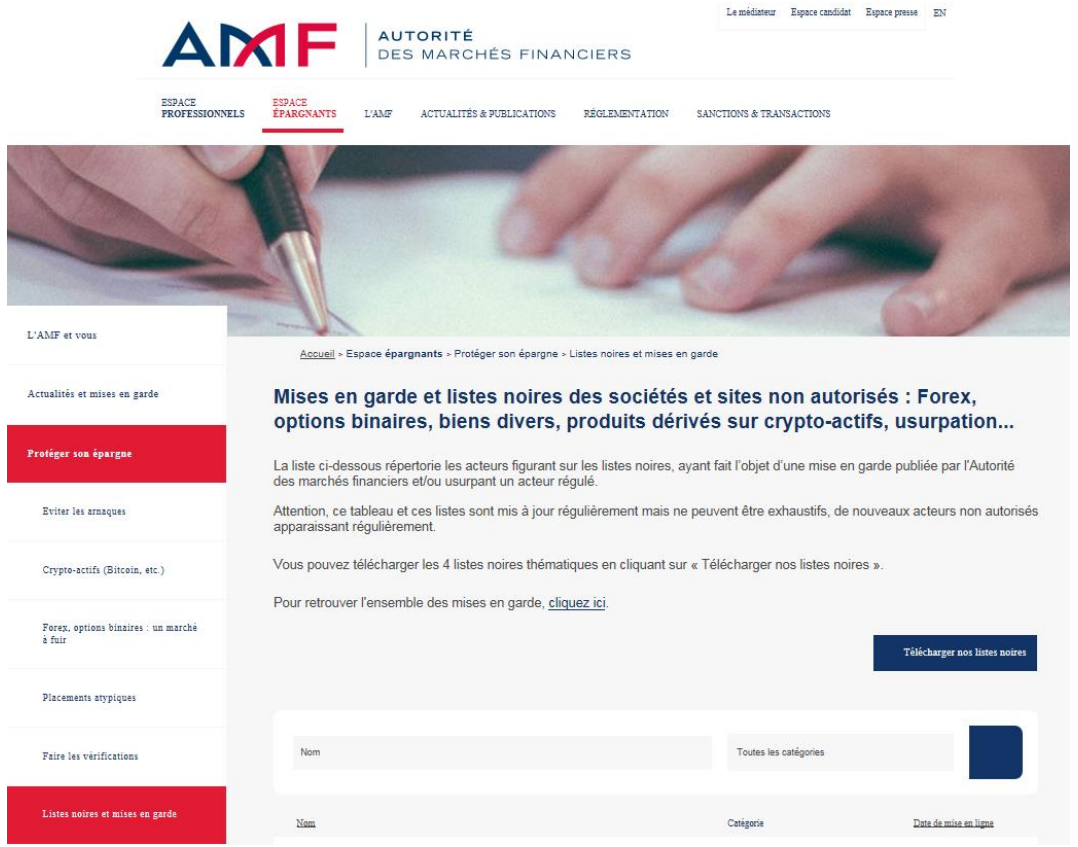
**Construisez un cheptel pour votre famille enfants et petits enfants.**

# LES FAUX PLACEMENTS

Cible :
Surtout les particuliers

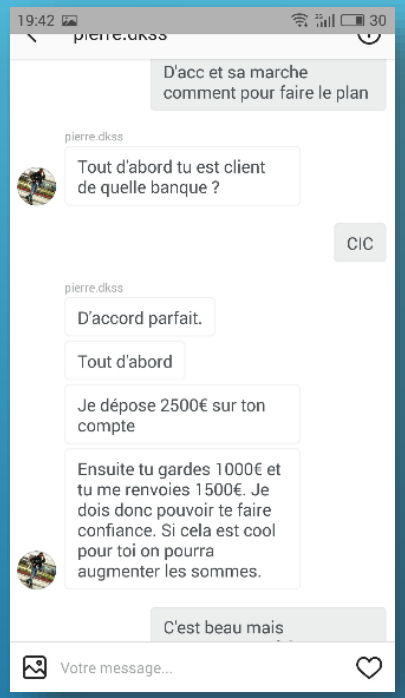
**Malheureusement, les sites d'investissement étaient faux et référencés dans la liste noire des sites d'investissement de l'AMF**

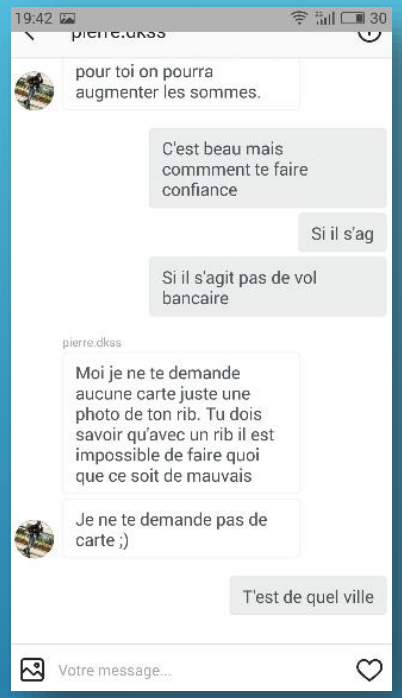


# LES ARNAQUES AUX REMISES DE CHEQUES SUITE A CONTACT SUR LES RESEAUX SOCIAUX

Cible :
Surtout les particuliers


**Les principaux préjudices :**

- Pertes financières (les chèques revenant impayés)
- Responsabilité du particulier engagée (encaissement d'un chèque pour autrui)

- L'interlocuteur a prétexté une **impossibilité** d'utiliser son compte bancaire.
- Il a alors proposé de réaliser des opérations telles que des dépôts de chèques via **le compte bancaire de la victime** en échange d'une **compensation financière**.

# LES ESCROQUERIES SENTIMENTALES

Cible :
Surtout les particuliers

**Clip de prévention : arnaques aux sentiments sur Internet**

https://youtu.be/g92SmyD13X0?list=PLWicS46zmIk17eWTCwbfAnHSVvnQ4d8_W


Clip de prévention : arnaques aux sentiments sur internet (version longue)

**Le mode opératoire :**

- L'escroc gagne **la confiance** de la victime en dévoilant **rapidement des sentiments** à son égard
- Il va ensuite demander de **l'argent**, des **cadeaux**…
- Si la victime n'envoie pas l'argent, le fraudeur peut se montrer **insistant** et lui **faire du chantage** (en s'appuyant sur des photos privées ou des informations confidentielles)

# AUTRES ARNAQUES

Cible :
Surtout les particuliers

## Faux crédits immobiliers

**Les principaux préjudices :**

- Pertes financières
- Usurpation d'identité (en cas d'envoi des justificatifs d'identité, revenu et domicile)

## Fausses annonces en ligne

## Sextorsions

## Locations saisonnières

**Liste (malheureusement) Non exhaustive…**

# NOS RECOMMANDATIONS

## Rester vigilant et détecter les promesses irréalistes

- Toujours se méfier des offres trop attractives
- Ne pas cliquer sur les liens contenus dans un email dont l'expéditeur est inconnu

## Avant d'investir des vérifications s'imposent

- Consulter la liste noire des sites d'investissement frauduleux de l'AMF ainsi que les recommandations essentielles avant d'investir
- S'assurer que le site et le conseiller soient enregistrés dans les fichiers des autorités
- Vérifier l'offre d'un prétendu établissement financier en se rendant en agence (et surtout pas celle figurant sur l'offre frauduleuse)

## En cas de doute

- Ne communiquer aucun document ou information confidentiel
- N'effectuer aucun transfert d'argent à la demande d'inconnus !
- Ne pas déposer des chèques pour le compte d'inconnus et ne pas communiquer ses coordonnées bancaires pour leur permettre de le faire directement via leur compte

# POUR CONCLURE

Le rôle du banquier

Ressources utiles

# LE RÔLE DU BANQUIER

1. **Connaître et être sensibilisé aux principales menaces**

2. **Accompagner et conseiller les clients sur les risques de fraude et cybercriminels**

3. **Faire preuve de vigilance au quotidien**

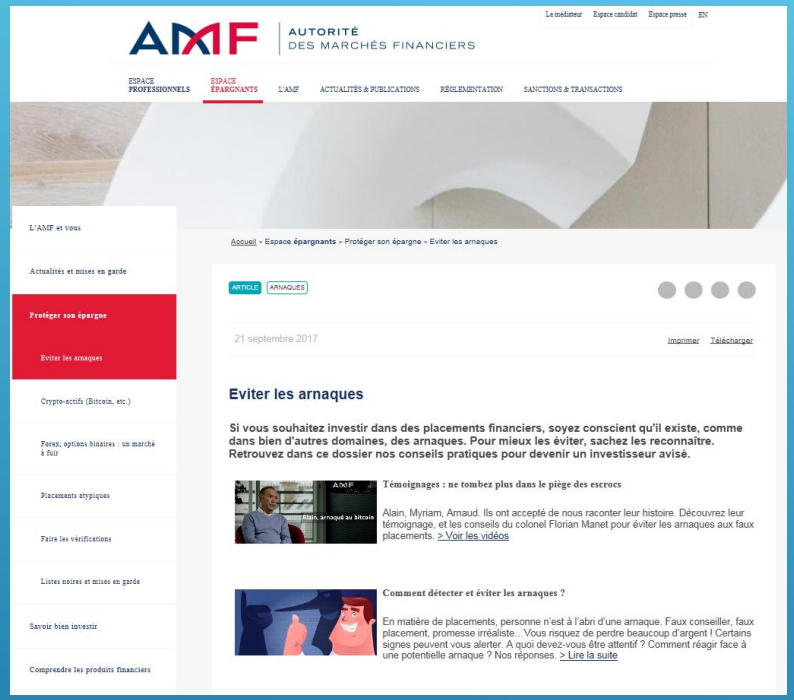
   (Entrée en relation de nouveaux clients, opérations inhabituelles…)

4. **Réagir au plus vite en cas de fraude**

# RESSOURCES UTILES

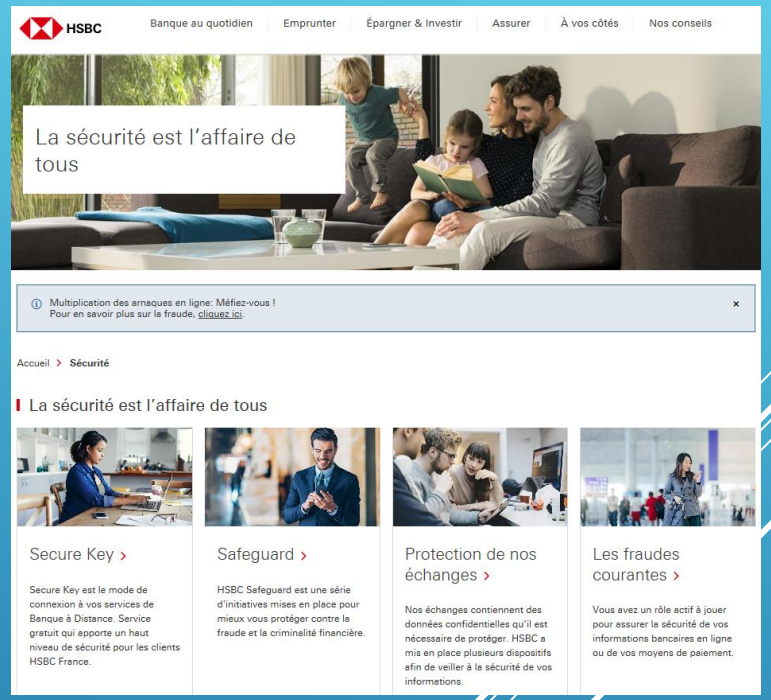

**Le site Cyber malveillance**

https://www.cybermalveillance.gouv.fr




**Le site de l'AMF**

https://www.amf-france.org/fr




**Les sites institutionnels des banques**

A titre d'exemple :
www.hsbc.fr/securite
https://www.business.hsbc.fr/fr-fr/securite