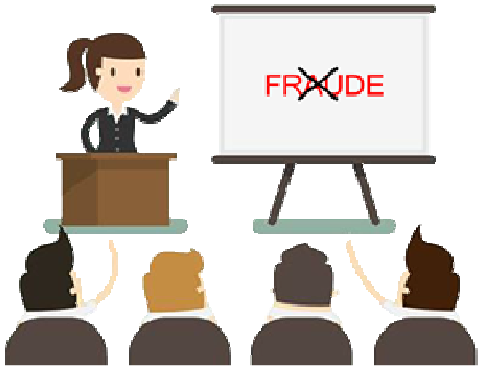
PRÉVENTION
DES FRAUDES BANCAIRES
PAR INGÉNIERIE SOCIALE

Isabelle HARDOUIN

Société Générale

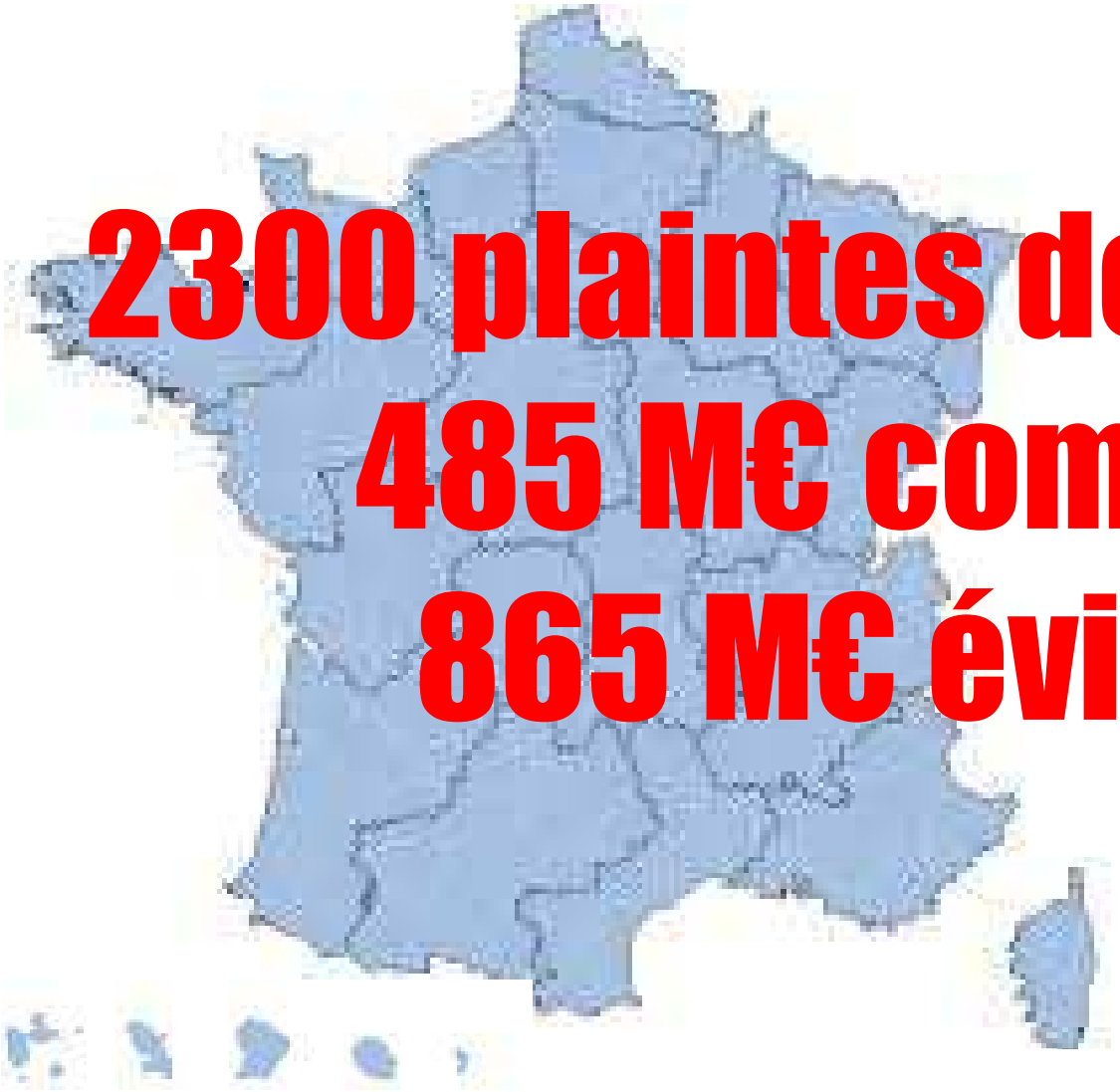
Paiements & Cash Management Régional



SOCIETE GENERALE

DEVELOPPONS ENSEMBLE
L'ESPRIT D'EQUIPE

Selon l'OCRGDF : les fraudes par ingénierie sociale depuis 2010, c'est…



2300 plaintes déposées
485 M€ commis
865 M€ évités

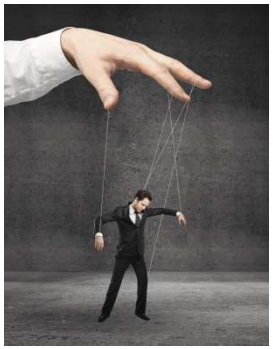
Des conséquences financières, (notamment pour les PME / TPE pouvant aller jusqu'à des redressements ou liquidations judicaires) mais aussi sociales et humaines :

- licenciement du comptable,
- conflits sociaux,
- suicide ...

Qu’est-ce que l’ingénierie sociale ?

Forme de délinquance astucieuse qui consiste à manipuler une personne en lui faisant croire qu’elle a affaire à un interlocuteur légitime, en vue de lui faire réaliser une action ou une opération (ex.: un virement bancaire)

EXEMPLES



Novembre 2014 :
Sur demande d’une personne usurpant l’identité de son PDG et d’un cabinet d’avocat, une comptable a ordonné **13 virements** vers l’étranger pour un montant de **1.275.000 €** étalés sur une durée de **35 jours**.

Janvier 2016 :
une « fraude au président » entraîne la liquidation judiciaire d’une société spécialisée dans la fabrication de meuble de bureau et de magasin.
42 salariés se retrouvent sans emploi. L’entreprise a deux mois pour clore le carnet de commandes.

Les outils des fraudeurs, en synthèse

• **Collecte d'informations publiques** sur les sites internet de l'entreprise, Infogreffe, les sites sociaux des collaborateurs (Facebook, Tweeter…), les réseaux professionnels (Viadeo, Linkedin..)

☞ Objectif : Identifier les fonctions dans l'entreprise et obtenir des informations personnelles ou professionnelles sur les individus clés, et l'entreprise elle-même

☞ A retenir : Limiter la diffusion d'information sur Internet

• **Plateforme de dématérialisation téléphonique**

• **Outil ou service Internet de téléphonie**

• **Service de télécopie par Internet**

• **Outil d'envoi de mail**

☞ Objectif : Usurper une identité en affichant un numéro d'appel ou un numéro de télécopie français, ou l'adresse mail légitime de la victime.

☞ A retenir : Ne pas accorder sa confiance sur la seule base d'informations affichées !

• **Service Internet ou outil de prise de main à distance d'un ordinateur**

☞ Objectif : Consulter l'écran de la victime ou effectuer des opérations à sa place

☞ A retenir : Ne jamais donner le contrôle de son ordinateur sans avoir vérifié l'identité du demandeur et la légitimité de la demande. Sécuriser le système d'information de l'entreprise

Exemples de fraudes

LA FRAUDE AU PRÉSIDENT :

- Le principe : Usurper l'identité d'un donneur d'ordres pour exiger d'un collaborateur qu'il effectue un virement frauduleux, en prétextant l'urgence et la confidentialité
- Méthode : en se faisant passer pour un haut responsable de l'entreprise, l'escroc place le collaborateur en position de subordination hiérarchique. En position de force dans la relation, l'escroc dispose de puissants ressorts pour manipuler sa victime. Il fait alors usage de l'autorité qu'on lui suppose « c'est un ordre que je vous donne là » tout en valorisant le collaborateur « je vous fais confiance ».

LE FAUX TEST DE VIREMENT :

- Le principe : Se faire passer pour le service télématique d'une banque et prétexter des tests de compatibilité avec l'entreprise cliente pour demander à la victime d'effectuer un virement bancaire.
- Méthode : Pour faciliter la fraude, l'escroc peut suggérer à la victime de lui laisser prendre la main sur son ordinateur. Il utilise alors un site de support informatique permettant de voir tout ce qui se passe sur l'ordinateur distant, et même prendre le contrôle.

Exemples de fraudes

LA FRAUDE AU CHANGEMENT DE COORDONNEES BANCAIRES :

- Le principe : Prétexter un changement de coordonnées bancaires pour diverses raisons : délocalisation, problème de compte, etc. afin d'ordonner à la victime d'effectuer un virement à l'étranger.
- Méthode : L'escroc, via un e-mail en provenance d'un fournisseur ou à caractère officiel, prétend un changement de coordonnées bancaires pour ordonner un virement frauduleux. Le fraudeur peut notamment joindre dans son mail une facture à l'appui de sa demande et dont le nouveau RIB figure dessus. Ce mode opératoire peut toucher les entreprises locateurs de société de gestion immobilière : escroquerie au bail locatif (cf scénario type). Il peut aussi s'agir de fausses factures, escroquerie connue sous le nom « F.O.V.I. à la nigériane » (cf. scénario type)

TROYEN BANCAIRE :

- Le principe : Envoyer un fichier contaminé contenant le cheval de Troie pour permettre à un pirate d'accéder à votre poste de travail.
- Méthode : Une fois le programme installé sur votre ordinateur, le pirate peut, par exemple, voler vos mots de passe et/ou identifiants, copier des données sensibles, prendre le contrôle de votre poste de travail pour se connecter à vos outils de banque à distance et exécuter des ordres de paiements…

Ce qu'il faut retenir …

FRAUDE AU PRÉSIDENT :

- Demande urgente et confidentielle
- Virement inhabituel (montant important vers un compte inconnu ou un pays avec lequel l'entreprise n'a aucune activité)
- Demande exceptionnelle ne respectant pas les procédures internes.

FAUX VIREMENTS :

Les demandes de tests sont toujours à l'initiative du client, qui en choisit lui-même ses caractéristiques (N° de comptes bénéficiaires et montants)

Ainsi, Société Générale ne sollicite jamais un client afin de :

- Réaliser des virements tests ;
- Communiquer des informations confidentielles par téléphone ou e-mail (en particulier : identifiant et mot de passe) ;
- Prendre le contrôle de son PC.

CHANGEMENT DE RIB :

- La demande émane-t-elle bien de votre relation ?
- S'interroger sur la nouvelle domiciliation bancaire: est-elle située à l'étranger ?

TROYEN BANCAIRE :

- Alerte de l'antivirus ou message d'erreur de l'antivirus (Antivirus désactivé) après ouverture d'une pièce jointe
- Demande intempestive de validation d'un ajout de compte tiers

LA LUTTE CONTRE

L'INGENIERIE SOCIALE

Prévention dans les entreprises

Sensibiliser largement le personnel susceptible d'être contacté par les escrocs

- Connaissance des interlocuteurs (clients, fournisseurs, partenaires) ;
- Esprit critique ; exercice du droit d'alerte ;
- Valoriser les tentatives de fraudes stoppées.

Culture Risque

Limiter la diffusion d'informations

- Réseaux sociaux professionnels (LinkedIn…), et personnels (Facebook) ;
- Sites internet de l'entreprise ;
- Modèles de fax de l'entreprise ;
- Signatures manuscrites des dirigeants autorisés à valider les opérations (y compris sur les sites internet de l'entreprise).

Ne pas se contenter des informations affichées

- Falsification de l'adresse mail apparente de l'expéditeur ;
- Falsification du numéro appelant qui s'affiche sur votre téléphone.

Sécuriser le système d'information

- Protéger les postes de travail : Antivirus à jour, correctif de sécurité (ex.: Windows Update, Acrobat) ;
- Protéger les points d'accès internet : Firewall, analyse antivirale des fichiers téléchargés, antivirus de messagerie, filtrage des pièces jointes …
- Sensibiliser les utilisateurs ;
- Auditer régulièrement la sécurité du système d'information

A traiter avec votre service informatique !

Prévention dans les entreprises

Mettre en place des procédures internes sécurisées :

- Processus clairs et formalisés ;
- Ségrégation des rôles :
  - dissocier saisie et validation des ordres (virements, déclaration de BIC/IBAN) ;
- Contrôles réguliers (respect des procédures, vérifications des comptes...) ;
- Accès limité aux données et applications sensibles

Sécuriser les virements bancaires :

L'ingénierie sociale a pour but la réalisation de virements frauduleux, il convient de :

- **Proscrire les virements papier / fax** (moyen de paiement avec lequel le risque de faux est élevé)
- Privilégier les canaux automatisés : Web banking, Protocoles bancaires (Ebics, SWIFTNet…) en respectant strictement toutes les consignes de sécurité afférentes à ces outils
- Communiquer lors d'un rendez-vous avec la banque : les noms, signatures, fonctions et coordonnées des personnes à joindre en cas de doute sur des opérations bancaires.

Conduite à tenir dans les entreprises

1. **Savoir résister à la pression, avoir un sens critique ;**
2. **Respecter les procédures internes ;**
3. **Vérifier la légitimité de la demande :**
    - **Contre-appel vers un numéro déjà référencé,** voire vers plusieurs personnes
    - **Toute autre méthode validée par votre entité**
4. **Ne pas se laisser isoler :**
    - Ne pas hésiter à faire appel à un collègue ou un responsable.

En cas de fraude avérée ou supposée

Alerter un responsable interne

ET la(es) banque(s) et les autorités de police compétentes

QUE FAIRE EN CAS DE FRAUDE DETECTEE :

La récupération des fonds dépend des actions engagées simultanément par plusieurs acteurs (BANQUE / ENTREPRISE / POLICE).

ENTREPRISE :

- **prévenir la banque** pour qu'elle demande immédiatement le blocage des fonds à la banque destinataire du virement frauduleux
- **déposer plainte en France auprès des autorités compétentes et selon le cas, à l'étranger** auprès de la police locale (indispensable en Chine ou Pologne) pour confirmer la demande de gel des fonds
- **procéder à un contrôle complet du système informatique** (vérification de présence de logiciels malveillants …)

BANQUE :

- appliquer la « procédure de récupération des fonds »
- solliciter le réseau TRACFIN (sans mentionner l'ouverture d'une procédure judicaire)
- renforcer la sécurité du compte et des contrats Banque à Distance du client (changement codes confidentiels …)

POLICE :

- demande de gel des fonds par l'intermédiaire d'Europol / Interpol et de l'attaché de sécurité intérieure dans le pays destinataire
- officialisation de cette demande par une ordonnance de saisine pénale des fonds, délivrée par un magistrat et collecte de renseignements sur le titulaire du compte à l'étranger et la destination finale des fonds (par Demande d'Entraide Pénale Internationale ou Commission Rogatoire Internationale)

Le temps qui passe joue pour les escrocs … !

Services de police compétents en matière d'ingénierie sociale

Sur Paris et petite couronne (départements 75, 92, 93 et 94) :

Brigade des Fraudes aux Moyens de Paiement (BFMP)

Commandant Fonctionnel Bernard HENRY, adjoint à la chef de service, 01 55 75 23 14.

Commandant Philippe LAURENT, 01 55 75 23 08.

122-126 Rue du Château des Rentiers

75013 PARIS

Compétence nationale :

Office Central pour la Répression de la Grande Délinquance Financière (OCRGDF)

101 Rue des Trois Fontenot

92 000 NANTERRE

Secrétariat : 01 40 97 84 17

En province :

Sûreté départementale ou Brigade de Sûreté Urbaine
Police Judiciaire

Supports de sensibilisation

FEDERATION BANCAIRE FRANCAISE : http://www.lesclesdelabanque.com

Conclusion

- **Les tentatives de fraudes ne peuvent pas être évitées**
- **Les fraudeurs sont de plus en plus inventifs et organisés**

Mais les impacts peuvent être limités

grâce à la vigilance de chacun au quotidien

Merci pour votre attention