WHO SHOULD YOU CONTACT?

POLICE SERVICES IN CHARGE OF SOCIAL ENGINEERING CRIMES IN FRANCE:

- **Paris and inner suburbs (departments 92, 93 and 94)**

  Brigade des Fraudes aux Moyens de Paiement (BFMP)
  122 – 126 rue du Château des Rentiers
  75013 PARIS

  Receptionist: **+33 (0)1 55 75 22 94**

- **National contact**

  Office Central pour la Répression
  de la Grande Délinquance Financière (OCRGDF)
  101, rue des Trois Fontanot
  92000 NANTERRE

  Receptionist: **+33 (0)1 40 97 84 17**

- **Others**

  Service Régional de Police Judiciaire (SRPJ) or Brigade de Recherches of the Gendarmerie Nationale (outside of Paris)

If you are suspicious, don't hesitate to contact your usual Societe Generale customer adviser.

SOCIETE GENERALE

Banque & Assurances

Société Générale - BDDF/DCM/CCM Tour Granite 75886 PARIS CEDEX 18 - S.A. au capital de 998 320 373,75 EUR - 552 120 222 RCS PARIS. Siège social : 29, bd Haussmann 75009 PARIS - Crédit photos : Samuel Melo - GettyImages - SG - 10/2013

Société Générale adhère à Ecofolio et participe au financement du recyclage des papiers. Ce document a été conçu par Société Générale dans le souci d'une incidence minimale sur l'environnement et imprimé sur du papier issu de forêts gérées durablement.

PREVENTING BANK FRAUD
caused by social engineering

DEVELOPPONS ENSEMBLE

L'ESPRIT D'EQUIPE SOCIETE GENERALE

Don’t forget:

INFORMATION SECURITY IS EVERYONE’S BUSINESS!

Fraudsters prey on a company’s weaknesses, such as a lack of coordination between the different teams involved in a process:
if you are suspicious about something don’t hesitate to contact your customer adviser at Societe Generale.

Social engineering

is defined as the «art» of manipulating people into performing an action or divulging information.

Fraudulent behaviour is nothing new; scams, cons and embezzlement have always been a part of any economy.

What are new, however, are the technical resources and means of communication (email, social networks) available to the general public, which fraudsters use to launch a variety of complex attacks.

What’s more, the sentences faced by cybercriminals are limited compared to more «traditional» offences.

Lastly, the international dimension of these crimes makes it very difficult for the police to carry out investigations and arrest the perpetrators.

Banks were the first structures to have been targeted by this type of fraud. However, these attacks are now targeting French companies, their foreign subsidiaries and the French operations of foreign companies (finance departments, in particular). Banks have had to contend with this problem for years and Societe Generale would like to raise its customers’ awareness of the issue.

Preventive measures

The best practices used in the fight against social engineering listed below are used by Societe Generale and are constantly being updated: for maximum effectiveness, we encourage you to apply them in your organisation.

1

SECURE YOUR PROCESSES AND TOOLS:

- Establish clear written procedures:
  - *If possible, automate Cash Management / Treasury processes*
- Secure access to applications and sensitive data:
  - *Limit user rights to the bare minimum*
  - *Consider using strong authentication systems for sensitive functions*
- Segregate duties:
  - *Separate order entry and validation responsibilities (transfers, BIC/IBAN statements)*
- Implement ongoing controls
  - *Compliance with procedures, checking of accounts, etc.*

2

SECURE YOUR EXCHANGES WITH THE BANK:

- Limit paper or fax transfers (where the risk of fraud is high)
- Use automated channels whenever possible (Sogecash Net, Sogecash Web, Ebics, SWIFTNet, etc.) and closely follow all their security recommendations (e-secure key, user rights, etc.)
- Use meetings with the bank to communicate the names, signatures, functions and contact information of authorised individuals and persons who should be informed in the event a suspicious transaction arises

3

RAISE YOUR EMPLOYEES' AWARENESS ABOUT APPROPRIATE BEHAVIOUR:

- Follow operating procedures and perform the planned verifications
- Know your client, supplier, partner, etc.
- Critical thinking - use your whistle-blowing power
- Don't trust appearances: fraudsters can easily manipulate systems in order to make their email address or telephone number look like someone else's
- Managers should applaud employees' efforts to halt fraud

FUNCTIONS MOST EXPOSED TO FRAUD:
corporate treasurers – accountants – staff using payment instruments

4

LIMIT THE SPREAD OF INFORMATION:

- Control the publication of information on the company's websites
- Recommend that employees do not share sensitive information on professional social networks (LinkedIn, etc.) and social media (Facebook, etc.)
- Limit access to sensitive documents, such as the company's letterhead
- Maintain the confidentiality of the hand-written signatures of corporate officers authorised to validate operations (including on company websites)

A FEW CASES OF SOCIAL ENGINEERING:
alert criteria and appropriate responses

The imagination of fraudsters is limitless and cases of social engineering have been increasingly frequent in the past few months. A few signs can tip you off...

ALERT CRITERIA

DEFRAUDING THE CEO

- Urgent and confidential request
- Unusual transfer (large amount, to an unknown account or to a country where the company does not do business)
- Exceptional request that does not follow internal procedures

FRAUDULENT SEPA TRANSFERS

Societe Generale never contacts clients to:

- Carry out test transfers.
- Communicate confidential information over the phone or by email (especially logins and passwords)
- Take control of their PC

PHONE LINE HIJACKING

- A site or department receives no phone calls for an abnormally long period of time
- Someone you know contacts you on your mobile to inform you that an unknown person is answering calls on your land line

HOW TO RESPOND TO AN UNUSUAL REQUEST

1. **Stand up to pressure and ask questions**
2. **Follow internal procedures**
3. **Check that the request is legitimate:**
   - *Call the person back on a number that you have in your files*
   - *Use any other method that has been approved by your entity*
4. **Don't get trapped alone**
   Don't hesitate to ask a colleague or superior for help

In the event of suspected or confirmed fraud:
Alert the appropriate manager in charge of fraud AND your bank(s)

DON'T FORGET!

- Fraud attempts are unavoidable in a normal commercial or industrial activity.
- Fraudsters are very creative, often very well organised and may also have very strong technical skills.

BUT...

- In addition to the technical solutions used by IT departments to thwart attacks, you can limit the impact of fraud by:
  - **having reliable internal processes and ensuring they are correctly followed**
  - **ensuring staff are on alert at all times**
  - **constantly sharing information (best practices, information on attacks averted, etc.).**