COMMISSIONS AFTE

Commission Systèmes d’information – Sécurité

Mai 2014

Preventing bank fraud

- Data protection
- Best practice
- Preventive measures

What is social engineering ?

- Art of manipulating people into performing an action or divulging information.
- **What is new ?** Technical ressources and means of communication (emails, social networks) available to general public which fraudsters use to launch a variety of complex attacks and to get information about people or the company.
- **What's more?** The international dimension of these crimes makes it very difficult for the police to carry out investigations and arrest the perpetrators.
- **Nowadays :** These attacks are now targeting many French companies, and their foreign subsidiaries (Finance department in particular)
- Don't forget : Information security is everyone's business. Fraudsters prey on a company's weakness : if you are suspicious don't hesitate to contact your hierarchy.

Corporate Treasurers -> raise entities' awareness of this issue.

Data proctection

Data protection 1/2

- It is not rare to receive emails from unknown people asking for personal information or to click on links. These attacks aim at the personal systems, we need to be very suspicious.

- Attacks of IT systems of the company are more and more frequent. The contents of these kind of emails are generally drafted to click a link or activate an attachment. It is necessary to be particularly watchful because once an attachment or a link sent by a hacker is activated, hostile programs can be installed and become a threat for systems.

The fraudsters can pirate email addresses : please be careful.

Data protection : Best practice to face email attacks

- **Sender :**
  - ✓ Do you know the sender? It is the usual one ? Does he/she often contact you ?
  - ✓ If your colleagues send emails from their professional address it is not normal that they use the personal one.

- **Link :**
  - ✓ Do not open a link from an unknown sender.
  - ✓ Do not click on link on your Iphone/Blackberry from unknown sender.
  - ✓ If the link seems to be suspect, do not click (Fanciful address, spelling mistake..).

- **Attachment :**
  - ✓ Do not open an attachment from an unknown sender.
  - ✓ If you need to open attachment, do it on your professional computer because it is protected again virus.

- **Text :**
  - ✓ Evaluate the quality of the text and images.
  - ✓ Spelling mistakes in the mother tongue of the sender need to arouse suspicious.

- **The reply, if everything feels like authentic :**
  - ✓ Am I authorized to communicate this information?
  - ✓ Does my correspondent needs this kind of information?
  - ✓ Do not give data, if the replies to the above question are YES. In case of doubt, please contact your hierarchy.

Have the appropriate reaction

Fraudsters ? Real experts !

- ✓ Don't forget that fraudsters are very creative, often very well organized and may also have very strong technical skills.
- ✓ They know perfectly how to imitate signatures
- ✓ They know how to falsify documents
- ✓ They know how to imitate voices, or emails
- ✓ They ask for a high level of confidentiality
- ✓ They have a good knowlegde of fragility of companies (buy or sell of one entity, top management changes, change of governance..)
- ✓ They have boldness, perseverance and the capacity to manipulate an interlocutor.

Best practice

Commission Systèmes d'information - Sécurité

A few signs can tip you off…

Alert criteria

- Defrauding the CEO
  - Urgent and confidential request
  - Unusual transfer (large amount, to an unkown accountor or to a country where the company does not do business)
  - Exceptional request that does not follow internal procedures
- Fraudulent transfers
  - Banks never contact clients to :
  - Carry out test transfers
  - Communicate confidential information over the phone or by email (especially login or password)
- Phone line hijacking
  - A site or department never receives phone calls from the CEO or the CFO.
  - Someone you know contacts you on your mobile phone to inform you that an unkown person is answering calls on your land line.
  - Carry out test transfers
  - Communicate confidential information by phone or by email (especially login or password)

The imagination of fraudsters is limitless and cases of social engineering have been increasingly frequent in the past few months.

Some examples of fraud

- False paper transfer order
- Urgent request by phone from the CEO or CFO to do a transfer for an acquisition which has to remain confidential.
- Ask the accounting department to execute a transfer abroad to unmask a swindler, acting as the manager of the company and specifying that this request returns within the framework of an investigation on fraud and that confidentiality must be insured.
- Request of modification of a bank account details of a supplier by phone, confirmed by a false email from a good address of the mentioned supplier.
- Urgent request of transfer by phone, with the use of a synthesizer of voice.
- Request of issuing a transfer to test files in the SEPA format : do not send file by email.
- Forgery of e-mails or paper documents by collecting information on the Internet website of the company (logo, address, fax, e-mail and the same signature as the managers).
- Use of technologies to reveal local telephone numbers while these calls emanate from foreign countries.
- Use of technologies to pirate email addresses (suppliers, managers of the company) while these messages emanate from email addresses of the fraudsters.

How to respond to an unusual request ?

- Stand up to pressure and ask questions
- Follow internal procedures
- Check that the request is legitimate :
  - Call the person back on a number that you have in your contact list or Outlook
  - Use any other method to verify that is the «good» person.
- 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 your manager AND your bank which did the wire.

Preventive measures

Best practice to fight against social engineering

- **Secure our processes and tools by automating Cash Management/Treasury processes :**
  - ✓ Secure access to applications and sensitive data : do not communicate password by mail, do not write password on post it or in file.
  - ✓ Segregate duties: separate order entry and validation responsabilities
  - ✓ Implement ongoing controls : checking bank details, compliance with procedure
  - ✓ Do not trash the sensitive information: signature, letterhead, template of paper transfer .. Please destroy it in the crusher.
- **Secure your exchanges with the bank :**
  - ✓ Limit paper or fax transfers where the risk of fraud is high
  - ✓ Use automated channels whenever possible (Allmybanks, Web-banking ..)
  - ✓ Inform your bank of persons who should be informed if a suspicious transaction arises
- **Awareness about appropriate behaviour :**
  - ✓ Perform verification and follow procedure
  - ✓ Don’t trust appearences
  - ✓ Know your client, supplier, partner etc …
- **Limit the spread of information** :
  - ✓ Control the publication of information on the company’s website
  - ✓ Do not share sensitive information on professionnal social networks and social media…
  - ✓ Limit access to sensitive documents, such as the company’s letterhead
  - ✓ Maintain the confidentiallity of the hand-written signatures of Corporate officers authorised to validate operations (including on company’s websites)

Functions most exposed to fraud : treasurers, accountants, staff using payment instruments.

Appendix : TO DO LIST

- **Centralized banking power :**
  - ✓ Modify, as soon as possible, the banking power once a person leaves your entity.

- **Paper transfers :**
  - ✓ Limit « paper transfer »
  - ✓ Use automated channels

- **Awareness about appropriate behaviour :**
  - ✓ Perform verification and follow procedure
  - ✓ Don’t trust appearences
  - ✓ Know your client, supplier, partner etc …

- **Limit the spread of information** :
  - ✓ Control the publication of information on the company’s website
  - ✓ Do not share sensitive information on professionnal social networks and social media…
  - ✓ Limit access to sensitive documents, such as the company’s letterhead
  - ✓ Maintain the confidentiality of the hand-written signatures of Corporate officers authorized to validate operations (including on company’s websites)