# CREDIT TRANSFER FRAUD

## TRAINING KIT

Impersonation fraud has caused losses of several billion euros all around the world – Have you taken steps to protect your business?

*Credit: Shutterstock*

BNP PARIBAS CASH MANAGEMENT
June 2018

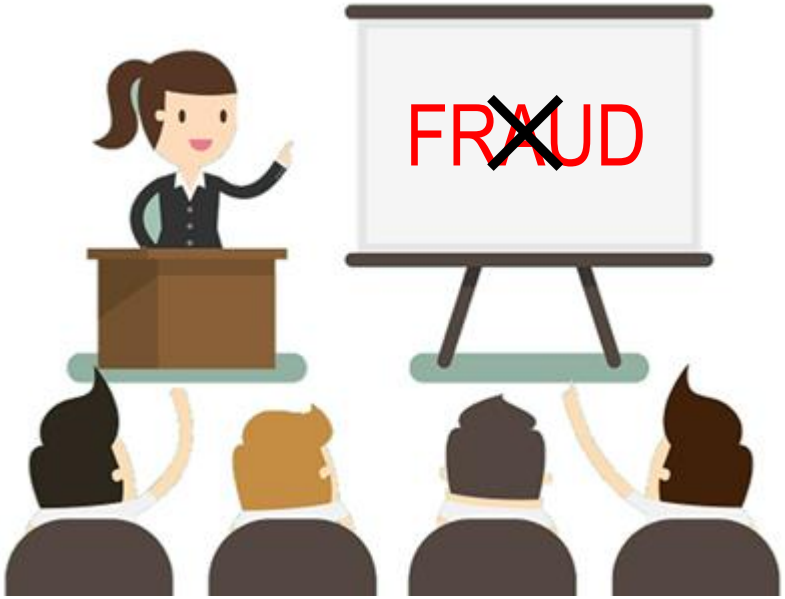
BNP PARIBAS

The bank for a changing world

# Make your staff aware of the dangers!

To guard against fraud, it is not enough to set up procedures, tools and controls.

**It is very important to keep your staff informed and to train them** so they can detect and counter fraud attempts and cyber attacks. The fact is that in almost all cases **fraudsters take advantage of human weakness.**




- **Hold regular training or awareness sessions**: don't simply rely on sending emails.
- **Train accounting and treasury staff, but do not hesitate to raise awareness amongst all employees** liable to be duped into giving information to fraudsters (assistants …) or installing malware on their PC.
- **Do not omit new arrivals, temporary employees, employees on fixed-term contracts**, etc. These are ideal targets.
- **Review your awareness sessions** at least once a year: the threats are constantly evolving and your staff must stay alert.
- **In addition to awareness sessions, provide very clear written instructions** to your employees.

This document contains sound advice and specific guidelines which you can adapt to your business and pass on to your employees.

*Credit: Shutterstock*

# The fake CEO scam

## EXAMPLE

**Click on the image to view the video:**


https://banqueentreprise.bnpparibas/rsc/contrib/video/dossiers/Hello_Here_Is_Your_Chairman.mp4

## THE WARNING SIGNS

- **A contact who does not usually call you** (an executive, a board member, a lawyer, etc.)
- **Urgency** of the situation (acquisition, fiscal inspection, etc.)
- **Secrecy** and confidentiality ("especially not to speak about it. Here is a telephone number for encrypting our conversations…")
- **Flattery** ("I am told that I can count on you")
- **Intimidation** ("Listen to me! It's urgent!")

## PROTECT YOURSELF

- **Check the identity of your contact** by reconnecting to him or her using particulars your are sure of, for example from the company directory (and not those sent by the contact). No blame will ever fall on you for this.
- **Check email addresses**: fraudsters sometimes use similar addresses (for example: john.smith@sale-team.com instead of john.smith@sales-team.com).
- **Tell your manager**: a well intentioned person would not ask you to conceal information from your managers.
- **Comply with the segregation of duties**
  - If you are allowed to make large payments by yourself, you are at risk. Talk to your manager (no one should have the three authorisations of creating a third party account, inputting a transfer and validating it).
  - Avoid transfer orders and validations by fax.
  - Means of authentication and signature are personal: never give them to colleagues, and refuse to accept them if they try to give you theirs.
  - Segregation of duties not only protects the business: it also protects you.
  - Management teams can warn teams they will never ask to execute urgent payments outside usual procedures.

## AND REMEMBER

- Fraudsters often know a great deal about a business and are able to imitate people's voices.
- If the scam fails, the fraudster can call the CEO himself pretending to be a police officer.

# The fake vendor scam (and fake landlord, fake factor…)

## EXAMPLE

An accountant receives a letter from a supplier, informing that all invoices should be paid to the bank account of a factor, domiciled in Poland. The accountant changes that IBAN in his supplier database. Several payments are made to Poland until the real supplier informs the accountant that he has not received any payment for the last 3 months.

In order to simplify our accounting organization and focus on improving our productivity, we entered into a factoring contract with:

*SCHELSER INVEST*
*info@factor-fr.eu*
*UL.M.J. PILSUDZKIEGO 3A*
*56100 WOLOW - POLAND*

Please pay to the order of
« SCHLESER INVEST »
NIP : 9880186621 Regon : 360233219

*BANK: BANK PEKAO*
*Pl. Bankowy 2, 00-950 WARSAW – POLAND*
*IBAN : PL87 1240 1037 1978 0010 5475 8017*

Before attacking you, the fraudster impersonated your identity and contacted your suppliers to steal invoices from them.

Fraudsters can use email addresses that resemble that of your provider, but also yours; They can thus intervene in all your exchanges of emails.

## THE WARNING SIGNS

- Any request for a **change of beneficiary account** (by mail, by email, on the invoice, by phone, etc.).
- Especially if the account is **domiciled in a foreign country**.

## PROTECT YOURSELF…

- **Look at email headers** to check sender's email addresses
- **Check the identity of your contact** by getting back in touch with him using particulars known to be accurate (and not those sent by the person)
- Do not wait until you should make the payment
- **Be suspicious if the new account is domiciled abroad**
  - ISO country code: first 2 letters of IBAN and 5th and 6th letters of BIC code.
  - Cyprus: **CY**17002001280000001200527600 - BIC: ABKL**CY**2N
  - France: **FR**7630046001290029721519546 -BIC: ABCD**FR**1N
- **Use two channels for accounts domiciled abroad** (for example, check the identity by e-mail and by phone).

**> Article: corporates' best practices**

## …AND YOUR CLIENTS

- **Check any request for your invoices,** tax information, etc. (beware of fake clients, auditors, tax inspectors, public administrations…)
- **Write to your clients** to inform them of vendor scam risks.
- **Protect your customer and supplier databases** against hacking.

**> Article: beware of invoice theft**

## AND REMEMBER

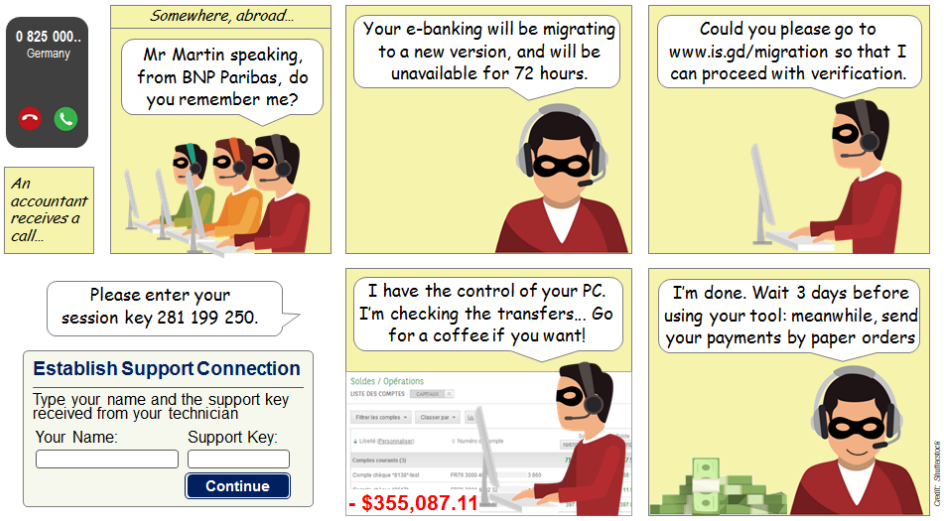
- The fake landlord and fake factor frauds are variations of this scam.
- At first, fraudsters generally steal invoices from the supplier, by email, mail, telephone, or computer intrusion.
- Some fraudsters hack the servers of companies to steal customer and supplier lists, in order to operate this type of scam.
- Fraudsters use registered letters.

**REGISTERED LETTER**

# The fake technician scam (bank, software vendor…)

## EXAMPLE

**Click on the image to enlarge the comic**




**A victim's story:**

https://banqueentreprise.bnpparibas/rsc/contrib/document/infos-com/Fake_technican_scam_client_story.pdf

## THE WARNING SIGNS

- **Someone offering to help you with your payment tools** when you have not personally asked for help
- **Questions about your payment tools or procedures**
- **A link you are not familiar with** (for example shortened URLs such as: www.id5.com/bnp, www.tin.com/sepa08, www.is.gd/sepabnp, www.tinyurl.com/migration, etc.)
- **A request to take control of your PC remotely**
- **A suggestion to do a test transfer**

## PROTECT YOURSELF

- **Contact your relationship manager** using the known particulars to check the identity of anyone claiming to be on our staff.
- **Refuse to allow your PC to be controlled remotely by anyone** whose identity is uncertain: do not go to an Internet address, do not click on a link.
- **Never do a test at the request of a technician**: do not credit a third-party account, do not confirm a transaction or transfer. Even on your own initiative, never do a test with more than €1.
- **Never give anyone any code** (e.g. number generated by your wireless reader, password, PIN code, etc.)
- **Protect your computer network and your PCs** against hacking and malicious software.

## AND REMEMBER

- No BNP Paribas technician will ever contact you to carry out an upgrade, maintenance, tests, etc., unless you have personally asked for assistance.
- Fraudsters can also claim to be with your software vendor.
- Scammers know banking systems very well; they are often familiar with current incidents and commercial operations, even the name of your relationship manager.
- All the better to dupe you, the fraudster can make preliminary calls during which he helps you without cheating you.
- If you are equipped with a wireless reader, the fraudster can say to you: "Don't tell me your PIN code, I'm not supposed to know it. Just give me the code displayed on your wireless reader".

# Fraud by malicious software (malware)

## EXAMPLE

An accountant receives an email from a supplier containing an invoice. When it is opened, malicious code installs malware on his PC. The malware creates a money transfer on his payment tool, and displays a fake validation page. Carelessly, the accountant enters his validation code. The malware then validates the transfer with the code.


**More about malware:**
https://banqueentreprise.bnpparibas/rsc/contrib/document/infos-com/Malware_alert_Protect_your_business.pdf

## THE WARNING SIGNS

- Any email from a known or unknown contact that has an **unusual subject or content**
- **An unusual validation page**, or some slowness or unavailability of your web banking tool

## PROTECT YOURSELF

- **Upon receiving an email**
  - Do you know the sender? Is it their usual address? Were you expecting this email? Is the subject or message unusual?
  - If in doubt, do not open attachments or links.
  - If you open an attachment, do it on a workstation protected by antivirus software, not on your smartphone.
  - Do not allow the auto-execution of macros.
  - Set your email software so that it does not open attachments automatically.
- **Protect your computer systems**
  - Use a recent and updated operating system and navigator.
  - Have an updated firewall, antivirus and malware detector.
  - Restrict software installation rights to administrators.
  - Distrust smart phones (usually no antivirus software installed) and personal computers in particular.
- **Use your payment applications properly**
  - Do not connect when hacking or malware is suspected.
  - Log off from your application after each session.
  - Remove your means of validation when finished using it.
  - Never disclose your ID, passwords, means of validation, etc. to anyone, by any means whatsoever.
  - Do not log on from a PC or private smartphone.
  - If possible, make your payments on a PC dedicated to that purpose.

## AND REMEMBER

- A fraudulent email could come from one of your usual contacts if his or her workstation has been infected. If in doubt, contact him or her.

# Good reflexes: use common sense!

## In case of unusual credit transfer requests

- Inform your hierarchy
- Check your correspondent's identity using safe contact details
- Do not yield to emergency
- Follow segregation of duties
- Do not share your validation means

## In case of account or co-ordinate modification

- Check your correspondent's identity using safe contact details
- Don't wait until you have to make the payment
- If the account is domiciled abroad, and for Tier-1 vendors, double-check
- Also check in case of co-ordinates change
- Check **email headers**

## In case of technical officer's call or email

- Contact your Relationship Manager (or editor)
- Do not give remote access to your PC
- Do not perform tests above 1 €
- Never give any code to anyone, not even the bank

# In case of fraudulent transfer (or suspicion)

1 

**NOTIFY YOUR MANAGEMENT AND PRESERVE EVIDENCE**

2 


**CONTACT YOUR RELATIONSHIP MANAGER IMMEDIATELY**

3 

**FILE A COMPLAINT WITH THE POLICE IN YOUR COUNTRY**

**Emergency Call List:**

**Emergency Call List:**

**Emergency Call List:**

*Credit: Shutterstock*