PROTECTING INFORMATION

TRAINING KIT

Most payment frauds begin with information theft by email, phone, malware or computer hacking - Have you taken steps to protect your business?

Credit: Shutterstock

BNP PARIBAS CASH MANAGEMENT
June 2018

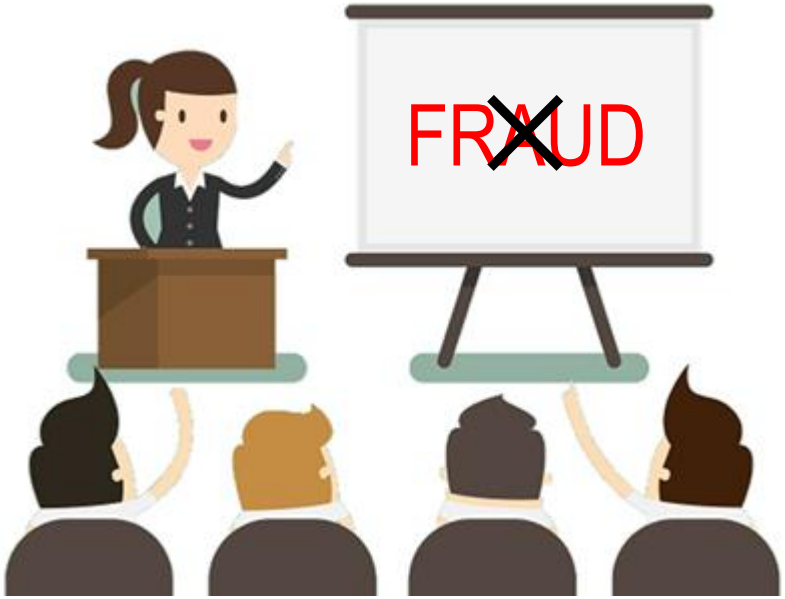
BNP PARIBAS

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

Information dissemination and social engineering

EXAMPLE

Click on the image to see the video

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

Another video: "Dave the medium": https://www.youtube.com/watch?v=F7pYHN9iC9I

Beware invoice theft

From: Direction générale des Finances publiques [mailto: [redacted]@dgfip-financesgouv.com]
Subject: [redacted] - VAT Declaration 3310/CA3

As part of the examination of your VAT declaration (3310 / CA3), I thank you kindly to communicate the following information:

- The references (company name and contact details) of your 2 largest regular supplier.
- The amount of purchases made by these 2 suppliers each month, over the last 3 months.
- The payment due date, as well as the payment method.
- An account statement, as well as a duplicate invoice for each supplier.

In order to treat your file in the best conditions, I thank you kindly for giving me these elements as soon as possible. I remain at your disposal for any further information.

[redacted] Public Finance Inspector

THE WARNING SIGNS

- **An unknown person** making contact with you for whatever reason and asking you for information, even trivial information.
- **Any request concerning your invoices, your main clients, your leases, etc.** from someone pretending to be your client, an auditor, tax authorities…
- **The quantity and nature of the information on your company** available on social networks, your web site, the works council web site, forums, etc.

PROTECT YOURSELF

- **Limit the amount of publicly available information**
  - Limit the amount of information available on the Internet (social networks, blogs, web sites …).
  - Do not circulate potentially sensitive documents (letter templates, signatures...).
  - If possible, use different signatures for your bank orders from for your public documents (articles of association, …).
  - Be discreet outside your company about your role (payment preparation, signing authorisations …).
- **Check the identity of anyone seeking information**
  - Do not give information to people you do not know (head-hunters, survey organisations, unknown colleague, etc.).
  - All kinds of information no matter how trivial can be useful to a fraudster (holiday dates, email addresses, children's names, etc.).
  - Be particularly suspicious of anyone seeking information on your payment procedures and tools, your invoices, your main clients, your leases (clients, auditors, public administrations…)
  - Check the requestor's identity before sending your invoices again.
  - Always check the identity of your contact using his or her known particulars (and not those supplied by your correspondent).

AND REMEMBER

- "The Internet never forgets": once information has been published on the Internet, it is extremely difficult to remove it.

Phishing and Spear Phishing

EXAMPLE

Click on the image to see the film

http://youtu.be/5aJ0mZntZEc

THE WARNING SIGNS

- **An email that seems to come from an institution** you have an establish relationship with (Linkedin, bank, supplier, customer, tax authorities…), with a link or an attachment
- **An unexpected request** which seems to have a logical basis (invoice…)
- **An alarming or inciting message** urging you to open a file or click
- **Any inconsistency** in the email (spelling…)

Credit: Shutterstock

PROTECT YOURSELF

- **Check if the email is legitimate**
  - Check the subject and content of the email carefully (spelling, alarming message…), as well as the sender's email address, especially the domain.
  - You can check a link by going over it with the mouse (the forwarding address is displayed at the bottom of your navigator).
- **Develop sharp reflexes!**
  - If in doubt, do not open attachments and do not click on any of the links or clickable images provided.
  - In particular, do not sign in on the web site proposed in the email (do not enter a password, or a code sent by SMS).
  - To access your banking tool or social network app, always use Favourites or input its usual address or use the native app.
  - Do not call any phone numbers given in these emails.
  - Do not reply to these emails.
  - Do not hesitate to contact the sender using safe contact details.

AND REMEMBER

- Spear phishing is a phishing attack directed at specific individuals or companies to steal data, install a malware, etc. The sender may seem to be someone you know.
- Some fraudsters go further and also intercept the code sent by SMS by your bank, either by asking for it on a fake web site, or by asking your telephone operator to reroute your phone line.
- If you encounter a default on your mobile phone (prolonged loss of network, invalid SIM card) it might be an attack by a fraudster. In this case, contact your relationship manager and your telephone operator immediately

Malicious software (malware)

EXAMPLE

Malware: **software which you install unknowingly** by clicking on a link or opening a document, which spies on you and allows the fraudster to take control of your PC or smart phone, or steal data.

Click on the image to see the film

http://youtu.be/AbVj0Akl4P8

More about malware:

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

THE WARNING SIGNS

- Any email from an **unknown contact** containing a link or attachment.
- Any email from a known contact with an **unusual subject or content**.

PROTECT YOURSELF

- **Upon receiving an email**
  - Do you know the sender? Is it their usual address?
  - Is it normal for a colleague to use a private email address?
  - Is there something unusual about the subject or the message?
- **Be suspicious of attachments**
  - If in doubt, do not open attachments.
  - If you open an attachment, do it on a work station protected by antivirus software, not on your smartphone or your private PC, and do not allow the execution of macros.
  - Do not open attachments containing jokes or slide shows.
  - Set your email software so that it does not open attachments automatically.
- **Be suspicious of links contained in an email**
  - Never click on a link sent by an unknown sender.
  - Do not open links from your smartphone, but rather from your PC.
  - On your PC, run your mouse over the link to see if it goes to the website claimed. If not, do not follow the link.
- **In general, only go to trustworthy web sites.**

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.
- Be suspicious of anyone contacting you offering assistance with your payment application. Check their identity against their known particulars (and not those the person has given you).
- Never trust messages asking you to call your bank: always check the phone number.

Credit: Shutterstock

Hacking and Intrusions

EXAMPLE


Marc Ayadi: "It is possible to break into 80% of treasury applications"

DIRECTIONS FINANCIÈRES

NOS PARTENAIRES

LUX

* Les Echos Business 11/03/2015

Deloitte: "When we perform intrusion tests, **we can access treasury systems in 80% of cases**. Unless everything is encrypted, it is possible to **modify the amounts and supplier account details**..."*

THE WARNING SIGNS

- **Hold-ups**, **unusually busy network**, **higher than usual disk activity, alterations to files** are potential signs of a hack or virus infection on your PC or smartphone.

PROTECT YOURSELF

- **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 smartphones (usually no antivirus software installed) and private computers in particular.
  - Restrict access to your customer and supplier databases.
  - If possible, have intrusion tests carried out on your ERP / treasury sys.
- **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.
  - Computerize your payment procedures as far as possible (to prevent a fraudster altering a payment file).
  - Do not log on from a PC or private smartphone.
  - If possible, make your payments on a PC dedicated to that purpose.
  - **For more info, consult the US CERT website**

AND REMEMBER

- Deloitte: "When we perform intrusion tests, we can access treasury systems in 80% of cases. Unless everything is encrypted, it is possible to modify the amounts and supplier account details."
- Our "Secured Flows" solution provides additional country and account controls independent of your information system.

Good reflexes: be cautious!

Build a culture of risk

- Be discreet on social networks
- If possible, use a separate signature for public documents (statutes, etc.)
- Beware of requests for invoices, tax information, etc.
- Beware of fake clients, auditors, public administrations ...

Protect your Information System

- Use up-to-date OS, browser, firewall, antivirus and malware detection software
- Restrict installation rights to administrators
- Protect your customer and supplier databases

In case of unusual email

- Beware of unusual emails even if they come from someone you know
- If in doubt, don't touch attachments or links
- Take the habit to check email headers
- Do not allow the execution of macros when opening attachments

Make good use of your payment application

- Do not connect on a smartphone or a private PC
- Beware of unusual validation pages or unusual slowness
- Unplug your validation means when you are not using it
- If you suspect malware, do not log on, and contact your relationship manager

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