BANK FRAUD

HOW TO DETECT IT AND GUARD AGAINST IT

Every year, **lots of companies fall victim to fraud**.

Below you will find the most common fraud techniques and **our tips for identifying them and protecting yourself against them**.

PHISHING

Why would your "bank" ask you for information it already has?

For example: "Urgent! Please confirm your bank details immediately, or we will have to close your account!"

PRINCIPLE

Fraudsters extract confidential information by purporting to be a trustworthy entity: bank, government agency, telephone operator, etc… In most cases, they send emails to a very large number of companies. The troubling nature of their message will prompt some people to connect to a fake website and provide information.

THE TYPICAL SCENARIO

1. Mass sending of emails
2. Troubling message
3. Input of confidential data
4. Use of extracted data

WHAT SHOULD YOU DO IF YOU RECEIVE A SUSPICIOUS EMAIL?

Look out for signs that might alert you: implausible sender's email address, syntax errors or spelling mistakes, link or site with an very similar URL address, no "https" in the internet address of the site visited or padlock indicating a secure connection;

Do not click on the links;

Do not open the attachments;

Do not reply;

If you have the slightest doubt whether this email has been sent to you by Societe Generale, forward it to the following email address: securite@societegenerale.fr.

BANK TROJAN FRAUD

A fraudster circulates a virus hidden in an attachment to a malicious eMAIL

For example: "Please find attached your invoice..."

PRINCIPLE

When you open the attachment, the virus is installed on the computer and starts to record everything you do on it. It might also try to spread via the company's internal network and infect other computers.

As well as communicating confidential information to the fraudster, the virus also enables him to **remotely take contro**l of the computer(s) and to **perform fraudulent transactions**.

THE TYPICAL SCENARIO

1. Receip of an e-mail with attachment
2. Click on the attachment
3. Installation of the virus on the computer and possible spread to the company's internal network
4. Remote control of the computer
5. Entry and validation of fraudulent transactions

HOW DO YOU SPOT THE FRAUD?

Pay attention to the origin and content of the emails you receive (see paragraph on Phishing methods). **Also beware of unusual behaviour that you might notice on Sogecash Web**: appearance of unusual waiting messages, information request windows, etc.

SOCIAL ENGINEERING

FAKE CEO

Careful: the person on the phone might not be who he says he is.

Example: "This is your CEO speaking... I'm trusting you with this urgent transaction... Keep it secret until the official announcement!"

PRINCIPLE

The fraudster takes on the identity of an authority figure to demand that a team member executes a fraudulent transaction, with the pretext of urgency and confidentiality. By pretending to be a high-ranking company figure, the fraudster has powerful levers to manipulate his victim. He then makes use of his apparent authority – "I'm giving you an order" – while also building up the team member – "I'm counting on you".

THE TYPICAL SCENARIO

1. Contact
2. Urgent request
3. Force of persuasion
4. Transfer order

WHAT SHOULD YOU DO IF YOU RECEIVE AN UNUSUAL REQUEST?

Comply with internal procedures: they were put in place to prevent this and other types of fraud.

Resist the pressure and adopt a critical mindset when faced with an overly insistent person, if necessary calling on a colleague or a manager.

Listen to your intuition: if a request seems dubious, it probably is!

Check the legitimacy of the request, for example by making a confirmation call to an already-listed number.

FAKE SEPA TRANSFER TEST

What if this so-called "test" was actually a fraudulent transfer?

For example: "We need to carry out a test... The transactions placed will be fictional... We're here to help you!"

PRINCIPLE

The fraudster pretends to be the information management department of a bank or a provider and to have compatibility tests for the client company to run in order to ask the victim to make a bank transfer. To facilitate the

fraud, the fraudster may suggest that the victim allows her to take control of her computer. He then takes remote control of the computer and sees everything that happens on it.

THE TYPICAL SCENARIO

1. Contact
2. Request of a transfer test
3. Control of the computer
4. Fake validation

WHAT SHOULD YOU DO IF YOU RECEIVE AN UNUSUAL REQUEST?

Bear in mind that your bank or provider will never contact you to:

- **perform test transfers.** Test requests always come from customers, who set the characteristics themselves. Their amounts never exceed a few euros (penny test);
- **communicate confidential information** by telephone or email, in particular a username, an activation code or a secret code;
- **take control of your computer.**

Check the legitimacy of the request by making a confirmation call to an already-listed number or implementing the planned internal procedure.

Do not send confirmations of transfer orders **to an unusual number** without checking the veracity of the request.

Resist the pressure and adopt a critical mindset when faced with an overly insistent person, if necessary calling on a colleague or a manager.

Listen to your intuition: if a request seems dubious, it probably is!

REDIRECTION OF YOUR TELEPHONE LINE

A stranger answers instead of you when you receive a call!

For example: "We've been flooded... Could you redirect calls to our backup site?"

PRINCIPLE

The fraudster redirects a company's telephone line to a fake backup line, in order to confirm a fraudulent transfer order to the bank. First, the fraudster will have found out about the company's **business continuity** plan and security procedures by sending a malicious email containing spyware.

THE TYPICAL SCENARIO

1. Sending of malicious e-mail
2. Extraction of information
3. Redirection of the line
4. Transfer request
5. Fake validation

HOW DO YOU SPOT THE FRAUD?

It is possible that a fraud is happening if:

- one of your company's sites or departments **does not receive any telephone calls** for an abnormally long period;
- one of your acquaintances contacts you on your mobile and tells you **that a stranger is answering calls** on your landline.

WHAT DO YOU DO NOW?

Immediately contact your telephone operator and regular Societe Generale advisor or the Sogecash Web hotline.

PREVENTIVE MEASURES AND THE RIGHT INSTINCTS TO LIMIT THE RISK OF FRAUD

The best practices listed here will help you to protect your company against social engineering.

MAKE YOUR ACCESS CODES SECURE

- **Choose your Sogecash Web secret code carefully and change it very regularly.** Avoid secret codes that are very easy to guess (date of birth, etc.) or already in use (phone access, etc.)
- Don't tell anyone your Sogecash Web identifier and secret code (not your colleagues, or the police, or your bank…)
- **Keep these codes safe, where nobody else can access them, and do not store them in the same place** (for example, do not store them on the device, in a file, on a community platform, or on the cloud).

DOWNLOAD THE SOGECASH WEB MOBILE APP SECURELY

- **Click on the link provided on our site www.sogecashweb.com.** (When you connect to www.sogecashweb.com on a smartphone or an iOS or Android tablet, we display a specific screen giving you direct access to the App Store or Google Play where you can download our app).

DO NOT USE SOGECASH WEB MOBILE ON A “ROOTED” OR “JAILBROKEN” DEVICE

- **Do not use Sogecash Web Mobile on a "rooted" or "jailbroken" device** which allows you to download apps not verified by Apple or Google. This will make your device vulnerable

KEEP YOUR CONNECTIONS SECURE

- Choose a recognised internet service provider and follow its security advice.
- Check for https ("s" for secure) before the site's address.
- Do not use a search engine to access Sogecash Web.
- Do not access Sogecash Web on a public computer or a device connected to an unsecured WiFi network.
- Check the date and hour of last connection to Sogecash Web, displayed on the dashboard. The last connection channel is also displayed on Sogecash Web Mobile.
- As soon as you have finished browsing, log out using the "logout" button.
- We recommend you to set your browser so that the tracks of your browsing would be deleted when disconnecting.

CONTROL THE INFORMATION

- **Limit the amount of information you post about your organisation** (social networks, websites, template letters, signature, etc.) and **control the information posted** on the company's websites.
- Urge team members **not to post sensitive information on professional and personal social networking sites**.
- Make sure you **limit access to sensitive documents**, such as the company's fax template.
- **Keep confidential the handwritten signatures** of senior figures authorised to confirm transactions.
- Do not give out too many details on your company's corporate hierarchy in your out-of-office email message. Fraudsters often use periods of leave to send emails and, using out-of-office emails, gather as much information as possible on the hierarchies of their target companies.

PUT IN PLACE SECURE INTERNAL PROCEDURES

- Define **clear** and **formalised** processes.
  Secure access to **sensitive applications** and **data.**
  Limit users' rights to what is strictly necessary.

Equip people in sensitive roles with strong authentication devices.

- Implement **separation of duties.**
  If possible, try to ensure double administration and double confirmation of orders.
- Carry out **regular checks.**
  Comply with procedures, account verification, etc.
- Your regular Societe Generale contact is there to help you.
- Also, do not forget to delete a user when your team member changes job and no longer works on Sogecash Web, or leaves the company.

RAISE YOUR TEAM MEMBERS' AWARENESS

- **The most exposed team members to attempted fraud:**
  Treasurers - Accountants - People working with means of payment.
- Comply with operational procedures and carry out the required checks.
- Be vigilant if contacted by an unfamiliar person (customers, suppliers, partners, etc.)
- Retain a critical mindset and exercise your right to notify.
- Do not content yourself with the displayed information: fraudsters can easily modify the sender's visible email address or the caller's telephone number displayed on their target's phone.
- As managers, enhance fraud attempts thwarted by your team members' vigilance.

KEEP COMMUNICATION WITH THE BANK SECURELY

- Limit paper or fax transfers, which are easier to forge than other means of payment.
- Try to use automated channels such as Sogecash Web, Sogecash Net, EBICS, SWIFTNet, etc.
- Comply with the security instructions related to your tool: strong authentication with 3SKey or Secure Access, user rights for Sogecash Web, etc.
- Disconnect your 3SKEY when you are not using it. It should be kept in a safe place. That way if a fraudster manages to install software to remotely take control of your computer, he may not be able to do anything if the key is no longer connected.
- Check the information provided by Secure Access when validating orders on Sogecash Web Mobile.
- Inform your bank about the contacts to reach if they have any doubts about bank transactions.

MAKE THE COMPANY'S INFORMATION SYSTEM SECURE

- Antivirus software, security patches, personal and company firewall, etc.

WHAT DO YOU DO IN A PROVEN OR SUSPECTED CASE OF FRAUD?

Inform your manager.
Notify your bank: Your regular Societe Generale contact or the Sogecash Web hotline on +33 (0)1 42 14 13 12. You can also click on "contact" on our homepage and fill in the form, which our support team will deal with immediately.

Do not hesitate to contact us if you have the slightest doubt (e.g. regarding a suspect access or transaction, or if the system works in a suspicious way).