

# FRAUD AND CYBER RISKS

## AWARENESS KIT FOR BUSINESS

*Have you taken steps to  
protect your business?*



BNP PARIBAS CASH MANAGEMENT

2024



**BNP PARIBAS**

The bank for a changing world

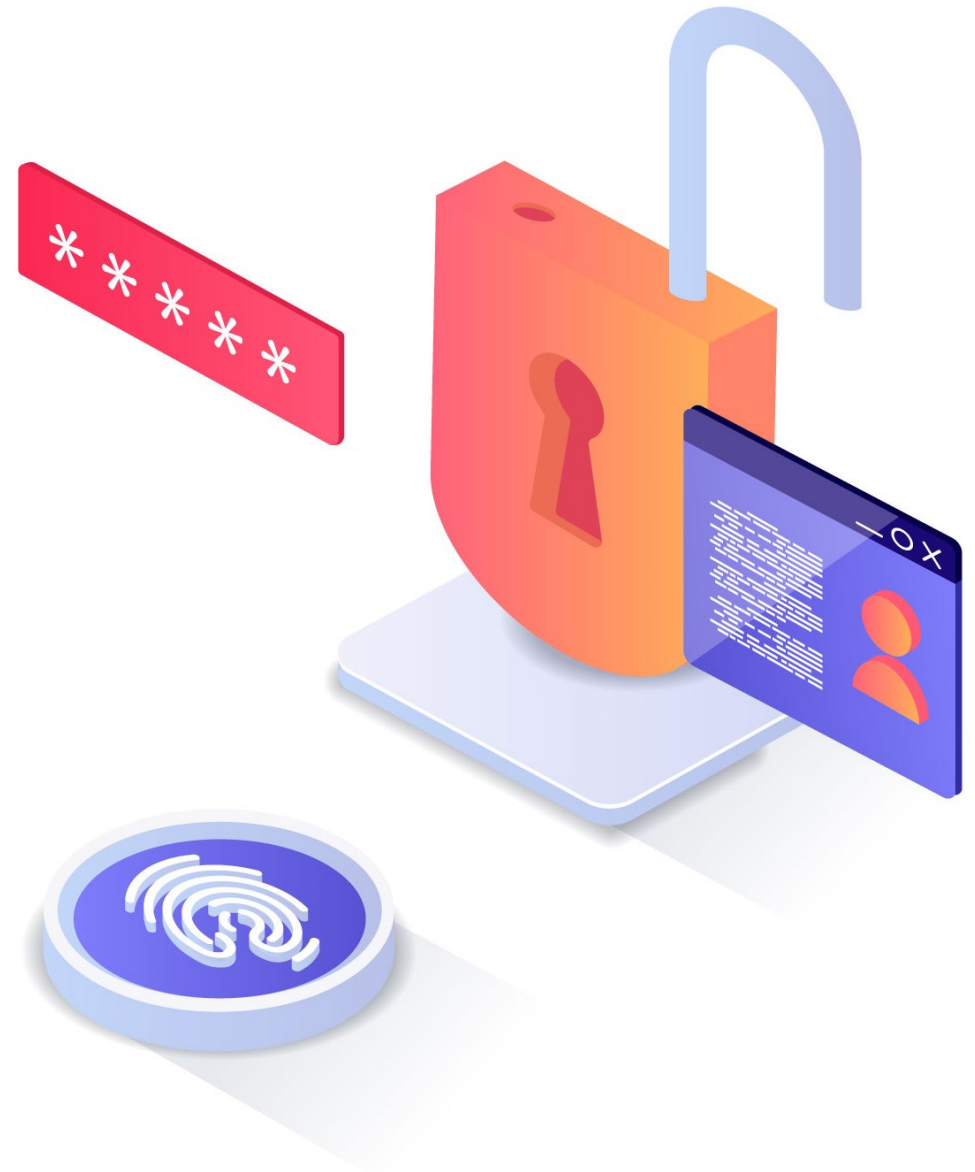
**01 INTRODUCTION**  
Make your staff aware of the dangers!

**02 FRAUD SCHEME OVERVIEW**  
The fake CEO scam, the fake vendor scam...

**03 THE TECHNIQUES**  
Information theft and social engineering, spoofing...

**04 CYBER RISKS**  
Phishing and spear phishing, malware, ransomware...

**05 CONCLUSION**  
Develop sharp reflexes, in case of fraudulent transfers



# MAKE YOUR STAFF AWARE OF THE DANGERS!



To protect your company against fraud, it is not enough to have procedures, tools and controls.

It is very important to **keep your staff informed and trained** so they can detect and counter fraud attempts and cyber attacks. In almost all cases **fraudsters take advantage of human weakness**.

#### DO:

- **Hold regular training:** Do not just rely on sending emails
- **Ensure that temporary employees and employees on fixed-term contracts** have inductions on fraud as they are ideal targets
- **Train accounting and treasury staff to raise awareness amongst all employees** liable to be duped into giving information to fraudsters (assistants...) or inadvertently installing malware on the Network
- **Retrain staff** at least once a year: threats are constantly evolving and your staff must stay alert
- In **addition to Training, provide very clear written instructions** to your employees (P & P's)

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



# FRAUD SCHEME OVERVIEW

---

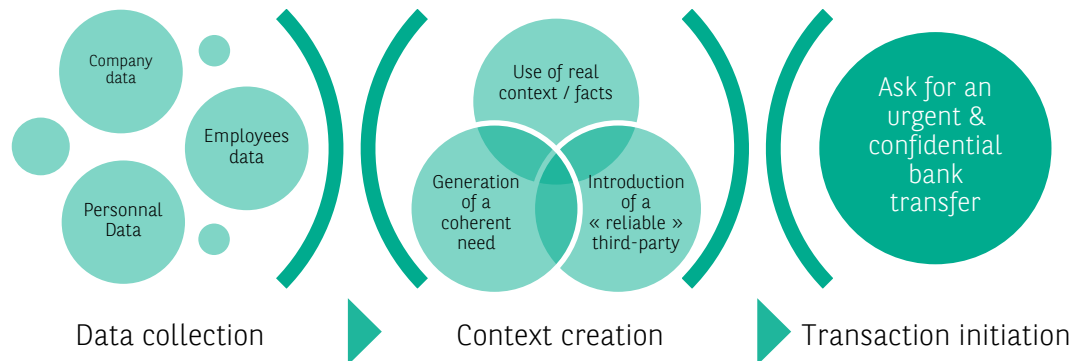


# THE FAKE CEO SCAM

## EXAMPLE

You receive an **email** or a **WhatsApp message** or a **call** from a fake executive ordering you to make an urgent payment:

*“We have been working on a financial operation which must remain strictly confidential. I've chosen you for your discretion and great work. Our law firm will contact you to give you the details.”*



## THE WARNING SIGNS

- **An email** about the acquisition of a company, a tax audit...
- **An unexpected solicitation by lawyer**, an executive, a board member...
- **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 rely on you”)
- **Intimidation** or harassment (“Listen to me! It’s urgent!”)

## PROTECT YOURSELF

- **Be aware** Management will never ask you make urgent payments that do not follow normal procedures
- **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 (or set up one-off) large payments by yourself, you are at risk; a **minimum of dual authorisation** should be mandatory
  - Avoid transfer orders and validations by fax; it is easy for fraudsters to get signature samples
  - Passwords and Log-in’s are personal: Never give them to colleagues; report them if they try to give you theirs
- **Make common sense checks:**
  - **Check email addresses:** fraudsters often use similar addresses (for example: john.smith@sale-team.com instead of john.smith@sales-team.com). (See page 7)
  - **Check the identity of your contacts** by re-contacting them using known and verified details, not those given by the sender

## AND REMEMBER

- Fraudsters use Voice over IP telephone platforms and can **simulate local phone calls** in most countries; they use **caller ID spoofing** techniques to impersonate telephone numbers; they also use **WhatsApp** calls or messages
- Fraudsters often know a great deal about your business and can **mimic people’s voices** (“deepfake”)
- If the scam fails, the fraudster may then call the CEO pretending to be a **police officer** or the **bank**

**! We note an increase of email address hacking, so stay alert even when the email address is legitimate.**

# THE FAKE CEO SCAM

## Signs that should ring a bell!

- Email spoofing
- Emergency / Date close to public holiday...
- Specific Context
- Confidentiality
- Flattery
- Involvement of 3rd party (law firm...)

**RE: URGENT – Please proceed ASAP !**



✕ john.smith@qwerty-analysis.com <john.smith@presidency.com>

Monday June 17 at 3:44 PM

À: kate@qwerty-analysis.com

Kate,

For the last months we have been working, in coordination and under the supervision of the SEC on acquiring a Chinese company. This takeover bid must remain **strictly confidential**, no one else needs to know for now.

The **COVID-19** seems to be playing in our favour as our offer has been accepted sooner than expected. The public announcement of this takeover will take place Friday, July 4th 2020 in our office with the presence of the entire board.

I've chosen you for your discretion and great work within the company. Please contact **immediately** our **law firm** (**robert.johns@kpmg-lawyer.com**). He will give you the bank details to make the credit transfer **immediately**.

Please **send me the balances of the accounts**.

This is very sensitive, so **please only communicate with me through this email (john.smith@presidency.com)**, in order for us not to infringe SEC regulations.

**John Smith**





# THE FAKE VENDOR SCAM (AND FAKE FACTOR, LANDLORD...)

## EXAMPLE

A fake supplier informs you (by email, mail, telephone) that its bank account changed, and all invoices should be paid to the new account :

### Payment information

  john@company.com Today at 3:02 PM  
À: kate@qwerty-analysis.com

Due to the news of the Corona-virus disease we are changing banks and sending payments directly to our factory for payments, so please let me know total payment ready to be made so I can forward you our updated payment information.



BTW BE 044	Scammer's contact details	CENTRE
RPR Bruxelles 044		RUE DU
Telefoon : +32 (0)2 1		1170 BRUXELLES
Fax : +32 (0)2 1		
E-mail :		
Klantcode : CEP		
IBAN : PL87124010371978001054758017		

**INVOICE**

92190 MEUDON Paris, 2014, 30<sup>th</sup> September

Subject: modification of our bank account details **REGISTERED LETTER**

Dear Sir,

Further to today's call, please find our new bank account details, due to the outsourcing of our accounting department to Poland.

This measure is effective immediately, for the payment of all your rent, for the premises located 92190 Meudon.

## THE WARNING SIGNS

- Any request for a **change of beneficiary account** (by mail, by email, on the invoice, by telephone, etc.)
- Recent supplier's **contact change** (email, phone number...)

## PROTECT YOURSELF

Follow a procedure in case of bank account detail or contact detail modification:

- Check the **identity** of your contact using **verifiable contact details** (and not those sent in the invoice); do not wait! until you should make the payment
- Pay particular attention to your largest suppliers
- Be very 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: ABKLCY2N
  - France: **FR**7630046001290029721519546 -BIC: ABCDFR1N
- Complete your procedure with an **Account Validation Solution**, such as the one provided by **BNP Paribas' partner : Sis ID**. ([sis-id.com/en/](https://sis-id.com/en/)). Ask your business manager for a demo.
- Appoint very few people authorised to **modify vendor details and ensure dual control on changes**; train these people regularly and make them accountable

## AND REMEMBER

- Fraudsters use **registered letters**
- Fake landlord and fake factor scams are variations of this fraud:

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

- Before attacking, fraudsters generally **steal real invoices** from the supplier, using impersonation or hacking techniques
- Beware**: Scammers can use email addresses that resemble that of your provider - **or are exactly the same**; then high jacking your emails (See page 7)

 **We note an increase of email address hacking, so stay alert even when the email address is legitimate.**



BNP PARIBAS

The bank for a changing world

# THE FAKE TECHNICIAN SCAM

## EXAMPLE


A scammer pretending to be a bank technician contacts you, claiming whether a technical malfunction or the need to run some tests.

Through elaborate psychological control mechanisms that put you in perfect confidence, the scammer manages to recover your access and validation codes to your online banking sites. By connecting remotely to your tools, he is free to issue and validate payments for his benefit.

A different approach, based on similar techniques, consists purely and simply for the scammer to take control of your computer, by making you accept the control of your PC directly by himself.

## 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](http://www.id5.com/bnp), [www.tin.com/sepa08](http://www.tin.com/sepa08), [www.tinyurl.com/migr](http://www.tinyurl.com/migr), etc.)
- A request to take control of your PC remotely
- A suggestion to do a test transfer
- A threatening approach, pretending for example that your account might be blocked or your payments processed twice unless you communicate your codes to your caller. **Remember that BNPP staff will never ask you to provide your codes over the phone or by email.**

 **Fraudsters may call their victims after having committed a scam and ask questions pretending to help their victims get their money back. In reality, they are gathering information to improve their fraud techniques. If you have been a victim of a fraud and the fraudster contacts you again, hang up immediately.**

## PROTECT YOURSELF

- **Do not trust caller ID:** fraudsters may impersonate your relationship managers' telephone number (phone spoofing)
- **Contact your relationship manager** using known details to verify the identity of anyone claiming to be BNP Paribas Staff (or software vendor's staff)
- **Refuse to allow your PC to be controlled remotely by anyone who you cannot verify**, do not go to an Internet address, do not click on links / downloads
- **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 (Penny Test)
- **Never give anyone any codes** (e.g. number generated by your wireless reader, password, PIN code, etc.)
- **Protect your computer network and your PCs** against hacking and malicious software, by ensuring regular updates/patches

## AND REMEMBER

- **No BNP Paribas technician will ever contact you** unless you have personally asked for assistance
- Fraudsters can also claim to be your **banking software vendor**
- **Scammers know banking systems very well;** they may even be aware of current issues; even the name of your relationship manager
- In order to dupe you, the fraudster may make several **preliminary calls to establish trust**, without scamming you the 1st time.
- If you are equipped with a wireless reader, the fraudster may say: "Don't tell me your PIN code, I'm not supposed to know it; **just give me the code displayed on the wireless reader**"
- **A new scheme of this type of fraud involves contacting you to update your BNP Paribas identification tools. Be alert!**



# THE FAKE EMPLOYEE SCAM / SALARY SCAM

## EXAMPLE

This scheme is similar to the vendor scam:

- A fake employee informs you (by email, mail, telephone) that their bank account has changed, and their salary should be paid to the new account.
- Your company end up paying a fraudulent account.



**RE: New IBAN**

**JS**  **john.smith@gmail.com** 26/07 - 12:02

**To :** kate@qwerty-analysis.com

Hello Kate,

I will contact you with my personal e-mail address because I can no longer connect to my professional address since yesterday. I mentioned it to the IT support but pending their return. I preferred to contact you immediately.

I have recently changed banks and would like to transfer my next salary on the attached IBAN.

Kind Regards.  
John Smith

## THE WARNING SIGNS

- Any request for a **change of beneficiary account** (by mail, by email, on the invoice, by telephone, etc.)
- Recent employee's **contact change** (email, phone number...)
- Be particularly vigilant if the account is located in a **foreign country** or in a **non tier-1 bank** (especially internet-only banks)

## PROTECT YOURSELF

Follow a procedure in case of bank account detail or contact detail modification:

- **Check the identity** of your contact using **verifiable contact details** (and not those sent in the mail); do not wait! until you have to make the payment
- **Be very 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: ABKLCY2N
  - France: **FR**7630046001290029721519546 -BIC: ABCDFR1N
- Complete your procedure with an **Account Validation Solution**, such as the one provided by **BNP Paribas' partner : Sis ID**. ([sis-id.com/en/](https://sis-id.com/en/)). Ask your business manager for a demo.
- **Appoint very few people authorised to modify employee details and ensure dual control on changes**; train these people regularly and make them accountable

## AND REMEMBER

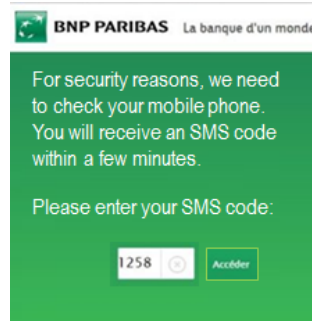
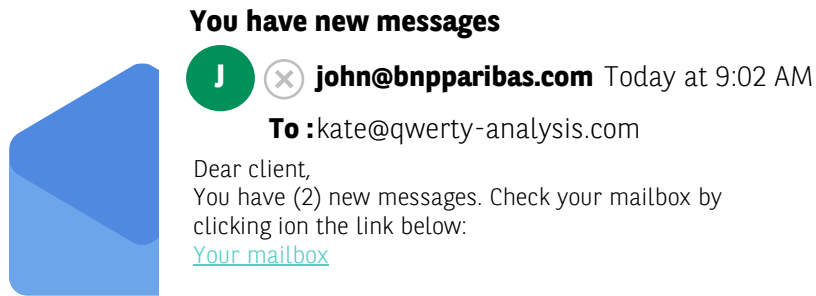
- Fraudsters use **registered letters**
- Fraudsters **often perfectly know the company** and can use the information collected on the internet to pass themselves off as your employee.
- **Caution!** Until now, this type of fraud has generally been carried out by e-mail and is becoming increasingly sophisticated and dangerous. Fraudsters don't hesitate to call on the phone, mimic a voice, etc.
- **Check email addresses!** Fraudsters sometimes use similar addresses (for example jean.dupont@sale-team.com instead of jean.dupont@sales-team.com) **but beware: it also happens that fraudsters write from the legitimate mailboxes of employees they managed to hack** (this case is more and more frequent) !



# THE PHISHING FRAUD – VIA EMAIL OR TEXT MESSAGE

## EXAMPLE

You receive an email that appears to come from your bank. If you click on the link, a bogus page of the bank opens and asks for information (passwords, credit card number, etc.). Fraudsters can also steal an SMS code sent by your bank to validate an account or card purchase.



Phishing is very common, and can affect your **phone company**, your **electricity or gas supplier**, **administration**, your **email provider** (Gmail, Hotmail...), **social networks**, and more.

Info: we received a request for a new SIM card for your mobile contract. If you are not responsible for this request, please contact immediately the Help Desk at 12345



Fraudsters can also **intercept the code sent by SMS by your bank** by having a new SIM card sent by your telephone operator. This is known as **SIM swapping**.

## THE WARNING SIGNS

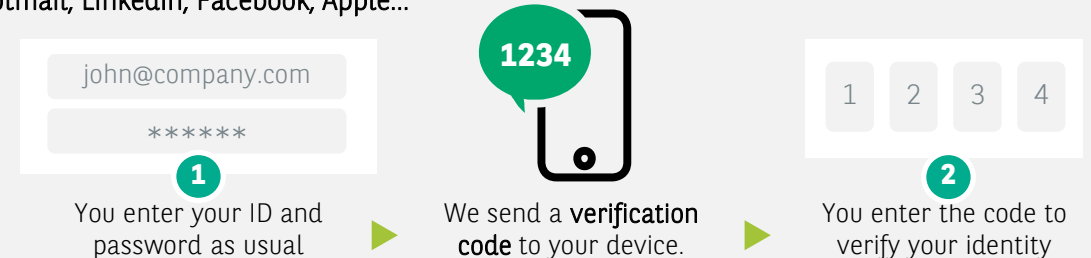
- An email that seems to come from an institution you have an establish relationship with (LinkedIn, bank, supplier, customer, tax authorities...), with a link or an attachment
- An unexpected request which seems to have a logical basis (invoice...)
- An alarming or inciting message urging you to open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

## PROTECT YOURSELF

### Develop sharp reflexes!

- Carefully check the **subject** and **content** of the email carefully (spelling, alarming message...), as well as the **sender's email address**, especially the domain
- As a general rule, do not open attachments and **do not click on any of the links or clickable images** provided in an email you receive
- To access your banking tool or social network app, always use the native app or use Favourites or input its usual address in your browser; check the presence of **https://** and the **lock icon**
- If by mistake, you click on a link in an email, do not sign in on the web site: **do not enter a password, or a code sent by SMS**
- **Do not open or reply to suspicious emails**; do not call any phone numbers given in these emails

Use strong authentication on your web banking site. Turn on 2-Step authentication on Gmail, Hotmail, LinkedIn, Facebook, Apple...



## AND REMEMBER

- If you encounter a **default on your mobile phone** (prolonged loss of network, invalid SIM card), you may be victim of **SIM swapping**; contact your telephone operator
- **Spear phishing** is a phishing attack directed at specific individuals or companies to steal data, install malware, etc.; the sender may seem to be someone you know
- **Check links by hovering over the URLs**; the forwarding address is displayed at the bottom of your navigator)

# THE PHISHING FRAUD – VIA INTERNET SEARCH / FAKE WEBSITE

## EXAMPLE

You search for your banking site on your regular search engine by entering your usual keywords.

If you don't pay attention, you click on a wrong link : **a fake internet page** of the bank opens and asks for information (passwords, bank card number, etc.). Sometimes the fraudster can also retrieve a code sent to you by SMS or email from your bank to validate a device, account or card purchase.

It is a phishing technique without specific targeting but which can affect all those whose users access the site via a search engine.

Scammers create web **sites visually close to official sites** from any room and artificially raise them in the search through sponsored advertisements, see sophisticated referencing techniques, making false sites appear first in the search.

## THE WARNING SIGNS – REAL USE CASE

- A sponsored link
- An unusual extension
- Language inconsistencies

+ on the website:

- Any inconsistency (spelling errors, old logo ...).
- Incoherent and/or old content
- No access granted despite proper input of the Login and password

The screenshot shows a search engine interface with the query 'bnp entreprise'. Below the search bar, there are two search results. The first result is labeled 'Fake site' and is for 'entreprisesenligne.net'. It features a search bar, navigation tabs (Tout, Images, Vidéos, Actualités, Carte, Shopping, Préférences), and a list of services: 'Stormschade Repareren', 'Daklekkage', 'Contact', and 'Platte Daken'. The second result is labeled 'Real Site' and is for 'BNP Paribas Entreprises | Solutions bancaires pour les Entreprises'. It includes a search bar, navigation tabs, and a list of services: 'Stormschade Repareren', 'Daklekkage', 'Contact', and 'Platte Daken'. The 'Fake site' result is circled in red, and the 'Real Site' result is circled in green.

## PROTECT YOURSELF

- Do not go through a search engine to find your e-banking site:
  - Record it in your favorites
  - Or enter the full address on your browser's bar
- If, however, you need to go through a search engine, be VERY VIGILANT:
  - Enter the full address, rather than standard keywords.
  - Do not click on sponsored links.
  - Read the site address carefully before clicking to detect any anomalies (letters missing or added, dash in addition, unusual extension, inadequate language...)
  - Check that the site description is consistent and written in appropriate language
  - Make sure there are no unusual features: specific characters, language inadequate for the site visited...
- Do not share your means of access, even among colleagues
- Use the strong authentication offered by your bank. Check the alerting emails sent by your bank and notify it immediately if you receive them for a action that you did not initiate.

## AND REMEMBER

- Below are the links to the official BNP Paribas websites :
  - Connexis Cash : <https://connexis.bnpparibas.com/>
  - MaBanqueEntreprise : <https://mabanqueentreprise.bnpparibas.com/>
  - MaBanque : <https://mabanque.bnpparibas.com/>
  - MaBanquePro : <https://mabanquepro.bnpparibas.com/>
  - MaBanquePrivée : <https://mabanqueprivée.bnpparibas.com/>
- Do not communicate any code to anyone
- Some fraudsters intercept the single-use code sent by SMS (SIM SWAPING techniques). If you encounter an anomaly with your mobile phone (prolonged network loss) contact your operator.



# CHECK SCAMS

## EXAMPLE

### Sending a check then requesting a refund by bank transfer

A customer or a prospect sends you a payment by check, for an amount much higher than the invoice. Claiming an error, he asks you to cash the check and return the excess received by bank transfer, less a commission to apologize for the constraint.

The check will turn out to be fake, but your transfer will be real!

Variation: the check can be for the right amount and the bogus customer can simply ask for the refund by bank transfer, claiming a cancellation.

*“Please find attached the payment of the invoice for the rental of the space for the seminar scheduled in 2 months.”*

*The amount is **double** than expected*



*“My apologies, I confused the amount with that of another quote. Can you transfer me the surplus? Please keep an additional 10% for your account to apologize for the inconvenience.”*

There are other types of fraud with checks:

- Use by a criminal of a **lost or stolen check**.
- **Falsification of a check by a criminal**. This process consists of fraudulently modifying the amount or the beneficiary of a valid check, stolen for example from the beneficiary's mailbox.

## THE WARNING SIGNS

- A person domiciled abroad, contacts you by email (written in English or in very approximate French) and says he is interested in acquiring a good or service.
- The buyer then sends you a check for a much higher amount than initially agreed and finds an excuse to justify the difference.
- He asks you to **return part of the surplus to him**. Compensation is **generously granted** to you for your own expense and inconvenience.

## PROTECT YOURSELF

- If you accept payment by check and receive a check for an amount greater than the sale, we invite you not to cash it before investigation.
- **Never reimburse a customer by bank transfer if he paid by check before you have ensured with your bank that the check has been duly cashed** (the fact that the amount appears on your account does not mean that the bank has already checked whether the check was funded).
- **Prefer electronic payments to checks as much as possible**, especially abroad (long and complex processing times, etc.).
- **A check book must be kept in a secure place**. There are many opportunities for theft, especially when sending check books.
- **In case of fraud, report the facts to the police**. Keep all the documents in your possession (emails exchanged with the scammer, check etc.) in order to facilitate the investigations.

## AND REMEMBER

- In France, checks represent 44% of the amount of fraud, while they represent only 4% of transactions.
- The regulations do not impose a maximum amount for a check, but for certain transactions such as the purchase of a used car between private individuals, the bank check remains the norm.
- In the event of an error in the drafting of your check **with a difference between the amount in figures and that in words, only the latter will be taken into account** when cashing it! (with reference to article L131-10 of the Monetary and Financial Code).
- A check issued is valid for one year and 8 days (from the date of issue).



*Usually, a check is credited no later than one business day after it has been registered. But beware ! Just because the money appears in your bank account doesn't mean the money is actually available! A check can be rejected within an average of 8 days.*



# PAYMENT FRAUD (CORPORATE CARD)

## EXAMPLE

A malicious person steals bank details (card number, credit card code, SMS code) in order to make payments in the name of the legitimate holder, but to his own benefit.

*“Hello, I am Mr. SMITH, BNPP technician, I am contacting you regarding unusual transactions detected on your payment card.*

*- Have you recently made a payment of €936.5 to Primark”*

There are several types of card fraud:

- **Fraud following a loss or theft of a card:** especially after observing your code, a crook will use trickery to steal your card.
- **White Plastic Skimming Fraud:** A tampered ATM allows the scammer to copy your card. Practiced in particular in countries using only the CB track
- **Internet fraud: theft of card data**
  - **SIM SWAP:** Some fraudsters intercept the single-use code sent by SMS by your bank by having a SIM card sent to them by your telephone operator.
  - **Impersonation of a trusted third party:** Fraudsters call the customer pretending to be a known institution (Banque de France, etc.), the BNP Paribas fraud department, or a trustworthy entity.

## THE WARNING SIGNS

- During the call, the customer is **put under pressure** in the face of **an emergency**, for example an ongoing fraud.
- The interlocutor reassures the customer by asking him to cancel the payments made via the **communication of the code received by SMS**. This is actually the code to validate the payment.

## PROTECT YOURSELF

- **Do not rely on the number displayed**, as fraudsters can fake a legitimate number.
- If in doubt about the interlocutor, **hang up and call the usual interlocutor**, on trusted contact details.
- **BNP Paribas will never ask to validate transactions by phone.**
- In the event of a suspicious or doubtful movement, **immediately change the connection codes, and contact BNP Paribas** to put in place the appropriate security measures, for example renewing the card.
- **Get informed and communicate to your teams:**



*ECB – Report on card fraud in the Euro Zone :  
Seventh report on card fraud*



*UK Finance – Scam alert: Fake automated calls  
claiming to be banks and card companies*

## AND REMEMBER

- In the event of fraud on your BNP Paribas Corporate, Procurement, Virtual, Travel or Purchasing card:
  1. **Oppose the card immediately:**
    - by telephone by contacting your dedicated customer service or the opposition center
    - online on the website dedicated to managing the card
  2. **Dispute fraudulent transactions as soon as possible**
    - If you object by telephone, your contact person will guide you through this process. If you object on the internet, the dispute form is available directly online. You can present a limited period to dispute (you will find this period in the Conditions of Operation of your card).



*It is estimated today that approximately 90% of current fraud experienced by our customers are linked to identity theft techniques by a trusted third party.*



# THE TECHNIQUES

---



# PHISHING – THE MAIN VECTOR USED BY SCAMMERS

## DÉFINITION

« An attempt to trick someone into giving information over the internet or by email that would allow someone else to take money from them, for example by taking money out of their bank account »

Source: [PHISHING | English meaning - Cambridge Dictionary/](#)

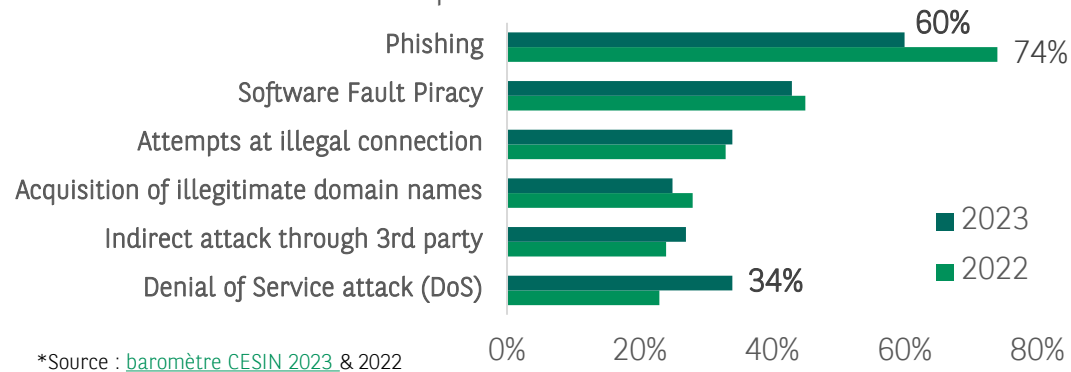
If you receive an email from a sender who calls itself an official or familiar body and wants access to your personal data on the Internet, **you must refuse**.

**Phishing is very common**, and can involve your telephone operator, your electricity or gas supplier, administration, online e-mail, social networks, etc.

It concerns both personal and professional e-mail addresses and telephone numbers.

It is the main vector for cyber attacks, because it is one of the simplest to set up.

Most common types of attack recorded by French companies in 2023



\*Source : [baromètre CESIN 2023 & 2022](#)

## EXEMPLES :

### Phishing received by email

- Carefully check the sender's subject, content and email address of the emails you receive.
- Using a credible context, fraudsters will play the opportunity or threat card to invite you to click on the links and transmit your information.

### You have new messages

**A** **primevideo@nanbV1.com** Today at 9:02 AM

**To :** Tom.STROA@Lycos.com

Hello Tom,  
Last day for to test of our "Prime Video" offer. The automatic renewal of your subscription has been successful. **An invoice of EUR 380 TTC** will be sent to you at your address..

You have 5 days to cancel your order by clicking on the button below:

[Cancellation](#)

### Phishing by SMS / text message

- Check the number and content carefully. Do not click on any links. Connect directly to the site in case of doubt.
- Absolute vigilance in all known cases below:
  - « Hi Dad, here is my new phone number. Can you whatsapp at this address : XXX ? »
  - « Good Morning, This is the delivery guy. Your package could not be delivered. Please book a new timeslot at this address XXX »
  - « DHL : Because of an incident, your delivery could not be proceed. An Action is required from you at XXX. »
  - « Netflix : Your subscription has been blocked. Please update your information at this address XXX »

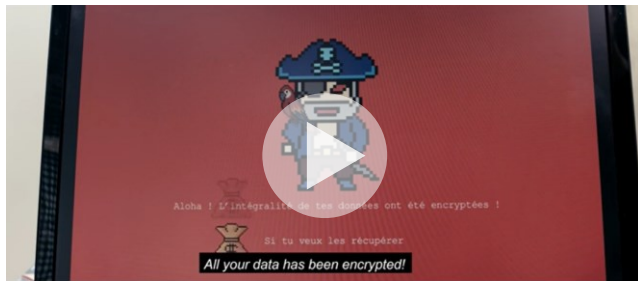


# INFORMATION THEFT AND SOCIAL ENGINEERING

## EXAMPLE

You receive an email, a mail or a phone call from someone asking for information (invoices, rental fees, contact details...):

*“As part of the audit of your VAT declaration, kindly provide details of your two largest regular suppliers, an account statement and duplicate invoices for each of them.”*



OTHER VIDEO  
*Dave the medium*

Source : <https://vimeo.com/962159764/61deee4306>

## THE WARNING SIGNS

- An **unknown person** making contact with you for whatever reason and asking you for information that seems trivial
- Any request concerning **your invoices, your clients, your leases, etc.** from someone claiming to be your client, auditor, tax authorities...

## PROTECT YOURSELF

### Verify the identity of anyone seeking information

- Do not give information to **people you do not know** (head-hunters, survey organisations, unknown colleague, etc.)
- Be particularly suspicious of anyone seeking information on your **invoices**, your **clients**, your **suppliers**, your **payments**, your **leases**, your payment procedures and tools
- Always verify the identity of your contact using his or her known contact details (and not those supplied by the correspondent)

### 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 bank orders than those on publically available documents
- Be **discreet outside your company** about your role (payment preparation, signing authorisations...)

**If possible, encrypt sensitive information and use TLS for external email communication**

## AND REMEMBER

- **All kinds of information no matter how trivial** can be useful to a fraudster (holiday dates, email addresses, children's names, etc.)
- **“The Internet rarely forgets”**: Once information has been published on the Internet, it is difficult to remove it



# INFORMATION THEFT AND SOCIAL ENGINEERING

## Data gathering techniques used by hackers

Data gathering on social networks, business registers, out of office messages...

Calls of fake surveyor, auditor, travel agency, head hunter, public administration, hotline ...

**Experience**

AR Specialist & Treasury  
janv. 2014 - aujourd'hui  
2 ans 11 mois

\* Ensure compliance of payment order signature and approvals sent by account department, perform daily banking transactions. (Payments for vendor, tax, payroll, repurchase agreements)  
\* Assistance in other daily bank transactions relations with banks and bank account reconciliations.

**Boris Estafador**  
Junior Project Manager - Cash Management - Fraud prevention à BNP Paribas  
Cergy, Île-de-France, France · + de 500 relations · Coordonnées

**Expérience**

**Junior Project Manager Cash Management - Fraud Prevention**  
BNP Paribas · Contrat en alternance  
sept. 2020 - Aujourd'hui · 2 mois  
Levallois-Perret, Île-de-France, France

Build of an Avast firewall with a 12-digit code as part of the major anti fraud project SAG 360

**Lori Kaufman**  
2:34 PM

Automatic reply: Meeting about new plan  
To: John Smith

I will be out of the office from February 13 through February 17. If you contact Matt Jones at [matt.jones@mycompany.com](mailto:matt.jones@mycompany.com). I will be returnin



Voice over IP calls simulating local numbers, caller ID spoofing, voice changer software, diversion of phone line...



BNP PARIBAS

The bank for a changing world

# EMAIL ADDRESS SPOOFING

## EXAMPLE

Fraudsters often use email addresses that resemble that of their victims whose identity they usurp: this is called **email spoofing**, and here are some examples:

- Alias forgery: `bill.gates@microsoft.com` <fraudster@gmail.com>
- Use of sub-domain: `bill.gates@microsoft.presidency.com`
- Real "From" address, bogus "Reply-To" address:
- From: `bill.gates@legit-company.com`
- Reply to: `bill.gates@legit-company.presidency.com`
- Brand name with a dash ('-'): `bill.gates@microsoft-corp.com`
- Brand name homograph: replacing 'O' with '0', 'l' with capital 'i', 'l' or 'L' with '1' ... : `bill.gates@1egit-company.com`
- Miss-spelled brand names: `bill.gates@nnicrosoft.com`
- Use of an uncommon domain: `bill.gates@microsoft.top`

More rarely, fraudsters falsify email headers, or even take control of the sender's email box.

## THE WARNING SIGNS

- Most of the warning signs come from **the subject or content of the email** itself (request for information, urgent transfer, change of account...), or from its unusual or unknown sender
- As a general rule, pay attention to the **email addresses of senders**, especially when the subject or content of an email is suspicious
- An email ending in your **spam box** is more likely to be a spoofed email
- Bad grammar or **spelling mistakes** are tell-tale signs; do not click links or open attachments

## PROTECT YOURSELF

### Vigilance when receiving an email

- In case of doubt about an email, do not reply; call your correspondent using verified details
- Learn to check email addresses carefully, in case of suspicious or sensitive requests, or in case of an unusual sender; for this, learn to read detailed email headers



READ MORE

*Instructions to read detailed email headers*

### Email authentication and filters

- Your IT department can monitor or reserve **domain names** similar to your company's
- They can also **filter emails which are not authenticated** with standard protocols: SPF, DKIM, DMARC; if necessary, blacklists and / or whitelists can be set up for specific domains
- If possible, external emails should be marked as such 'EXTERNAL'

## AND REMEMBER

The fraudster can usurp not only the email address of your correspondent but also yours. It sends you the answers it receives from your interlocutor, and vice versa. **The illusion is perfect.**



Crédit : Shutterstock



# CYBER RISKS

---



# PHISHING AND SPEAR PHISHING

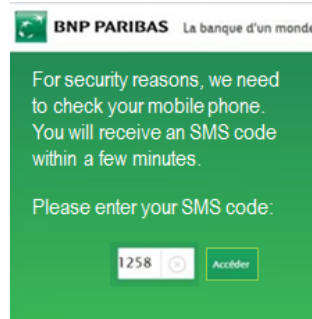
## EXAMPLE

You receive an email that appears to come from your bank. If you click on the link, a bogus page of the bank opens and asks for information (passwords, credit card number, etc.). Fraudsters can also steal an SMS code sent by your bank to validate an account or card purchase.

### You have new messages

**J**  **john@bnpparibas.com** Today at 9:02 AM  
**A:** kate@qwerty-analysis.com

Dear client,  
You have (2) new messages. Check your mailbox by clicking on the link below:  
[Your mailbox](#)



Phishing is very common, and can affect your **phone company**, your **electricity or gas supplier**, **administration**, your **email provider** (Gmail, Hotmail...), **social networks**, and more.

Info: we received a request for a new SIM card for your mobile contract. If you are not responsible for this request, please contact immediately the Help Desk at 12345



Fraudsters can also **intercept the code sent by SMS by your bank** by having a new SIM card sent by your telephone operator. This is known as **SIM swapping**.

## THE WARNING SIGNS

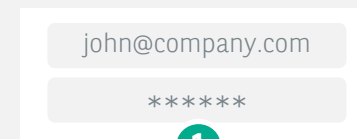
- An email that seems to come from an institution you have an establish relationship with (LinkedIn, bank, supplier, customer, tax authorities...), with a link or an attachment
- An unexpected request which seems to have a logical basis (invoice...)
- An alarming or inciting message urging you to open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

## PROTECT YOURSELF

### Develop sharp reflexes!

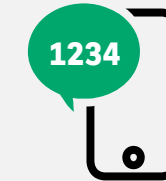
- Carefully check the **subject** and **content** of the email carefully (spelling, alarming message...), as well as the **sender's email address**, especially the domain
- As a general rule, do not open attachments and **do not click on any of the links or clickable images** provided in an email you receive
- To access your banking tool or social network app, always use the native app or use Favourites or input its usual address in your browser; check the presence of **https://** and the **lock icon**
- If by mistake, you click on a link in an email, do not sign in on the web site: **do not enter a password, or a code sent by SMS**
- **Do not open or reply to suspicious emails**; do not call any phone numbers given in these emails

Use strong authentication on your web banking site. Turn on 2-Step authentication on Gmail, Hotmail, LinkedIn, Facebook, Apple...

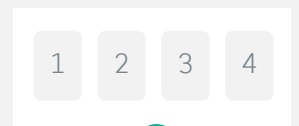


1

You enter your ID and password as usual



We send a **verification code** to your device.



2

You enter the code to verify your identity

## AND REMEMBER

- If you encounter a **default on your mobile phone** (prolonged loss of network, invalid SIM card), you may be victim of **SIM swapping**; contact your telephone operator
- **Spear phishing** is a phishing attack directed at specific individuals or companies to steal data, install malware, etc.; the sender may seem to be someone you know
- **Check links by hovering over the URLs**; the forwarding address is displayed at the bottom of your navigator)



BNP PARIBAS

The bank for a changing world

# MALICIOUS SOFTWARE INFECTION (MALWARE)

## EXAMPLE

Malware is malicious software is installed inadvertently and without your knowledge; usually by clicking a link or opening a document.

### Unpaid invoice – Urgent

**SC**  **Accounting department** Today at 9:02AM  
À: kate@qwerty-analysis.com

By checking your account, unless we are mistaken, the payment of our invoice F00012 for an amount of €300 has not been received. You can download a duplicate of the invoice at this address:

[Download my invoice](#)

We kindly ask you to settle it as soon as possible.

Hello,  
You will find attached the invoice still awaiting payment for an amount of €1927.80.



**department** Today at 9:02AM



## THE WARNING SIGNS

- Any email from **an unknown contact** with a link or attachment
- Any email with **an unusual subject** or **intriguing content**
- Any file sent by email or downloaded, **containing embedded macros**



**WARNING : We can all be the victim of malware infection. The consequences can be very serious: Espionage, data theft, fraudulent transfers, encryption of company data leading to bribery and possible operating losses.**

## PROTECT YOURSELF

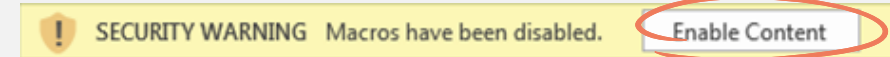
### Upon receiving an email

- 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**
- 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

### If you open an attachment or download a file:

- Do it on a workstation protected by antivirus, not on your smartphone
- Do not activate the content or allow the execution of **macros**:

**Do not click!**



### Protect your computer systems

- Update your operating system and antivirus **daily**
- Restrict software installation rights** to administrators
- Do not allow automatic **macro execution** or opening of attachments
- Block USB sticks** and file sharing sites
- Filter attachments** containing Visual Basic code (macros)
- Check **Remote Desktop Protocol** security (VPN or strong password) and beware of **website security breaches** (e.g.: contact forms)
- Avoid surfing on unknown websites (forum, blog, social network, marketplace etc.)
- If possible, **segment** your computer network

## AND REMEMBER

- Antivirus software often does **not detect malware**
- Fraudsters often use **links forwarding to files** hosted on DropBox, Google Drive, ... or on hacked SME's website, to counter filters
- More and more malware/trojans can run on your computer without any action on your part, just by visiting a website with security vulnerabilities

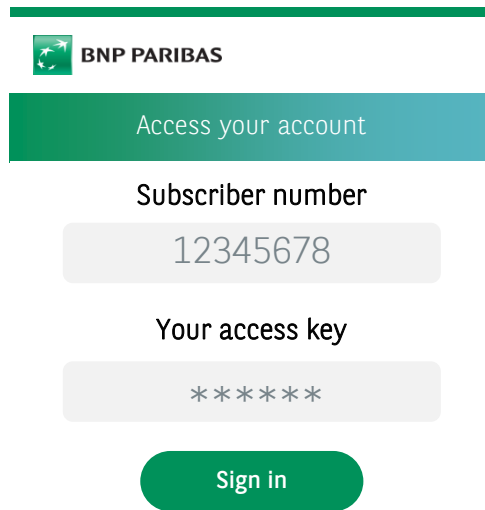


# "BANKING" MALWARE FRAUD

## EXAMPLE

Malware can create a transfer on your banking site. In particular, it can display a fake validation page to steal a validation code:

### Regular login page



BNP PARIBAS

Access your account

Subscriber number

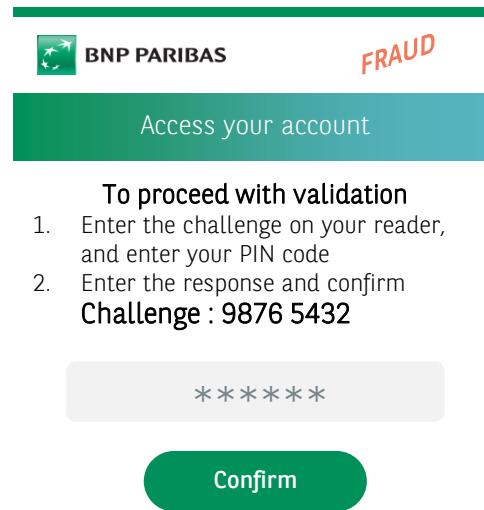
12345678

Your access key

\*\*\*\*\*

Sign in

### Bogus page: validation request at login



BNP PARIBAS **FRAUD**

Access your account

To proceed with validation

1. Enter the challenge on your reader, and enter your PIN code
2. Enter the response and confirm

Challenge : 9876 5432

\*\*\*\*\*

Confirm

## THE WARNING SIGNS

- Unusual **validation page**, or appearing after a period of unavailability of the banking tool
- Successive and potentially abnormal **authentication failures**
- **Slowness**, abnormally high network traffic, higher disk activity and/or file changes can be a sign of infection on your hardware

## PROTECT YOURSELF

### Use your payment applications properly

- Do not connect when hacking or malware is suspected; if in doubt, contact your **relationship manager**
- **Log off** from your application and remove your validation tool after each session. Also delete the navigation data present on your browser
- Never disclose your **ID, passwords, codes of validation**, etc. to anyone, by any means whatsoever
- Avoid connecting from a **private PC or smartphone** or from a **public Wi-Fi network**
- If you use payment file transfer, avoid manual steps as far as possible (to prevent a fraudster altering a payment file)
- If possible, make payments on PCs dedicated only for that purpose

### Segregate duties

- Always ensure a minimum of dual control on payments and vendor management
- Segregation of duties is not 100% safe against banking malware, but it is often effective

### Protect your IT installations

- Update your operating system and antivirus **daily**
- See other tips on page 18

## AND REMEMBER

- Deloitte: "When we perform **intrusion tests**, we can access treasury systems in 80% of cases; unless everything is encrypted, it is usually possible to modify amounts and supplier account details"
- "**Secure Flows**" payment watch solution provide additional country and account controls independent of your information system; it is available in France and will be rolled out in other countries

# A MAJOR RISK: RANSOMWARE

## EXAMPLE

Malware spreads across your computer network, and encrypts all files. It displays a message demanding the payment of a ransom, in exchange for a cryptographic key to decrypt your data.



## THE WARNING SIGNS



- Any suspicion of malware infection (for example: a macro in a suspect document has been executed by an employee...)
- A page telling you that your data has been encrypted

## PROTECT YOURSELF

### In case of attack

- Disconnect all infected PCs from the network to stop the attack
- Authorities strongly advise not paying any ransom

### Prevention

- Make regular backups of important data
- Strictly control access to the backup storage directory (ransomware may encrypt backups)
- Regularly store disconnected backups
- Regularly test your backups

### Prepare an action plan in case of an attack

- Talk in advance with your IT manager
- Plan a backup plan for your vital processes
- If possible, purchase cyber insurance, to cover expert assistance, operating loss, etc. and to give you access to 24/7 expert support

## AND REMEMBER

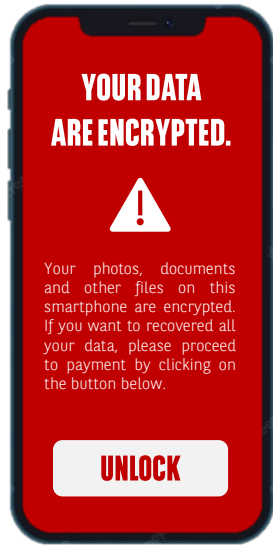
- Sometimes fraudsters threaten to publicly disclose compromised data if the victim does not pay a ransom
- In general, the cost of an attack is at least €40,000; the highest damages amount to hundreds of millions of euro



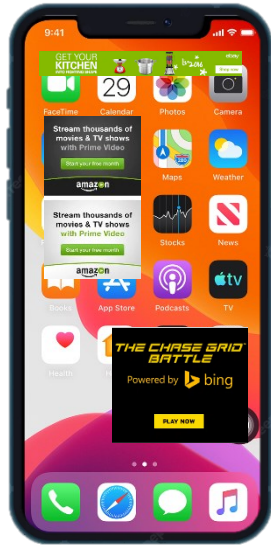
# SMARTPHONES: THE NEW TARGET

## EXAMPLE

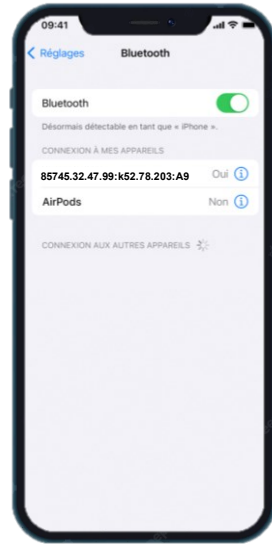
Android, IOS, WinPhone : any smartphone OS is totally secure. Our smartphones have a lot confidential informations (SMS, Mail, Photo, Social Networks etc.) and are often defenseless, a gold mine for a hacker!



Ransomware example



Adware example



Network hacking example

## SIGNS THAT SHOULD ALERT YOU



- **Ubiquitous ads** on your smartphone outside of your apps
- Registered **unidentified Bluetooth** devices on your smartphone
- Apps **installed** outside the official stores
- Unusual **calls or messages** in your logs

## PROTECT YOURSELF

- **Avoid risk**
  - Never download an application outside the official stores (Apple Store, Play Store)
  - Never run files: .apk, .ipa, .script etc... on your smartphone
  - Disable the NFC, Bluetooth and Infrared functions after use (for compatible phones)
  - Do not charge your smartphone on the self-service USB terminals
  - Check the legitimacy of an application's data access
  - Always enable two-factor authentication (2FA) if possible
  - Do not jailbreak your phone
- **In case of attack**
  - Notify anyone who may have received frauds messages from your phone
  - Change sensitive app (banking, social networks etc.) passwords
  - Quickly contact your phone's brand support
- **Prepare an action plan in case of an attack**
  - Make regular backups of your important data
  - Do not store your sensitive data or passwords on your smartphone
  - Avoid public wifi or unprotected internet networks as much as possible (or use a VPN)

## AND REMEMBER

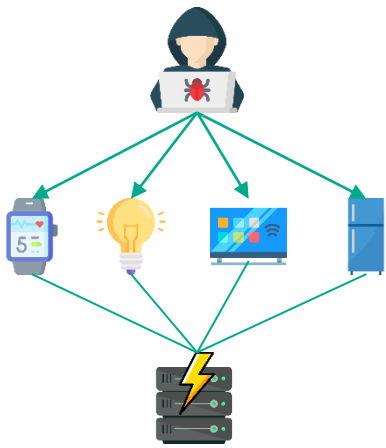
- 1 in 36 Android smartphones have risky apps installed (worldwide)
- Beginning of 2022, discovery of "Noreboot" techniques on iPhone which allows a hacker to remotely control the cameras and microphones of the smartphone without being detected



# CONNECTED OBJECTS, THE OPEN DOOR FOR HACKERS

## EXAMPLE

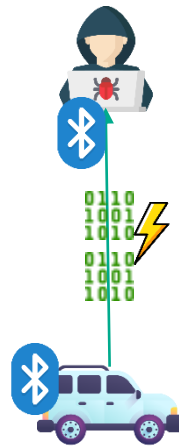
In recent years, the IOT (Internet of Things) have invaded our homes. The particularity of these devices: there are directly connected to the Internet. We can find televisions, watches, speakers, security cameras, light, refrigerators, baby monitors, etc. However, these devices are too often devoid of security systems !



DDoS Attack



Active listening



Data theft (Blueborne)

## SIGNS THAT SHOULD ALERT YOU

- Intensive use of your devices even when they are not in use (heat)
- Anomalous activity on your internet box (increased internet consumption)
- A change in the behavior of connected objects (change of language, error, etc.)
- Suddenly encrypted files on your device

## PROTECT YOURSELF

- **Avoid risk**
  - Disable the demo or guest accounts of your connected objects
  - Change the original IOT passwords for a stronger one
  - Implement encryption methods if possible
  - Avoid connecting your professional computer to a network with IOT, otherwise use the VPN provided by your company
  - Regularly update your devices to fix vulnerabilities
- **In case of attack**
  - Disconnect your devices from internet to stop the attack
  - Change the password of your devices
  - Make an update search for the latest security patches

## AND REMEMBER

- Your IOTs have, like your computer, an IP address visible to everyone on the web. A simple IP scan on the internet can find millions of unprotected connected objects
- The *Shodan* website can find all connected objects with an IP address visible on the internet (therefore unprotected)
- The *Insecam* website provides access to thousands of unprotected cameras in the world and the ability to consult them at any time

**! Even the least risky connected devices can be attacked. This is the case in 2020 with a wave of ransomware infecting connected coffee machines rendering them unusable if their owners did not pay the ransom.**

# CONCLUSION

---



# DEVELOP SHARP REFLEXES & USE COMMON SENSE!

## In case of unusual credit transfer requests

- Inform **Senior Management**
- Always follow due process no matter the perceived emergency
- Follow **segregation of duty** principles
- Check your correspondent's identity using **verified contact details**

## In case of vendor bank detail modification

- Check your correspondent's identity using **verified contact details**
- Also check in case of **contact details modification**
- If the account is domiciled **abroad**, and for your **largest vendors**, be extra vigilant

## In case a technician wants to help

- Contact your **relationship manager** (or software vendor) using verified contact details
- Do not give **remote access** to your PC
- **Do not perform payment tests** over € 1
- Never give any codes to anyone, not even the bank

## In case of a request for information

- Never give information to **people you do not know**
- Beware if someone asks you for **accounting information**
- Check your contact's identity using verified contact details, or via the switchboard

## On social networks and outside the company

- Be discreet on **social networks** and outside your company, regarding your role and function
- Do not publish **information useful to fraudsters** (charts, news about CEO's trips, letter templates, signatures...)
- If possible, use **different signatures** for bank orders than those available on publically available documents

## In case of email reception

- Carefully check the **subject, content** and sender's **email address**
- **Do not click on links in emails**: always use the native app or website; if by mistake, you click on a link in an email, **do not enter any information**
- If possible, do not open attachments or downloaded files; if you open a file, **do not enable content or execute macros**

## When using your banking application

- **Segregate duties**, use limit amounts, do not use paper orders and validation
- Avoid connecting from a **private PC** or smartphone or a **public Wi-Fi** network
- **Log off** from your application and remove your means of validation after each session
- Do not log on when malware is suspected (fake validation pages, unusual failures...); if in doubt, contact your **relationship manager**

## Protect your IT installations

- **Update** O.S. and antivirus daily
- **RDP security** (VPN or passwords)
- **Website security** (e.g. contact forms)
- If possible, **segment** your computer network
- **Block USB sticks** & file sharing sites
- **Filter emails** and attachments, and check email authentication (SPF, DKIM, DMARC)
- Make regular and tested **backups**
- Watch domain **similar** to yours
- If possible, encrypt sensitive data and use TLS for external emails



# IN CASE OF FRAUDULENT TRANSFERS (OR SUSPICION)



1

Notify your management and preserve evidence

 EMERGENCY CALL LIST



2

Contact your relationship manager immediately

 EMERGENCY CALL LIST



3

Contact the police and file a complaint in case of a successful fraud

 EMERGENCY CALL LIST

# DISCLAIMER

---

THIS DOCUMENT HAS BEEN PREPARED BY BNP PARIBAS FOR INFORMATIONAL PURPOSES ONLY. ALTHOUGH THE INFORMATION IN THIS DOCUMENT HAS BEEN OBTAINED FROM SOURCES WHICH BNP PARIBAS BELIEVES TO BE RELIABLE, WE DO NOT REPRESENT OR WARRANT ITS ACCURACY, AND SUCH INFORMATION MAY BE INCOMPLETE OR CONDENSED. THIS DOCUMENT DOES NOT CONSTITUTE A PROSPECTUS OR SOLICITATION. ALL ESTIMATES AND OPINIONS INCLUDED IN THIS DOCUMENT CONSTITUTE OUR JUDGEMENT AS OF THE DATE OF THE DOCUMENT AND MAY BE SUBJECT TO CHANGE WITHOUT NOTICE. CHANGES TO ASSUMPTIONS MAY HAVE A MATERIAL IMPACT ON ANY RECOMMENDATIONS MADE HEREIN.

THIS DOCUMENT IS CONFIDENTIAL AND IS BEING SUBMITTED TO SELECTED RECIPIENTS ONLY. IT MAY NOT BE REPRODUCED (IN WHOLE OR IN PART) TO ANY OTHER PERSON WITHOUT THE PRIOR WRITTEN PERMISSION OF BNP PARIBAS.

© 2024 BNP PARIBAS. ALL RIGHTS RESERVED.



**BNP PARIBAS**

The bank for a changing world