BNP PARIBAS

The bank for a changing world

PREVENT FRAUD TARGETING YOUR SUPPLIERS: WATCH OUT FOR INVOICE THEFT

Be vigilant to prevent the theft of invoices you issue. These may be stolen and modified to swindle your customers. Find out how fraudsters can go out stealing your invoices and diverting payments intended for you, and put measures in place that will protect your company.

YOUR CUSTOMERS CAN ALSO FALL VICTIM TO SUPPLIER FRAUD

A common scam involves making a fake request to change bank details: the fraudster pretends to be your accountant and asks your customer to change details of the account your company uses to take invoice payments. They may use one of the reasons below:

- a change of bank;
- an organisational change;
- use of a factoring agreement;
- the sale of the premises you rent, etc.

This is how they can misappropriate money intended for you.

INFORMATION THEFT, A PRECONDITION FOR VIRTUALLY ALL FRAUD

To ensure the scams succeed, the criminals must first steal information from you, such as:

- details of unpaid invoices;
- payment due dates;
- customer lists and correspondence details;
- bank account numbers;
- the identity of the person who sends out invoices, etc.

Fraudsters can infiltrate your company's information system in order to carry out the theft, which is why you must scrupulously protect your invoices and customer files.

IMPERSONATION – ANOTHER MUCH EASIER TECHNIQUE USED TO DEFRAUD

The simplest way to steal invoices from you is to pretend to be your customer's accountant. For example, a person contacts you by e-mail, mail and/or telephone to let you know that invoices have either not been received or have been mislaid, and asks you to re-send all those not yet paid.

Scammers can take other identities to steal information from you: an auditor, a tax inspector, a public administration asking you for information about your largest clients and your invoices, about your professional premises and the amount of your rent, etc.

Here is an example of an email sent by a fraudster to steal invoices - note: the name of the inspector refers to a real employee of the DGFIP, and the domain name of the address used by the fraudster (dgfip-financesgouv.com) closely resembles that of the DGFIP (dgfip.finances.gouv.fr):

From: DGFIP - Direction générale des Finances publiques [mailto: [redacted]@dgfip-financesgouv.com]
Sent: Wednesday, October 23, 2017 at 3:44 PM
To: [redacted]
Subject: [redacted] - VAT Declaration 3310/CA3

Dear Sir,

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 suppliers (excluding intra-group).
- The amount (excluding taxes) of purchases made by these 2 suppliers each month, over the last 3 months.
- The payment due date (every 15th, 30th or other of each month), as well as the payment method.
- Provide for each supplier an account statement for the period indicated, as well as a duplicate invoice.

The VAT refund application constitutes a contentious claim within the meaning of article L190 of the Book of Tax Procedures.

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

Best Regards,

[redacted]
Public Finance Inspector
Expertise Control Center
139 Rue de Bercy
75012 Paris
Tél. : 01.40.04.04.04
[redacted]@dgfip.finances.gouv.fr

HOW CAN YOU PROTECT YOURSELF FROM INFORMATION THEFT? VERIFY THE REQUEST

You should be suspicious of any person asking you for invoices or information, be they apparently a customer, auditor, tax inspector, market researcher, banking technician, etc. Verify their identity by contacting them using safe contact details:

- Do not reply to their e-mail directly. Instead, call the person back on a telephone number you know to be correct (not that indicated in the message), or via the firm's switchboard.
- If you receive a call, e-mail the individual using an address you know to be correct, asking for confirmation of the request.

As a general rule, be on your guard if contacted by somebody you do not know. Take all steps necessary to verify the identity of the individual before entering into any professional relationship.

Do not hesitate to halt the call on the pretext that you are unavailable, especially if an unfamiliar person calls you. Take the person's contact details, hang up, then check the details they gave or call them back through their telephone switchboard. Get into the habit of checking the e-mail addresses of your contacts: display the details of the sender's e-mail and look closely at the domain name (after the @). Ensure that what appears is a genuine domain name.

For example:

- john.qwerty@qwerty-brewery.com <john.qwerty@presidency.com> is undoubtedly a fake as it uses a misleading alias and a domain name unconnected with the company.
- John Qwerty <john.qwerty@qwerly-brewery.com> is suspect, as the domain name is close but not identical to the real one, differing by just one character.

Take the habit to check email headers. Find some instructions on **Google help centre**.

Finally, speak openly to those around you about the risks of fraud and alert your most important customers. Ask them to check carefully any request apparently made by your company to amend the details of a bank account.