BNP PARIBAS

The bank for a changing world

FAKE TECHNICIAN SCAM: A VICTIM'S STORY AND ADVICE TO HELP YOU PROTECT YOUR COMPANY

The fake technician scam is not very well known. Yet it is currently one of the most widely used scams targeting SMEs in particular. The story of Jean-Paul and Joëlle, whose company almost fell victim to the scam, shows how the fraudsters operate. Remind your employees of the risks and how they should behave if they are called by a technician.

"MR LUCAS FROM BNP PARIBAS SPEAKING"

"At around 4pm one Friday afternoon, we were contacted by somebody calling himself Mr Lucas from BNP Paribas, who asked to speak to the accounting department. Joëlle, who is responsible for payments, took the call.
"Mr Lucas explained to her that the site we use to make our payments was to be migrated to a new version. Joëlle had to answer a number of different questions on the way we operate: manual transfer or file import, who handles validation and how, and so on."

"HE HAD ALREADY CALLED ME A FEW MONTHS EARLIER"

"The reason I wasn't suspicious," adds Joëlle, "was that he was very well spoken, was very familiar with my tool and had already called me a few months earlier. The number displayed was a 800 number.
Despite all his questions, the man was very courteous and competent. He focused in particular on finding the best timing for the migration in order to minimise the impact on us, since the service would be inaccessible for 48 to 72 hours, he explained."

REMOTE ACCESS TO THE COMPUTER

"Another technician, Mr Martin, called me regarding the migration itself. He sent me a link that would give him remote access to my computer. I clicked on the link and then he gave me a session code that I entered on the interface.

This new technician spoke highly of the update. We then checked the configuration of my tool together: account statements, third-party management, upper limits and transfers."

"Before hanging up, he reminded me not to connect for three days and to make payments manually during the migration period."

MORE THAN €300,000 TRANSFERRED ABROAD

"When Joëlle told me on Monday morning that the BNP Paribas technician said we should not connect for three days, I thought that sounded dodgy," explains Jean-Paul. "I immediately contacted my relationship manager."

"He told me straight away that this was attempted fraud. He explained that migrations always take place during a weekend and that BNP Paribas never conducts an update online."

"We detected a fraudulent transfer of more than €300,000 to another country. Fortunately though, the bank was able to block the funds and we'll be reimbursed soon. I contacted the police on the same day to make a complaint."

"We were lucky. Otherwise, the consequences would have been terrible for the company as well as for Joëlle. She was very shaken and has now become extremely suspicious, believe me. As for me, I distributed the training kits provided by BNP Paribas among all my employees."

SIGNS TO WATCH OUT FOR:

- Any operator **offering you assistance** or a migration, a SEPA test, etc. relating to your payment tools if you have not personally sought an intervention (e.g. Mr Lucas, Lambert, Faure, Martin, Vigot, and so on)
- **Questions regarding your tools or payment processes**
- **An unfamiliar link** (for example, web address shorteners such as www.id5.com/bnp, www.tin.com/sepa08, www.is.gd/sepabnp, www.tinyurl.com/migration, etc.)
- A request to **obtain remote access to your computer** (for example through a service such as GoToAssist, ntrsupport.com, etc.)
- A suggestion to carry out a **test transfer**

PROTECT YOUR COMPANY AND YOUR EMPLOYEES!

- **Contact your relationship manager through the usual contact channels** to check the identity of anyone claiming to be a member of our teams.
- **Do not give remote access to your computer to anyone whose identity you are unsure of:** do not go to a website and do not click on a link.
- **Never carry out any test at the request of a technician:** do not add a third-party account or validate a transaction or remittance. Never carry out a test involving more than €1, even on your own initiative.
- **Never give any code to anyone** (e.g. the number generated by your wireless card reader, password or PIN, etc.).
- **Protect your computer network and PCs** from intrusion and malware.

And in general, **remind your employees of the following rule:** if an unfamiliar person calls you, do not hesitate to halt the call on the pretext that you are unavailable. Take their contact details, hang up, then check the details they gave or call them back through their telephone switchboard.

REMEMBER

- No BNP Paribas technician **should ever contact you** to carry out any update or maintenance, tests, and so on, unless you have personally requested the assistance of support teams.
- **Fraudsters are very familiar with banking tools:** they often know when servicing periods are scheduled, which commercial transactions are under way, and even the name of your bank relationship manager.
- To take advantage of you all the more readily, **the fraudster may make preliminary calls** during which they provide assistance without defrauding you.
- The fake technician may not necessarily claim to be from your bank; the fraudsters can also **pretend to represent your software vendor** or Microsoft, for example.