Why can invoices be temporarily blocked at Hoffmann & Partner?
blocked at Hoffmann & Partner?
An example of cyber security measures in practice

Cybercrime remains one of the biggest challenges for companies. In calendar week 33/2024 alone, the Federal Office for Cyber Security (BACS) in Bern recorded 711 reports of cyber incidents!
At Hoffmann & Partner, we have already taken several measures this year to protect our clients from threats such as CEO fraud and invoice manipulation.
Here we would like to give you a real-life example of protection against invoice manipulation:
In a recent case, one of our customers received an invoice from a long-standing supplier in Germany. At first glance, everything seemed fine, but on closer inspection we noticed two details: The layout of the invoice was slightly different and the IBAN differed from previous invoices in two numbers.

An example:
- Previous IBAN: DE89370400440532013000
- Changed IBAN: DE89370400440532031000

Due to the discrepancies, we temporarily blocked the payment until the situation was clarified. After consulting with the supplier, it turned out that it was an annoying typing error. The payment could not have been executed anyway due to the incorrect check digit, but the check was still important to rule out potential fraud.

We remember a CEO fraud in December last year, where fraudsters managed to open an account in a similar company name at a bank in Germany and to obtain money with a manipulated invoice. Remember: The bank is not obliged to check whether the IBAN matches the recipient's name!

Our practical recommendations:

- **Four-eyes principle**: double-checking can prevent fraud.

- **Check initial invoices and changed IBANs**: Contact the supplier by telephone, but do not use the telephone number on the invoice - this could be a fake. Instead, use information from the supplier's official website.

- **Account protection**: Use two-factor authentication (2FA).

- **Passwords**: Take advantage of a password manager and change passwords regularly.

- **Avoid ad hoc payments**: Plan payments carefully!
In a recent case, the fraudster posed as the CEO and asked the CFO to process an urgent payment. The fraudster wrote by email from the CEO's vacation home - thanks to social media, he knew where the CEO was. The fraudster instructed the CFO to quickly transfer a payment in connection with a major acquisition. He asked the CFO for absolute discretion.

- **Direct contact**: In the B2B sector, a phone call can offer more security than emails.

- **Regular IT security checks**: Check the security of your systems regularly with your IT service provider and consider taking out cybercrime insurance

Cyber criminals are constantly developing new methods to get their hands on your money. Hoffmann & Partner remains vigilant and works continuously to improve our security measures.

Our know-how - your advantage

Benefit from our many years of experience. We are at your disposal to inform you about secure and efficient processes.