Wumbel®

Fake letters

DR. BITTNER GROUP

When something comes at exactly the right moment...

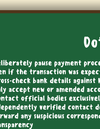
There are written letters and messages that, at first glance, appear completely unremarkable because they coincide exactly with a real-life event in terms of both timing and content. This exact match currently poses a major risk in day-to-day work, particularly in areas where payments are checked or authorised.

Fraudulent payment demands in circulation

There is currently a rise in fraudulent letters and emails in circulation that look identical to genuine correspondence from public authorities. The content often relates to actual processes within the company, such as a change of name, tax registration, or an alleged change to payment arrangements. The process is genuine, the letter appears plausible, and that is precisely why it is often not subjected to critical scrutiny. This modus operandi has long been known in the email sphere. However, fraudsters have now become more sophisticated and are targeting not only end customers but also businesses, as there is usually publicly available information about them. Whether it be a merger, a change in company structure or a change in management.

Why expectation is a gateway

Modern fraud no longer relies on chance, but on context. People are less likely to question information they expect to receive because it fits seamlessly into existing processes. Printed letters further reinforce this effect, as paper documents or letters from public authorities or banks are still perceived as official and binding.



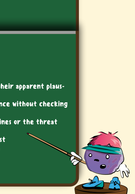
Who should be particularly careful

Areas particularly at risk are those where invoices are checked and payments are prepared or authorised. These include, amongst others, administrative roles, accounts, financial control, and anyone with payment authorisation. The risk does not arise from negligence, but from the deliberate exploitation of clearly defined roles and processes.

Typical characteristics that give a false sense of security

- **Refers to a real, recent event**
- **Uses the names of real government agencies and official titles**
- **Professionally designed with genuine logos, reference numbers and formal language**
- **Payment demands with deadlines or formal pressure**
- **Payments via a QR code**

Familiar features from official correspondence often give a false sense of security. However, the increased professionalism of fraudsters makes it necessary to remain vigilant and check the details carefully.



Discrepancies that give rise to particular mistrust

Every forged letter will contain (sometimes subtle) inconsistencies that fraudsters exploit, whether it be altered account details or a letter arriving too soon after the genuine one.

The following points may provide some insight:

- **Bank details with a foreign IBAN or unusual account information**
- **The letter or message is sent too soon after the transaction to which it refers**
- **The deadlines specified are very short and the consequences unusually severe**

What you should always check before making a payment!

Do's

- Deliberately pause payment processes briefly to check them, even if the transaction was expected
- Cross-check bank details against known master data
- Only accept new or amended account details after verification
- Contact official bodies exclusively using known, independently verified contact details
- Forward any suspicious correspondence internally and ensure transparency

Don'ts

- Approving payments solely on the basis of their apparent plausibility in terms of timing
- Copying account details from correspondence without checking them
- Allowing yourself to be pressured by deadlines or the threat of consequences
- Treating paper as an automatic sign of trust
- Ignoring minor discrepancies because they appear insignificant at first glance

Conclusion: this issue affects everyone in the company!

Such fraud attempts are often based on publicly available information and known or recently published company procedures. Remaining vigilant during the payment process is therefore part of a comprehensive strategy to protect company assets, internal information and personal data. Every fraud attempt that is detected reduces financial loss and also protects the organisation as a whole. If letters or messages arrive exactly when they are expected, this is not proof of authenticity but a reason to take a closer look.

Wumbel

Dr. Bittner Consulting
GmbH & Co. KG
Podbielskistraße 386
30659 Hannover
Servicenumber: 0800 88446688
Email: office@drbg.de

DR. BITTNER GROUP