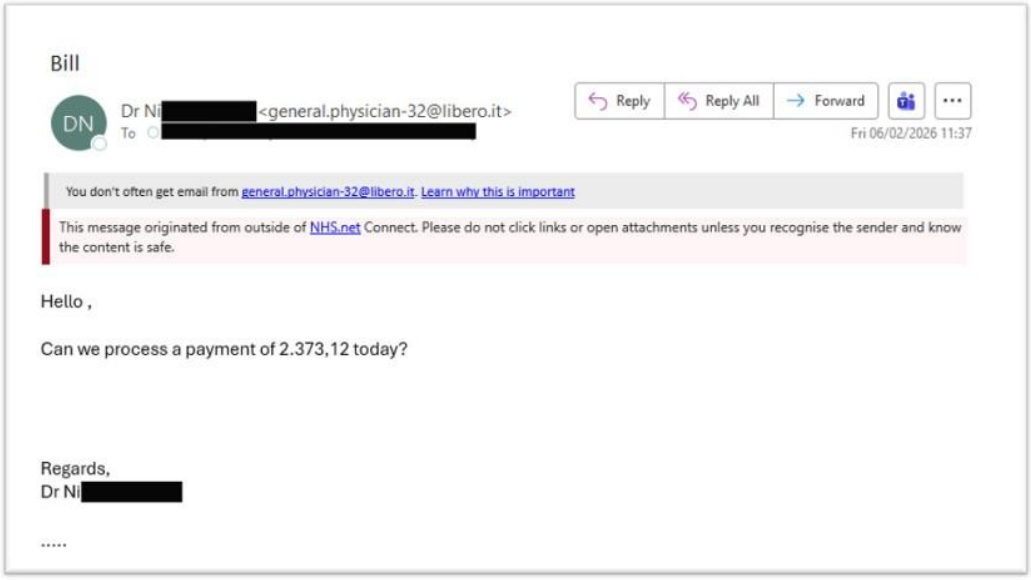
GP Fraud Alert

Our counter fraud provider has alerted us to a recent email impersonation scam that targeted a GP practice. This is part of an ongoing series where fraudsters pose as senior partners, practice leaders, locums or clinicians, using spoofed or look-alike email addresses to request urgent, high-value bank transfers.

This recent attempt resulted in a part payment being made before the fraud was identified. We are sharing the emails below to help you identify the fraud should your practice be targeted. It is important that any practice staff that are able to make payments are aware of how to recognise it as fraudulent should you be targeted. Please share this with your team:

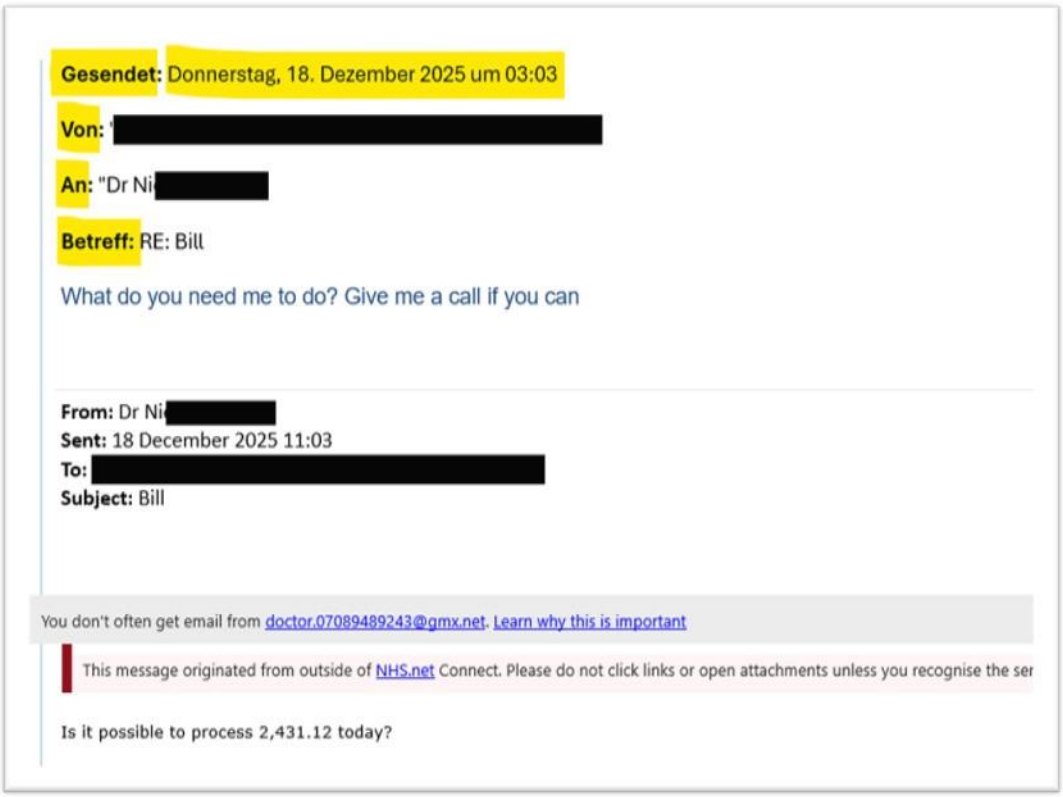
Email 1

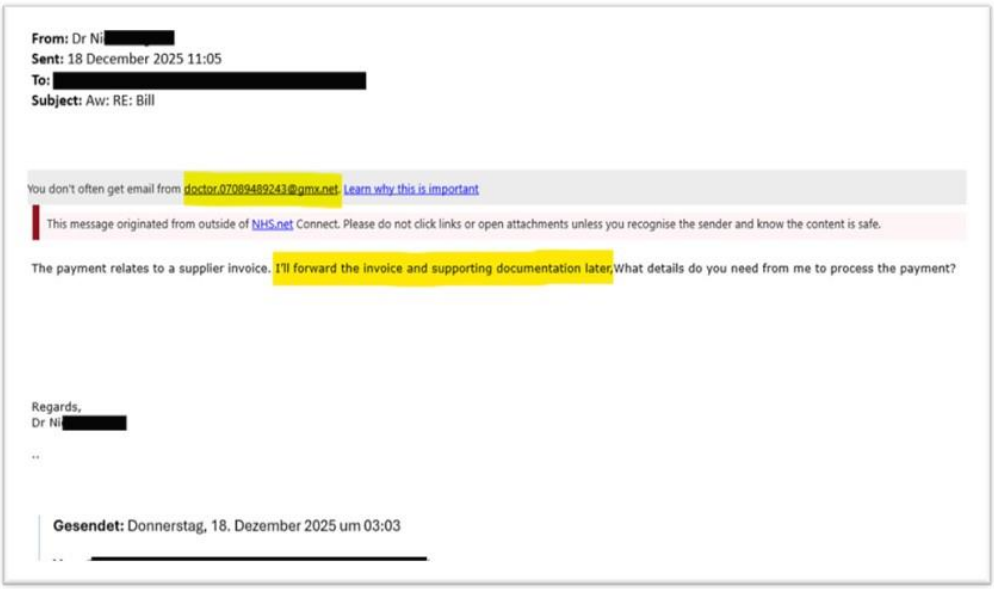


Key warning signs observed:

- Messages sent from non-NHS accounts (e.g. free email providers such as gmx.com, libero.it)
- NHS security banners warning the message is from an external source
- Requests for same-day payment or urgent action
- Lack of invoice, purchase history or supporting documentation

Response trail





Key warning signs observed:

- Some words in the email trail appear in a different language – this is as the recipient has their default language set to another language, in this case German.
- Unusual time showing – this occurs when the recipient's default time is set in a different time zone, indicating they are overseas.
- External email warning displays a different email address to the one expected – this occurs when the fraudsters 'spoof' the email name, making it appear to come from a different domain.
- Large number of digits used in the email address – emails addresses are finite and as they get reported they are blocked. Fraudsters need to generate numerous free email addresses so they are often forced to add a series of numbers to obtain an available unique address.
- Sense of urgency – fraudsters want you to act before you realise it is suspicious, or speak to the real doctor. They will often encourage an urgent payment with the promise of approval/ back up data being sent later.

Actions required:

- Flag any unexpected or unusual email requests for payment, especially those appearing to come from senior partners, GPs or practice leaders.
- Review any payment requests thoroughly to ensure the goods or services were legitimately ordered and received before making payment.
- Verify any requests for payment with the authoriser using an alternative communication method, such as face-to-face, telephone or nhs.net.
- Do not act on payment instructions received from non-NHS or free email providers (e.g., gmx.com, libero.it), even if the sender's name appears familiar.
- Refer any suspicious payment requests or impersonation attempts to your ICB's LCFS, or the NHS Counter Fraud Authority.