Fraud awareness for businesses

There is, unfortunately, an ever-present risk of fraudulent activity that targets businesses. Often the methods that are used are not particularly sophisticated, and they can affect companies of all sizes. This leaflet aims to highlight two of the more common methods of fraud so that you and your employees reduce the risk of falling victim to them, as once these payments are made, it is often unlikely that the money will be recovered.

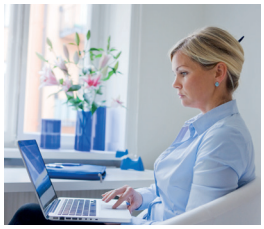
These are known as **"Invoice Redirection Fraud"** and "**CEO Fraud**".

Invoice Redirection Fraud

Invoice Redirection Fraud involves intercepting and then amending an expected payment request or invoice.

The fraudster may hack into a seemingly genuine email chain and provide replacement – but fraudulent – bank details for a genuine payment that is due to be made. Usually, either the genuine invoice has been replaced with one containing fraudulent bank details, or the victim receives an email asking for the payment to be sent to a new bank account. The intended outcome is the same: the payment is sent to the fraudster's account.

The fraud is often not spotted until a few days later when checks are made, or when the true recipient chases up a 'missing' payment.



CEO Fraud

CEO Fraud happens when a member of staff receives an email that appears to have come from an owner/director/colleague requesting that a payment is made. These email requests appear to be genuine but are sent by the fraudster as they have hacked into or imitated the person's email account. The member of staff takes the email at face value (without separately speaking to the owner/director/colleague) and makes the payment based on the email details to an account that the fraudster controls.

Best practice and fraud prevention

All businesses can be at risk from these frauds, but the following steps can reduce your vulnerability:

- Validate the bank account details personally with the genuine recipient on all requests for payment that are new to your business, or where you are advised that the bank account has changed
- Protect commercial information. If you wouldn't send it on a postcard, don't send it by unencrypted email
- Ensure that email accounts have a unique and complex password
- Use dual authority internet banking mandates to introduce a second line of checks
- Check that internet banking authorities for staff are set at appropriate levels
- Maintain up to date anti-virus software
- Have clear internal procedures within your business to specify how payment instructions are carried out

Finally, if you believe you are a victim of one of these scams, please contact your branch immediately.

handelsbanken.co.uk

Handelsbanken

Handelsbanken is the trading name of Svenska Handelsbanken AB (publ). Registered Office: Svenska Handelsbanken AB (publ), 3 Thomas More Square, London, E1W 1WY. Registered in England and Wales No, BR 000589. Incorporated in Sweden with limited liability. Registered in Sweden No, 502007-7862. Head Office in Stockholm. Authorised by the Swedish Financial Supervisory Authority (Finansinspektionen) and the Prudential Regulation Authority and subject to limited regulation by the Financial Conduct Authority and Prudential Regulation Authority. Details about the extent of our authorisation and regulation by the Prudential Regulation Authority, and regulation by the Financial Conduct Authority are available from us on request.