



Invoice/mandate fraud – Fact Sheet

In 2018, UK Finance reported that businesses had lost over £93m to invoice fraud.

How does it work?

Someone claiming to be from a regular supplier contacts you unexpectedly. They state that their bank account details have changed and ask you to change the payment details. You could also be contacted with a false invoice that is under your authority limit. A number of payments can be made before the scam is spotted.

How could you be contacted?

- Email
- Text message
- Phone call

Spot the signs

- Unusual financial request
- Poor spelling and grammar
- Unusual English (possibly translated from another language)
- Company logo and address add validity
- Errors in spelling of the company name and email address



Google Ireland Limited
Gordon House, Barrow Street,
Dublin 4
Ireland
Número de TVA: IE0388047V

Attention : Accounting Department

SUBJECT : Change of Bank Information

Dear

We kindly ask you to settle your bank account details for all of your Adwords accounts and billing.

ACCOUNT NAME	HYSOCBANK
BANK NAME	HSBC London
IBAN	GB33MIDL40051569113953
SWIFT	MIDLGB22
CLEARING CODE	BEVP050E

We wish you good reception.

Cordially,

Stop, Challenge, Protect

Think about what you are being asked to do, do you have an account with this company? Could this be fraudulent?

Contact the company using a phone number or an email that you have used before to ensure that it is a genuine request. If in any doubt, contact your manager.

Report any suspicious communication to Action Fraud and if you think you have been scammed, contact your bank.



TO STOP FRAUD™