# Payment diversion fraud

**Payment Diversion Fraud (PDF), also known as Business Email Compromise (BEC), tends to affect businesses and customers where electronic financial transactions are taking place.**

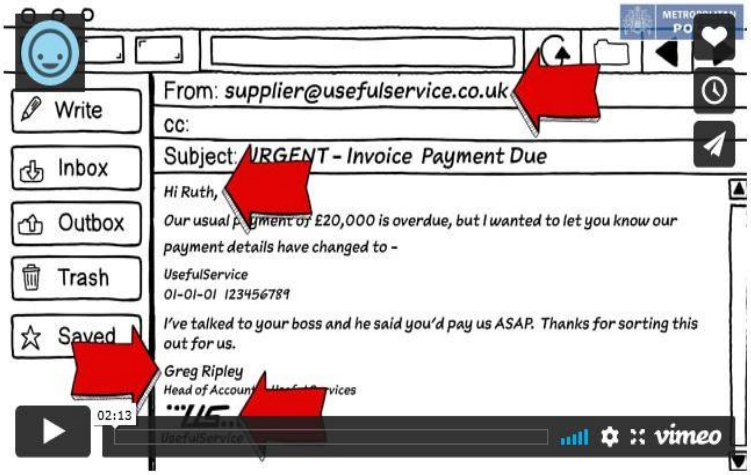

**What is Payment Diversion Fraud?**

Payment Diversion Fraud (PDF), also known as Business Email Compromise (BEC) or Mandate Fraud, affects businesses and customers where electronic financial transactions are taking place.

Criminals will contact businesses or customers via email, usually claiming to be from a company that the business or customer has been dealing with. They will request a payment to be made often or inform the recipient of a change of bank account details.

Criminals will often create fake e-mail addresses which are very similar to genuine business or customer addressees and send over fake invoices to make it more believable. All of this leads to payments from businesses and customers directly into bank accounts controlled by the criminals.

Criminals are experts at impersonating people and will spend hours researching you for their scams. Stop, think and follow the Take Five to Stop Fraud advice as it could protect you and your money.




Click on the below link to watch the video:

https://player.vimeo.com/video/547456909?

**Take Five to Stop Fraud advice**

**Advice for individuals**

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

**STOP:** Taking a moment to stop and think before parting with your money or information could keep you safe.

**CHALLENGE:** Could it be fake? It's ok to reject, refuse or ignore any requests for your financial or personal details. Only criminals will try to rush or panic you.

**PROTECT:** Contact your bank ***immediately*** if you think you've fallen for a scam, don't feel ashamed or embarrassed - you are not alone.

**Report it to Action Fraud online at www.actionfraud.police.uk/reporting-fraud-and-cyber-crime or by calling 0300 123 2040.**

If you're in Scotland, you can report to Police Scotland by calling 101.

**Advice for businesses**

Criminals are experts at impersonating people, businesses and the police. They spend hours researching your business for their scams, hoping you will let your guard down for just a moment.

**STOP:** If you receive a request to make an urgent payment, change supplier bank details or provide financial information, take a moment to stop and think.

**CHALLENGE:** Could it be fake? Verify all payments and supplier details directly with the company on a known phone number or in person first.

**PROTECT:** Contact your business' bank ***immediately*** if you think you've been scammed and report it to Action Fraud.

Advice can be found on the Take Five website addresses here:

https://takefive-stopfraud.org.uk/advice/general-advice/

https://takefive-stopfraud.org.uk/advice/business-advice/

**Improve your cyber security with NCSC Cyber Aware**

Use the 6 NCSC Cyber Aware actions to keep yourself safe. Further details of these are available at www.cyberaware.gov.uk, these are:

1. Use a strong and separate password for your email.
2. Create strong passwords using 3 random words.
3. Save your passwords in your browser.
4. Turn on two-factor authentication (2FA).
5. Update your devices.
6. Back up your data.

**Downloadable resources**

Business Email Compromise (BEC) Flyer (English version)

Business Email Compromise (BEC) Flyer (Welsh version)

Conveyancing Fraud Flyer (English version)

Conveyancing Fraud Flyer (Welsh version)

Conveyancing Fraud Flyer (Scottish version)