PAYMENT FRAUD

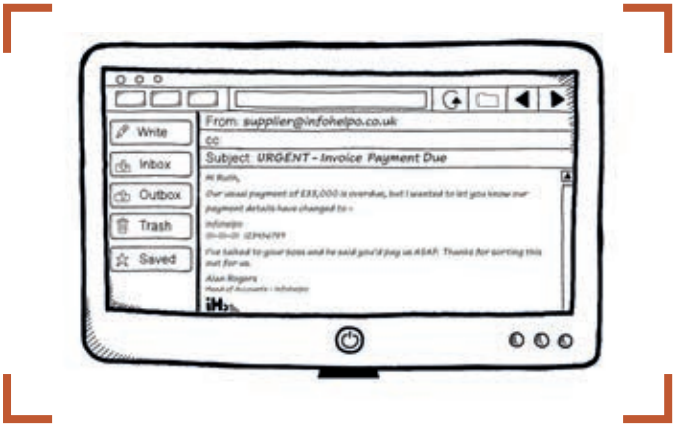
Payment fraud is a specific type of fraud which targets businesses with the intention of getting them to transfer money to a bank account operated by the criminal.

There are two main types of payment fraud, CEO fraud and Mandate Fraud. Both are usually targeted at staff within a company's accounts department and use spoofed sender email addresses (sometimes called Business Email Compromise).

CEO fraud involves an email that claims to be from a senior member of staff within a company such as a CEO (Chief Executive Officer). The email will ask the receiver to make a payment or transfer funds for an ongoing or new business transaction. Often the payment request is marked as urgent and pressure is applied to the receiver to make the payment as soon as possible.

Mandate fraud involves an email which appears to come from a known supplier. The email will request that future payments for products or services are made to a new bank account and give a reason for the account change.

In each instance, the new account will be under the control of the criminal and any funds paid in to it will be lost.



How to protect yourself

If an email is received requesting a change of bank details on an account or a one off payment, verify this by making direct contact with the organisation or person requesting the change. Ideally, phone them on a number you already have, failing that, double check the email used. Do not use any contact details from the suspicious email. Don't be pressurised by any email, or follow up phone call, as this may be the criminal. Always double check.

However, some criminals are getting wise to this, and so will prep a victim in advance by contacting them a few days or weeks earlier to change any stored phone numbers or emails to their own. So, it's a good idea to double check any contact when change of details occur. Make sure you double check via the original contact details.

Watch the Metropolitan Police's video on Payment Fraud at www.met.police.uk/littlemedia.

REMEMBER

Don't change bank details without double checking.

CAUTION

Sometimes, criminals will call in advance to fraudulently change contact numbers. Check when these change too.

THINK

Why does this payment have to be made?

PUSH PAYMENT FRAUD

Online banking makes managing money easier for the general public, however criminals are taking advantage of this ease of banking and using it to defraud the public.

Criminals can pretend to be from somewhere official, for example, your bank, or the tax office. They contact you via email, phone or social media, and then warn you of fake suspicious or criminal activity on your bank account. They state that they've set up a safe account for you to transfer your funds into. However, this is actually their account.

How to protect yourself

- ⚠ Be suspicious of a call out of the blue from someone claiming to be from a position of authority.
- ⚠ Take down the person's details (name, authority, department, branch etc.) and verify using independent source contact details.
- ⚠ A genuine official from the Police, your bank, HMRC or any other trusted authority will NEVER call you to ask you to verify your personal banking details, PIN or password, or threaten you with arrest.

- ⚠ Never transfer money into another account unless you are 100% certain of the owner of the account.
- ⚠ Your bank will never set up a “safe” account for you.
- ⚠ If you are a victim, contact your bank as soon as possible, as they may be able to help stop the transfer.
- ⚠ Watch the Metropolitan Police’s video on Impersonation Fraud at www.met.police.uk/littlemedia.

REMEMBER

Your bank will never set up a ‘safe account’.

CAUTION

Unless you definitely know who the account belongs to, it might not be safe.

THINK

Who told me this account was safe? Have I checked their identity?