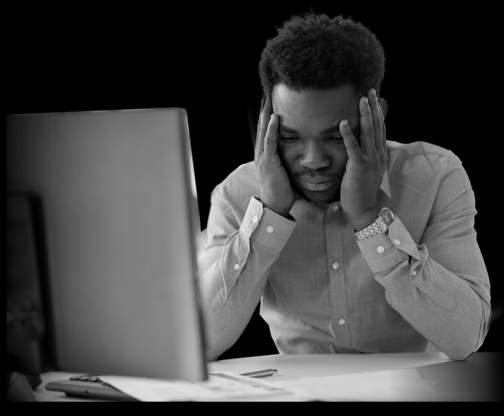
STOP! DON'T MAKE THAT PAYMENT.



PAYMENT DIVERSION FRAUD. KNOW THE DANGERS.

Payment Diversion Fraud (PDF) is where criminals target a specific individual, impersonate others, create or amend invoices and divert payments to criminal controlled bank accounts.

It affects everyone, though small and medium sized businesses are particularly vulnerable.

Make sure team members in finance, payroll and other departments which make payments are aware of the risk.
As year-end approaches, increased payments and workload make businesses more vulnerable.

Case study: City firm loses £340k after top PA's email is forged

A firm found 30 fake invoices, supposedly approved for payment to 21 different bank accounts.
Each invoice appeared to be from the CEO's personal assistant and had been sent to the Accounts Payable group e-mail box with authorisation for urgent payment.

After the company became aware of the fraud, internal enquiries established that the PA's emails were, in fact, 'spoofs', sent via an overseas website which helps criminals forge email addresses.

This successful fraud resulted in a loss of approximately **£340,000**.

Know the signs

- Have you been asked to urgently process a payment which is large or unusual?
- Or to change the bank details of an existing supplier, or set up a new supplier?
- Does the request contain spelling mistakes, errors or anything else odd?

Protect your business

- Think: is this request genuine?
- Verify emails or calls stating a change in bank details through an independent source – such as a phone call or in person.
- If you suspect you have been a victim of payment diversion fraud;
  - Contact your bank immediately.
  - Report to Action Fraud, visit actionfraud.police.uk or call 0300 123 2040. If in Scotland call 101 to report to Police Scotland.

NCA National Crime Agency

National Cyber Security Centre a part of GCHQ

ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk

A key component of Payment Diversion Fraud is Business Email compromise (BEC). Learn how to protect your business against BEC by following guidance from our partners in the National Cyber Security Centre:

What is business email compromise?

Business email compromise (or BEC) is a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information.

The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain viruses disguised as harmless attachments, which are activated when opened.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

Make yourself a harder target

Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing emails appear more convincing.

Review your privacy settings, and think about what you post across your social and professional accounts.

Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.

If you spot a suspicious email, **forward it to report@phishing.gov.uk,** or use the Report Phishing button in Outlook if you have it installed, and **then flag it as spam/junk in your email inbox.** Tell your IT department that you've identified it as potentially unsafe.

Will the emails **you send** get mistaken for phishing emails? Consider telling customers what they should look out for (such as '*we will never ask for your password')*

What to do if you've already clicked?

The most important thing is to not panic. Your IT department will have steps in place to help staff who think they've been phished.

If you think you've been a victim of a phishing attack, tell your IT department as soon as you can. The earlier you tell them, the more likely they'll be able to help.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult and will trick even the most careful user. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

Think about your usual working practices around financial transactions. If you get an email from an organisation you don't do business with, treat it with suspicion.

Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment to a particular account. Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?

Ensure that all important email requests are verified using another method (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person).

Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.

Some emails will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

STAY VIGILANT, STAY SAFE

To learn more about how to spot signs of payment diversion fraud, visit www.actionfraud.police.uk now.