Payment Diversion Fraud? What you need to know, and how to protect yourself.

- by Jon Shilland (NECC) & Andy Baguley (City of London Police)

We're all familiar with fraudulent emails that often litter our inboxes. With far-fetched promises about winning a Ferrari, or inheriting millions from a long-lost relative in a distant country, these attempted scams are often straightforward enough to see through.

Other fraud types are more insidious, and involve criminals deliberately targeting a specific individual. **Payment Diversion Fraud (PDF)** is a key example of this personalised, calculated crime.

PDF, also known as Business Email Compromise (BEC) or Mandate Fraud, involves criminals impersonating others, creating or amending invoices and diverting payments to bank accounts under their own control. This can target both businesses and individuals.

Why is PDF important and why now?

PDF is a significant threat to the UK economy with reported losses of around £152m in the year to September 2021, and over 4,600 individual cases. Businesses are particularly impacted by annual spikes in PDF that normally occur in March and November, and are associated with financial year-ends. PDF has been increasing and this trend is predicted to grow because of increased business activity associated with relaxing of Covid-19 restrictions, alongside the increased sophistication of fraudsters involved in PDF.

PDF affects all types of businesses and individuals. However, due to the targeted nature of this fraud type, small and medium sized businesses, which often have less comprehensive IT security, are particularly vulnerable. In addition, individuals that are purchasing houses and are involved in large financial transactions are also at risk. These two victim groups should be particularly vigilant to protect themselves against PDF.

Protect yourself and your business against PDF, by identifying the following red flags of PDF:

- Have you been asked to urgently process a payment that is large or unusual?
- Have you been asked to change the bank details of an existing supplier or to set up a new supplier?
- Is the language used in the email inconsistent with that of the genuine sender?
- Does the body of the email or email address contain spelling mistakes?

If you have any doubt about the transaction then do not transfer the money.

Protect yourself by, double-checking the payment request via an additional method using details from another source (such as text message, a phone call or in-person).

If you think you may have already been a victim of PDF, act fast! Immediately reporting the incident to your bank and Action Fraud (0300 1234 2040 or www.actionfraud.police.uk) gives you the best chance of recovering your funds.

Please visit the below webpage to download our Fact Sheet with further key advice/steps on how to protect yourself and your organisation from PDF:

Businesses:

Downloadable PDF fact sheet – (https://spaces.hightail.com/receive/WhbMzFSWw6)

Action Fraud PDF home page – (https://www.actionfraud.police.uk/a-z-of-fraud/payment-diversion-fraud)

Individuals:

Conveyancing Fraud flyer – (https://www.actionfraud.police.uk/a-z-of-fraud/payment-diversion-fraud)

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

A City of London firm found 30 fake invoices that purported to have been approved for payment to 21 different bank accounts to a total of £670,000.

All of the invoices appeared to be from the Personal Assistant (PA) to the company's CEO, and had been sent to the Accounts Payable group e-mail box with authorisation for urgent payment. All of these invoices were processed by the same member of the accounts team. While the company was able to stop some of the payments, this successful fraud resulted in a loss of approximately £340,000.

After the victim company became aware of the fraud, internal enquiries established that the e-mails purporting to be from the PA to the CEO were, in fact, 'spoofs', sent via a Czech-based spoofing website which helps criminals forge sender email addresses.

Additional enquiries established that the invoices were processed within minutes of their arrival to the accounts inbox, in contrast to normal working practices of processing similar invoices at least a day after.