Ulster Bank
Help for what matters

Detect and protect
Invoice Redirection

We're helping your business fight back against fraud and scams. A current threat you should be aware of is known as 'Invoice Redirection' – below we tell you how to spot it and how to protect your business against it.

Invoice Redirection

Fraudsters generally pose as a supplier or creditor and may advise you that their bank details have changed.

Spot the fraud

- Invoice redirection fraud usually happens when fraudsters identify key relationships between businesses
- A bogus instruction is created. Be alert, these requests can come via email, letter or via the telephone
- You may be asked to settle all future invoices to a new sort code and account number
- Funds are generally paid straight to the fraudster when the next invoice is due
- The original debt to the genuine supplier still stands

Protect your business

- Challenge any requests to amend account details
- Contact the supplier or creditor to independently verify the request
- Use contact information that you already hold on file, or that you have sourced independently. Don't rely on any contact details within the request as the fraudster may have altered these too
- Be aware that the letters may appear to be genuine with the correct letterheads, logos and signatures
- Check the email address. At first glance they may appear to be genuine
- Confirm to the supplier that the payment has been made
- Make all staff aware of this type of fraud

Don't forget – Failure to take adequate security precautions could ultimately leave your business liable for any losses which arise from fraud. The Bank will **NEVER** ask you for your full PIN and password online, **NEVER** ask for your PIN, password or card reader codes over the telephone and will **NEVER** ask you for card reader codes at log in.

Get in touch

If you suspect fraudulent activity on Bankline, call: 1800 946 517

For additional information please refer to our security centre at www.ulsterbank.ie/Banklinesecuritycentre