Fraud Case Study 2

A finance team employee received an email from one of their creditors notifying them of a new account number for payment.

Ruth works for a large multinational company and is responsible for paying creditors as invoices arise. She received an email from one of the company's creditors notifying her of new payment details. Ruth updated the account information on the online banking, but as no payment was due did not make any payment and went about her day.

The following month an invoice was submitted requesting payment. The invoice was legitimately from her supplier. A week passed and the supplier rang to request payment. Ruth knew that she had already made it and confirmed the new bank account details while on the phone, but was taken by surprise when they notified her they had not changed their bank account details at all!

Upon further investigation it was found that the email, advising of the new bank details for payment she had received, was fraudulent. When Ruth called the bank they confirmed that Ruth had made the payment the week before.

She knew that as she had authorised the payment and changed the details on the company's online banking system there was nothing she could do.

She informed her bank of the fraudulent incident to alert them of the case. While Ruth's bank endeavoured to recoup the transfer, the money had already been withdrawn from the other bank account. Not only did they lose this money, but the company still had an outstanding invoice to pay.

Question:

How could the fraud have been avoided?