News 21 Jun, 2021

Cyber Security: Bank Transfer Fraud

A reminder to be vigilant against bank transfer (or wire transfer) fraud.

There has been a significant increase in the sophistication and number of business email compromise attacks. These specialised phishing email attacks are more carefully targeted than ever and are regularly used to effect bank transfer fraud.

The fraudsters typically gain access to chains of emails through social engineering or malware attacks. From that information, together with profiles of the organisations involved, they can craft messages and attachments that appear to come from established business partners. A common tactic is to impersonate a senior executive and attempt to induce an employee or business partner into making a payment to a new bank account. Recovery of any such diverted payments is extremely problematic.

We recommend that you establish robust controls to verify the authenticity of a payment request or a change of bank account details:

- Where you are making a payment, telephone an existing contact at the beneficiary/payee organisation, using a previously known telephone number, to check whether the new banking details are legitimate. Alternatively, consider using secure encrypted email to a previously verified address.
- Where you are making a payment, check whether the change to the beneficiary's bank account makes sense. Does the beneficiary have links with the country in which the new bank account is based?
- Where you are due to receive a payment, advise those who are due to pay you to check that the new account details are legitimate.

As well as all the vital well-established infrastructure cyber security protections, remember that your employees are a key factor in ensuring the safety of your organisation and that of your business partners:

- Institute regular security awareness training for all employees and
- test its effectiveness with simulated phishing campaigns.