Banking & Payments Federation Ireland

Nassau House
Nassau Street
Dublin 2
Ireland

+353 (1) 671 5311
info@bpfi.ie

www.bpfi.ie

FRAUD ALERT- CEO/CFO Fraud - Spoofed Email Payment/Mandate Request

Publication by:
Banking & Payments Federation Ireland (BPFI)

For the attention of:
Irish Businesses

Purpose of Advisory:

To advise that a number of businesses in Ireland have recently been targeted by fraudsters using bogus emails which purport to be from a senior member of staff within the organisation requesting an urgent payment or electronic transfer be made outside of normal procedures or trading patterns.

Key Details:

A member of staff at the finance or accounts department receives an email purporting to be from a senior member of staff within the organisation, whether Director, CEO, Chairman, levels etc., requesting they arrange an urgent payment outside of their normal procedures due to exceptional circumstances.

The email appears to be genuine due to the address in the "From" box reflecting the genuine email address of the senior member of staff. With the recipient believing the email to be genuine, they arrange for the payment to be made through their preferred payment method for the credit of the fraudster's account, from where the monies are usually quickly withdrawn or transferred out.

There are two methods which the fraudster could use to facilitate this type of fraud attempt:

Email Spoofing

Using technical know-how, social engineering or malware, the fraudster is able to construct an email which appears to have come from another source, whilst disguising the true originator. Hovering the curser over the name in the "From" box will not reveal the true origination address in these cases and therefore the email appears genuine. The difference in the spoofed email account is very subtle and can easily be mistaken for the legitimate email address.

Banking & Payments Federation Ireland

Nassau House
Nassau Street
Dublin 2
Ireland

+353 (1) 671 5311
info@bpfi.ie

www.bpfi.ie

Hacked Email Accounts

The fraudster hacks into the victim's email account and starts issuing emails in the victim's name, including payment requests to banks or work colleagues. Customers that are more vulnerable to this type of attack are normally users of free email services such as Gmail, Hotmail and Yahoo, for example.

Red Flags:

- Any payment request which is outside of normal policy or process, especially if received by email
- Any urgent or confidential request not respecting the standard working procedure or trading patterns
- Any unusual payment request such as transfer of high amounts to an unknown or foreign account or to a country where the company has no market relations

---

Action:

- Businesses should have a specific documented internal process for the arrangement and authorisation of payments
- Any requests outside of that procedure, especially if received by email, should be regarded as suspicious
- For such requests, verbal contact should be made with the person sending the email, using a known contact number from the company's internal records, to confirm the request
- Businesses should strengthen their passwords for access to their email accounts, to include a mixture of uppercase letters, numbers and special characters, e.g. $&, etc.
- Businesses should avail of password manager applications and use passphrases instead of passwords