IRISH BANKING FEDERATION

Nassau House
Nassau Street
Dublin 2
Ireland

t: +353 1 671 5311
f: +353 1 679 6680
e: ibf@ibf.ie
w: www.ibf.ie

FRAUD ALERT - Social Engineering*

Publication by:
Irish Banking Federation

For the attention of:
Business Institutions and Associations – for onward transmission to members

Purpose of Memo:
To advise that a number of banking customers in Ireland have fallen prey to frauds that involve various forms of social engineering (where the information required is garnered from a person rather than breaking into a system).

Key Points:

1. **Phone Fraud Scam**
   - Some businesses and individuals have recently fallen victim to a sophisticated phone scam. The fraudster uses an invented scenario to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.
   - An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation to establish legitimacy in the mind of the target.
   - During the course of a phone call or series of calls, the perpetrators obtain enough information to take control of the victim's bank account including full details of the online banking passwords following which fraudulent high value payments are made.

2. **Email Account Hacked**
   - Personal email accounts of some customers (particularly company directors and individuals of high net worth) are being compromised, in many cases as a result of the individual responding to a Phishing email.
   - Having gained unlawful access to the company director's email account, the hacker will familiarise themselves with the email correspondence therein.
   - The hacker will then issue emails from this account, posing as the company director, providing an excuse as to why all contact with him must be by email ("I'm boarding a plane and will be out of reach")
   - The hacker may then either:
     1. Contact the bank purporting to be the company director, and instruct that a payment be made to a fraudulent beneficiary account, or
     2. Contact a colleague in the company's finance department (e.g. financial controller, or some such person) instructing the issuance of a high value payment to a fraudulent beneficiary. In this latter situation, the bank will have been given a legitimate payment instruction by the finance department.

Action:
Attempts to 'socially engineer' (i.e. manipulate) staff into divulging sensitive data, whether this is banking data or some kind of client data, must be recognised by the recipient for what it is – Criminal Activity.

In order to recognise such situations, ALL inbound calls/e-mails that seek any kind of sensitive information (re banking data, transaction data, customer records etc.) or make payment instructions should be treated as potentially suspect.

Where a staff member receives payment instructions via email, then enhanced checking procedures should be implemented at all times, e.g. call-backs must be made to ensure that customer emails have not been hacked. No customer information should be permitted to be disclosed via E-mail and payment instructions should only be processed in accordance with existing procedures.

Businesses should adopt robust identification processes and ensure that all calls/emails from strangers (who are seeking potentially sensitive information, of any kind) are handled with appropriate caution and that all instances of suspect calls are reported to management and to the Gardai / Police.

---

*Social Engineering in this context means techniques of manipulating people to obtain information (e.g. via e-mail or phone calls), or retrieving information from social networks, for the purpose of fraud.

This is a general notice issued by the Financial Crime and Security Department of the IBF on Behalf of IBF members.