GIAA Bulletin | Issue 4 – August 2016 | This 'red' Bulletin provides an Alert from Government's Internal Audit Provider

Government Internal Audit Agency

Executive Impersonation / 'CEO' Fraud

Executive impersonation fraud is on the rise, and is reported to have cost businesses $2bn globally over the last two years[1]. We have been alerted to recent attempts at executive impersonation or 'CEO' fraud. These frauds attempt to bypass traditional reliance on spam filters, and try to take advantage of informal internal control environments. The volume of personal and business information available online increases the risk of being exposed. Losses can be significant in value, difficult to recover and cause damage to reputation.

Jon Whitfield, Head of Government Internal Audit

This bulletin may be particularly helpful to:

- Accounting Officers;
- Finance Directors;
- Counter-fraud teams;
- Security officers; and,
- Finance teams.

What is Executive Impersonation fraud?

- A colleague receives an e-mail appearing to be from a known internal senior executive (e.g. Chief Executive, Finance Director).
- The e-mail instructs the colleague to process the payment request to an external party.
- It appears genuine as the details in the 'from' field may show the correct or similar address of the senior executive.
- Believing the request to be authentic, the colleague processes the payment and the funds are quickly withdrawn by the recipient.

Why is it increasing?

- A wealth of personal data is posted online by potential victims, allowing convincing impersonation.
- As the fraud targets individuals or small groups, it can be immune from spam filters.
- The crime is low-risk for the perpetrator and fast. In some cases money has been transferred in under an hour.
- Employees may be unlikely to question instructions purporting to come from senior management, particularly if this is 'the norm' or it appears to be exceptional and expressed as such.

What does it look like?

- The sender's e-mail may be a slight variation from the expected; e.g. ending in .org.uk rather than .gov.uk
- The e-mail may be followed by a phone call from a third party, adding to the perceived legitimacy of the transaction.
- The request will usually be urgent.
- The language or tone of the e-mail may differ from the colleague's normal communications.
- Its prevalence increases around peak leave periods when people may be out of the office.

How can it be detected?

- Raising awareness and training staff is one of the best ways to mitigate this risk.
- Treat all unexpected e-mails with caution.
- Always hover the mouse over the sender's name to reveal the address. This should show if a variation of the true address has been created.
- Always reply to the senior executive from a new e-mail chain. Never reply from the original e-mail.
- Phone or speak to the person requesting payment

Case Study – attempted executive impersonation fraud

A central Government body recently experienced an attempted executive impersonation fraud. The perpetrators attempted to impersonate a senior executive in order to generate an erroneous payment. Invoices were sent to a shared inbox requesting immediate payment. Fortunately, flags were raised by the finance team and no money was paid.

A lessons learnt exercise highlighted that applying the strict policy of only paying invoices with a purchase order, and having a finance team with deep knowledge of system processes and control - helped to detect the attempted fraud. It stressed that the need to increase awareness of this fraud is a high priority for the finance team, and regular updates from external sources should be shared. Actions were subsequently planned to raise awareness amongst staff of fraud risk via tailored training.

"According to security experts, although implementing security controls and enhanced authentication can help stop these attacks, educating employees against these socially-engineered schemes is one of the best ways to defend against this new form of fraud."[2]

How to protect your organisation

To perpetrate an executive impersonation fraud, fraudsters often use social engineering techniques to entice employees into revealing crucial confidential information such as staffing lists and job roles. Preventative steps can include:

- Ensure payment controls (e.g. two-stage authorisation, segregation of duties, PO requirement) are in place and tested for assurance purposes. Consider reviewing these if they can be easily over-ridden in the event of this type of attempt.
- Implement controls to assist verification of CEO or senior staff, such as establishing two points of contact for individuals so staff can check an instruction is legitimate.
- Be suspicious of unsolicited phone calls, visits, or e-mail messages asking about employees or internal information.
- Do not reveal personal or financial information in e-mails.
- Do not wear name badges outside work.

Responding to CEO fraud

It is important that your organisation has a policy/fraud response plan that can be followed in the event of an attempt. Key considerations include:

- Are staff aware of the existence/location of the policy and how to respond if this fraud were to occur?
- Is there a provision for ensuring security teams are informed of attempts?
- Acting quickly in order to mitigate loss and capturing details are both important – awareness of what to do can increase the likelihood of both of the above.
- Provision for an appropriate investigation and notification of authorities should be considered.

The risk is magnified due to the level of information available on senior executives and contracts via public sector transparency data and social media.

For additional advice or support, please get in touch with your Head of Internal Audit - or, send queries to information@giaa.gsi.gov.uk

Further guidance on fraud 'hot topics' is provided by Action Fraud: www.actionfraud.police.uk

[1] CEO e-mail scam costs companies $2bn, www.ft.com; Feb 24 2016

[2] Masquerading: Federal Authorities Issue Warnings Regarding New Form of Wire Fraud, securityworldexpo.com