

How to Spot a Social Engineering Fraud

CRIME

What is social engineering fraud?

This term is used to describe a wide variety of frauds where fraudsters dupe their victims into disclosing confidential information and making payments by using psychological manipulation known as “social engineering”. We describe common examples of social engineering frauds in the documents entitled “Fake President” Frauds and Payment Diversion Frauds.

How to spot a social engineering fraud

As an initial point, social engineering frauds are committed by a huge number of parties across the world. Accordingly, although many of these frauds have common aspects, they are all different.

Further they are constantly evolving and fraudsters are becoming increasingly sophisticated. Some approaches from fraudsters appear entirely legitimate and are quite convincing. Following on from this, the points below should not be taken as a checklist of what this type of fraud will entail but rather some warning signs that should form part of a wider control environment. In connection with this, we have also included below controls that can be introduced to help companies avoid being the victim of this type of crime.

Some common warning signs in the communications from fraudsters include the following:

- Spelling errors in email addresses and email addresses which whilst appearing legitimate, upon further investigation are found not to originate from the purported sender.
- Poor grammar and spelling in email correspondence and letters sent by fraudsters.
- Inconsistencies in who communications apparently originate from. For example an email that is purportedly from one individual but is received from an email account of another person.
- Incorrect job titles in email signatures.
- Communications specifying that replies should be made to specific individuals and specific email addresses only.
- Emails or letters accompanied by pressuring phone calls requesting that a particular change or payment be actioned straight away.
- Letters purportedly from suppliers / third parties including company logos but which do not appear to be on the company’s official headed paper – logos are often readily available on the internet.
- Letters containing contact details for a known supplier which differ to the ones usually used. This means that if a company tries to call or email to confirm payments / bank details they will contact the fraudsters rather than the genuine intended recipient of the funds.

- Payee bank accounts in locations or jurisdictions which have no apparent connection with the intended recipient of the funds. It is possible that a UK company might want you to pay its bank account in China but if this is a new arrangement it should warrant further checks.

It is worth remembering that fraudsters can hack email accounts meaning that they can include genuine historic email correspondence in their communications. Genuine previous correspondence must not be taken as evidence that recent communications are received from the same party. It is particularly easy to be duped by fraudsters in these instances.

What controls can be implemented to help avoid these frauds?

Before payments are made to unknown / unusual bank accounts, employees should be encouraged to telephone the payee using historic contact information (rather than any contact information included with the payment request).

Controls should also be in place surrounding the implementation of new supplier bank and contact information. Changes to this data should not be implemented by junior / inexperienced members of staff.

If the fraud involves an apparent instruction from senior management, employees should be encouraged to independently telephone the person involved.

Large payments to unknown bank accounts must be verified / authorised by two employees with both employees reviewing the supporting documentation. This control should never be circumvented and enables an independent "sense check".

Most importantly though, companies should ensure that all staff within their organisation with responsibility for suppliers' bank details or for making payments should be alerted to these types of fraud and watchful for key warning signs.

This material has been compiled with the assistance of ASL, to learn more visit [here](#)

American International Group, Inc. (NYSE: AIG) is a leading global insurance organization. AIG provides insurance solutions that help businesses and individuals in more than 200 countries and jurisdictions protect their assets and manage risks through AIG operations, licenses and authorizations as well as network partners. For additional information, visit www.aig.com. This website with additional information about AIG has been provided as a convenience, and the information contained on such website is not incorporated by reference herein.

AIG is the marketing name for the worldwide operations of American International Group, Inc. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions, and coverage is subject to underwriting requirements and actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

American International Group UK Limited is registered in England: company number 10737370. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. American International Group UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 781109). This information can be checked by visiting the FS Register (www.fca.org.uk/register).