Social Engineering Fraud Procedure

PHX110

Contents

Introduction 2
Your Responsibilities 2
What To Look Out For 2
- Request for confidential information 2
- Verification Procedures 2
- Fraudulent Hardware Orders 2
- Not using the same password for several logins and/or sharing passwords 3
- Verifying any changes to customer or vendor details 3
- Requests for Payment 3
- Rogue Devices 3
- Suspicious Unsolicited Emails 3
- Responding to offers made over the telephone or via email 3
- A party refuses to provide basic contact details 3
- Confidential disposal 4
- Unauthorised physical access 4
- Social Media Outlets 4
- Staff Awareness 4

What To Do If You Have A Suspicion Or Concern? 4
What To Do If You Are A Party To Facilitation Of Tax Evasion? 4
What To Do If You Feel Threatened Or Vulnerable? 5
Related Documents 5
Version Control 6
Document Approval 6

Introduction

Social engineering is the term used to describe a wide variety of frauds where fraudsters deceive their victims into disclosing confidential information or performing actions - such as making payments or allowing system and/or building access - by using psychological manipulation. The most common way of performing social engineering is over the telephone however it can also be carried out via email and in person.

Your Responsibilities

You must read, understand, and comply with all the information contained within our Social Engineering Fraud Policy, along with any awareness training you receive. All reports of incidents will be dealt with in a safe and confidential manner (see 'Whistleblowing Policy') and will be investigated rigorously. Any breach of this Policy by a staff member may ultimately lead to dismissal via the Company's disciplinary procedure.

What To Look Out For

Below are examples of risk areas and red flags that could arise during the course of your everyday working, and which should raise a concern under the Social Engineering Fraud Policy.

Examples could include, but are not restricted to the following:

Request for confidential information

You could be contacted by someone requesting confidential or sensitive information about the Company or a Phoenix employee. Such information should never be released to unknown and untrusted sources or to someone who does not have a valid reason for having it, even if that person identifies themselves as a Phoenix employee, a superior or a member of the Company's IT department. Should anyone have any doubts, politely refuse to engage in the conversation further, take the caller's details and report it to the ISC.

Verification Procedures

The Company verification procedures to ensure incoming monies received are verified and clearance is made prior to transferring money by wire, must be followed.

Fraudulent Hardware Orders

Extra vigilance is carried out on hardware orders.

Not using the same password for several logins and/or sharing passwords

Access to the Phoenix network is controlled by means of individual user logins and passwords. Passwords should not be the same for more than one login - be that on the Phoenix network or in the user's personal life - and should contain a combination of letters, numbers, and characters. Passwords should not be revealed to anyone, even a colleague, supervisor, or manager. See also 'Access Policy'.

Verifying any changes to customer or vendor details

Procedures to verify any changes to customer or vendor details, independent of the requestor of the change, are in place and must be followed.

Requests for Payment

Payments must only be made after the proper documents to support them i.e. an official Purchase Order have been raised. Appropriate segregation of duties is in place to ensure all documents are supported by the appropriate checks.

Rogue Devices

Company policies are in place to prevent any unapproved third-party software being installed on the Company network and/or unauthorised devices connected to the Company network. Should anyone have any doubts they should contact the IT department immediately.

Suspicious Unsolicited Emails

Only emails from trusted sources should ever be opened. Emails from suspicious sources should never been forwarded on, responded to or any attachments and/or links contained should ever be opened; they are to be deleted and the IT department informed immediately.

Responding to offers made over the telephone or via email

Offers that sound too good to be true generally are. Unsolicited emails offering to help solve a solution such as a computer issue or other technical matter should not be entertained. Such unsolicited emails should be deleted.

A party refuses to provide basic contact details

Situations where a party refuses to provide basic contact information, attempts to rush a conversation (act now, think later), uses intimidating language and requests confidential matter could be a sign of social engineering fraud. Recognise the psychological methods social engineer's use; power, authority, enticement, speed, and pressure.

Confidential disposal

Hard copy confidential documents and other tangible materials such as computer hardware and software are only to be disposed of using Approved Waste Disposal Carriers with Waste Transfer Notes retained as proof of confidential destruction and/or data removal. Hard copy disposal is managed by the Admin Dept, IT asset disposal is managed by Service Desk.

Unauthorised physical access

All visitors must report to Reception and state who they are due to visit. Visitors must wear their Visitor Pass at all times whilst on the premises. The building is secure and has external & internal CCTV cameras in operation 24/7 and Reception is manned during office hours. External doors have secure card swipe entry. The Company's server room is secured with authorised personnel having access and strict entry procedures in place.

Social Media Outlets

Social media posts on the Company's website are monitored by and restricted to authorised Marketing personnel only. Posted information is limited to new product/service announcements, webinars, and misc. marketing promotions. The likelihood of sensitive information being distributed via this platform is considered low however it remains a consideration.

Staff Awareness

Regular staff awareness is carried out to ensure employees are not deceived by fraudsters and that warning signs are recognised early in order that they can be stopped.

What To Do If You Have A Suspicion Or Concern?

Should you have a reasonable belief, suspicion or concern that someone has been engaged in social engineering fraud however insignificant it may be and whether it involves an employee or a third party, this must be reported to the Directors.

What To Do If You Are A Party To Facilitation Of Tax Evasion?

Should you ever be asked to do something, either by an employee of Phoenix or a third- party, where you suspect there may be social engineering fraud, or believe that you are a victim of another form of unlawful activity, this must be reported to the Directors.

What To Do If You Feel Threatened Or Vulnerable?

Should you refuse to act on a request, either by an employee of Phoenix or a third-party, which you think may result in social engineering fraud and you feel worried about the potential consequences, Phoenix will support you even if investigation finds that you were mistaken. Please also see our 'Whistleblowing Policy'.

Related Documents

Please also read:

- Expense Claim Policy
- Fraud, Bribery & Money Laundering Policy
- Whistleblowing Policy

Version Control

Author	Version	Date	Description
Trevor Hutchinson	1.0	22/04/2021	Original Document
Trevor Hutchinson	1.0	01/11/2021	Annual review – no changes
Trevor Hutchinson	1.0	01/11/2022	Annual review – no changes

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	22/04/2021	Managing Director
Sam Mudd	1.0	01/11/2021	Managing Director
Clare Metcalfe	1.0	01/11/2022	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 01/11/2022