Social Engineering Fraud Policy

PHX109

Contents

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.

Purpose & Scope

Phoenix ("the Company") is committed to the highest ethical standards and operates a framework for the prevention and detection of Social Engineering Fraud and will uphold all relevant UK legislation. It requires its employees and any person working on behalf of the Company to act at all times with honesty, integrity, propriety, and due care in all matters, but particularly in the safeguarding of the Company, its associated assets, its reputation, and that of its parent group.

Employee behaviour can have a huge impact on information security in organisations and therefore the Company requires anyone working with the business as an employee or contractor to be constantly aware of such fraud. Any suspicion of social engineering fraud must be reported to the Company Directors immediately. All reports 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.

Counter Measures

The countermeasures implemented by the Company to prevent, detect, and respond to Social Engineering Fraud include but are not limited to:

- Data Classification Assessment
- Verification Procedures
- Additional Verification Checks on Hardware Orders
- Procedures on all requests for Payment
- No unapproved third-party software / Rogue Devices to be used
- Company Policies in place re Suspicious Unsolicited Emails
- Social Media Outlets constantly monitored
- Only Approved Waste Disposal Carriers used for all waste (hard copies & software)
- Secure physical access to the building & CCTV in operation
- Network password policy in place
- Regular Staff Awareness & Refresher Training

<u>Reporting concerns or suspicions</u>

Should anyone 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.

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

Should an employee refuse to act on a request, either by an employee of Phoenix or a third-party, which they think may result in social engineering fraud and feel worried about the potential consequences, the Company will support them even if investigation finds that they were mistaken.

Ongoing Monitoring

The Company will maintain an effective system for monitoring compliance procedures to ensure it remains committed to its zero tolerance to social engineering fraud. This includes employee awareness and forms part of the induction process for all new employees.

Board Responsibility

The person with over-riding Board responsibility for the Company is Paul Emms, Group Finance Director.

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*   Clare Metcalfe, Operations Director

Dated: 01/11/2022