Monedo

MONEDO FINANCIAL SERVICES PVT. LTD.

PHISHING POLICY

Contents

1. Overview

The information and information systems used by Monedo Financial Services Pvt. Ltd. Monedo Financial Services Pvt. Ltd, will be referred as “Monedo”. This Phishing (“Policy”) establishes the processes and defines the requirements at Monedo.

2. Objectives

The purpose of this policy is to educate employees, partners, vendors, etc. about Phishing attacks and the types of phishing attacks that anyone can fall for which in turn can lead to impending disaster. Phishing is the cause of most cyber breaches. Most successful attacks against companies start with a phishing email. Adhering to the statements in this policy will help Monedo to be more resilient to phishing attacks.

3. Scope

This policy applies to all of Monedo employees and contractors accessing Monedo’s systems, network and information, whether from Monedo’s devices or personal device.

4. Ownership

The Ownership of this policy solely lies with IT Leadership team.

5. Responsibility for Implementation

The responsibility for overall implementation and upkeep of this policy rests with the IT leadership which consists of the Chief Technology Office (in this and other policies of the Monedo referred as “Chief Technology Officer” or “CTO”).

6. Reviews & Deviations

This Documents shall be reviewed by the IT Steering Committee annually against changing business and IT environment to ascertain its appropriateness. The modification of the SOP shall be approved by IT Steering Committee.

7. Communication

This SOP is communicated by CTO to the IT function and to third party as deemed necessary.

8. Operational Documentation

- ### Phishing Definition

  Phishing is a email-borne attack whose goal is to steal confidential information, such as login credentials or credit card numbers, usually to carry out various types of financial fraud. An attacker impersonates a trusted entity, such as a bank, government, ISP or large website, and tries to trick users into giving up their private information. These attached often take the form of "Urgent" emails asking users to take immediate action in order to prevent some impending disaster.

9. Policy

1. If an email is from an unknown sender, do not provide any personal information or take action by opening an attachment, clicking on a link, or entering information in a pop-up box.
2. If the email is from a known sender, check the identity of the sender before clicking on any attachment in the email. You can check the email of a sender by hovering over the name of

the sender when you cannot see the email address to be sure the email address looks correct.

3. If any email contains a link or asks you to enter information, carefully check the identity of the sender before taking action.
4. If you open and email that looks suspicious, look at the full email address of the sender and check the email carefully for errors like grammar or spelling mistakes.
5. If any email doesn't look legitimate, don't open any attachments or follow any directions in the email.
6. Bring any suspicious emails to the attention of your IT staff. Take a screen shot of the email and send it to the IT staff in a new email.
7. When receiving a document from an external source, only open it in the read/only protected view.

Examples of Phishing

- "Your account information needs to be validated in order for you to access your account. Please click here to update your information."
- "Your Debit card is about to expire. Please click here to update the information for your New card."

Users who click on the links in these emails may be taken to a phishing site - a webpage that looks like legitimate site they have visited before but is actually controlled by an attacker. Because the page looks familiar, users visiting these sites enter their username, password or other private information on the site. What they are not aware is that unknowingly they have given a third party all the information needed to hijack their account, steal their money, or open up new lines of credit in their name.

Protection against Phishing

- Be careful about responding to emails that ask you for sensitive information. You should be aware while clicking links in emails or responding to any emails that ask for account numbers, usernames and passwords, or other information. Monedo will never ask you for any such information via emails.
- Go to the site instead of clicking on suspicious emails. If you receive such emails asking for sensitive information rather open the link in a new browser and go to the Organisation's website. If you are not sure about such request from Monedo, please visit https://www.monedo.in/contact-us/ and let us know your concerns.
- Use a browser that has a Phishing filter. The latest versions of most browsers include phishing filters that can help you spot potential phishing attacks.