

<b>Business Unit:</b>	<b>Organisation Support &amp; Development</b>
<b>Document Title:</b>	<b>Phishing Awareness and Training Policy</b>
<b>Document No.</b>	<b>ICT029/PA&amp;T/V3/24</b>
<b>Source:</b>	<b>ETBI 22</b>
<b>Approved By:</b>	<b>Chief Executive LWETB</b>
<b>Noted by:</b>	<b>LWETB Board</b>
<b>Date Noted:</b>	<b>November 2024</b>

# **LONGFORD AND WESTMEATH EDUCATION AND TRAINING BOARD**

## **Phishing Awareness and Training Policy**

## Contents

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
1.1	Purpose of this Document .....	3
1.2	Scope and Constraints.....	3
1.3	Definitions .....	3
<b>2</b>	<b>Policy Overview .....</b>	<b>3</b>
2.0	Phishing overview .....	3
2.1	Phishing campaigns .....	4
2.2	User responsibility & reporting a suspected phishing email.....	4
<b>3</b>	<b>Enforcement.....</b>	<b>5</b>
<b>4.</b>	<b>Policy Review and Continuous Improvement.....</b>	<b>5</b>
<b>5.</b>	<b>Ownership and Approval .....</b>	<b>5</b>

## 1 Introduction

### 1.1 Purpose of this Document

This policy should be read in conjunction with all other ICT policies. The purpose of this policy is to ensure that there is a high level of phishing awareness among all users to protect the confidentiality, integrity, and availability of Longford Westmeath Education and Training Board (LWETB.) information, records, and data.

### 1.2 Scope and Constraints

The scope of this policy applies to all Users throughout LWETB.

### 1.3 Definitions

A full range of definitions is available in the ICT Security Frameworks Policy found [here](#).

## 2. Policy Overview / ICT responsibilities

LWETB understands that awareness is a key pillar of security within the organisation. LWETB continues to develop security consciousness within all areas of the organisation through awareness programs and focus on the best practice implementation of business and security processes.

- All LWETB. Users are to receive appropriate training in security matters at least annually. This may be in the form of classroom, online training, or via policy management/user awareness software agents on end-user systems.
- Priority will be given to those Users who have access to large amounts of personal data.
- A record will be maintained of those who have completed the training and shall be stored by the relevant Corporate Services staff .
- Where security awareness training includes phishing campaigns, the results of this exercise will be maintained as a baseline measurement of the level of security awareness that exists within the organisation. Subsequent phishing campaigns will then be conducted following security awareness training to measure the level of improvement in security awareness among staff.
- The Information Security Awareness training program will incorporate a section relating to phishing emails.
- Phishing Awareness training will explain what phishing emails are, how they work, how to identify them and what remedial action to take.
- The training program should ensure that all staff members achieve and maintain at least a basic level of understanding of phishing and other information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms.
- Information Security awareness and training will form part of the induction/orientation pack which will be part of the onboarding process and should commence at the earliest possible opportunity.
- The technical content and complexity of the training materials will reflect the audience and the type of work they perform.
- The location of the Information security training materials should be known to all staff and be readily available to them at all times

## 2.1 Phishing campaigns

- Phishing awareness campaigns will be carried out on a continuous/rolling basis to maintain a consistent level of awareness. Campaigns include but are not limited to Phishing (email), vishing (voice), and smishing (SMS).
- Campaigns will be conducted randomly throughout the year with no defined schedule, aiming towards a minimum of two campaigns per year.
- Campaigns may be targeted against specific departments or individuals based on a department's risk.
- Phishing campaign results will be used to measure the level of security awareness among staff.
- Campaign results data should be classified as sensitive and only be shared with appropriate and necessary users.

## 2.2 User Responsibilities

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The following rules must be observed when dealing with suspected phishing emails:

- Never send passwords, bank account numbers, or other private information in an email.
- Avoid clicking links in emails, especially any that are requesting private information.
- Be wary of any unexpected email attachments or links, even from people you know.
- Look for 'https://' and a lock icon in the address bar before entering any private information.
- Check for suspicious/unusual indicators within an email, such as poor grammar/spelling and time received (after midnight).
- Check the source and reply address of the email (hover mouse over display email address). The display name you see can be easily designed to look like it's coming from a genuine person, but the reply address can be completely unrelated and malicious.
- Watch out for banner messages and hints provided by the system that indicate that the email is external for example or that you don't often get emails from the sender in question as these may reinforce the suspicion that the email is malicious.
- Use other methods of communication to check with the sender if you still have any suspicions.
- Remote access is a high-risk activity and should only be permitted to verified LWETB ICT support through use of the ICT Support Helpdesk.

In the event of a suspected phishing attack, the following actions should be taken:

- Disconnect affected device from the network
- Power off the affected device
- Report any observed or suspected phishing emails or any security incidents as soon as possible as to the ICT Support Services copying [corporate@lwetb.ie](mailto:corporate@lwetb.ie).
- Change your LWETB. active directory (windows) login credentials.
- If credentials are shared for any personal accounts, these must also be changed.
- Provide access to your device if deemed necessary by the Corporate Services Department/ICT Support Services.


### 3. Enforcement

Individuals found to be in breach of this policy may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

### 4. Policy Review and Continuous Improvement

This document will be reviewed every two (2) years in line with best practice, and has been approved by senior management, who are committed to continually improving the protection of all LWETB. information assets and the protection of personal data where LWETB. is a controller or processor. This document will be reviewed by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within LWETB. The date of implementation is the date of Chief Executive approval.

### 5. Ownership and Approval

OWNER	DATE	SIGNATURE
<i>Organisation Support &amp; Development Director</i>	Nov 4, 2024	 <a href="#">Charlie Mitchell (Nov 4, 2024 16:58 GMT)</a>
AUTHORISED/APPROVED BY	DATE	SIGNATURE
<i>Chief Executive</i>	Nov 5, 2024	