Module 2 - Don't Take the Bait: Spotting Phishing & Social Engineering

A Quick Guide for Staff – Provided by Alpha IT Solutions

Introduction: The Digital Battleground

In today's digital world, our inboxes and social media feeds are often targeted by cybercriminals. These individuals are experts in **Phishing** and **Social Engineering**—psychological tactics designed to trick you into clicking malicious links, opening dangerous attachments, or surrendering personal information.

Know the Difference

- **Phishing:** Deceptive messages (email, text, or social media) that appear legitimate—such as from your bank or a colleague—but are designed to steal credentials or infect your device.
- **Social Engineering:** A broader term for manipulating people into performing actions or divulging confidential data. It preys on our trust, curiosity, fear, or desire for a good deal.

The Red Flags: What to Watch For

- **Unexpected Urgency:** Beware of phrases like *"Your account has been suspended!"* or *"Immediate action required!"* Attackers use fear to make you act without thinking.
- **Suspicious Sender Details:** Always check the **full email address**. A name might say "Amazon," but the address could be support@not-amazon.com. Look for subtle typos like micros0ft.com.
- **Generic Greetings:** Professional organisations usually use your name. Be wary of "Dear Customer" or "Valued Member."
- **Mismatched Links:** On a computer, **hover your mouse** over any link before clicking. A small pop-up will show the true destination. If the link text says paypal.com but the pop-up shows malicious-site.xyz, it is a scam.
- **Requests for Sensitive Data:** No legitimate organisation will ever ask for your password, full credit card number, or security codes via email.
- **Unexpected Attachments:** If you weren't expecting a file (especially ZIP, PDF, or Word docs), do not open it. These are common vehicles for malware.

The "Stop, Think, Protect" Protocol

If you encounter a suspicious message, follow these steps:

1. **Do NOT** click any links or open any attachments.
2. **Do NOT** reply to the sender.
3. **Report It:** Forward the suspicious email to your IT department or to **support@alphait.ie**.
4. **Verify Independently:** If you are unsure, contact the organisation directly using a **known, official phone number** from their website—never use the contact details provided in the suspicious message.

"A moment of caution can save you a world of trouble. Stay alert, stay safe!"

For technical assistance, please contact the Alpha IT Solutions support team.

Call: +353 (0)23 881 0061 | **Email:** support@alphait.ie

Scan Me