Phishing Awareness Tutorial

# Beginner Guide:

## What is Phishing?

Phishing is a type of cyber-attack where attackers pretend to be someone you trust — like a bank, company, or even a friend — to trick you into giving away your personal information (like passwords, credit cards, or money).

**Phishing = Fake Identity + Trickery = Your Data Stolen!**

A concise overview of phishing attacks and their implications.

**Here’s a Link:**

[**https://www.youtube.com/watch?v=XBkzBrXlle0**](https://www.youtube.com/watch?v=XBkzBrXlle0)

# Why Is Phishing Dangerous?



* **You could lose your bank money.**
* **Your social media accounts can get hacked.**
* **Your private information can be used illegally.**

**Explores the risks associated with phishing and how to mitigate them:**

**HERE’s a Link:**

<https://www.proofpoint.com/us/threat-reference/phishing>

# How to Identify a Phishing Email?

* Always check the sender’s email address.
* Look for spelling or grammar mistakes.
* Be careful of urgent language like "Act Now!" or "Immediate Action Required!"
* Don’t click suspicious links — hover over them to check where they go.
* If it sounds too good to be true, it probably is!

**Tips on recognizing phishing emails and avoiding scams**

Here’s a Link:

<https://www.youtube.com/watch?v=iHetr8xTWIU>

# Examples: Phishing vs Real Emails

**You can show two examples side by side:**

| **Real Email** | **Phishing Email** |
| --- | --- |
| * Correct email address | * Weird email address (example123@abcscam.com) |
| * Professional language | * Spelling mistakes, weird language |
| * No urgency | * "Your account will be locked in 24 hours!" |

**Here’s a Link: Provides visual examples of phishing emails and tactics used:**

<https://www.terranovasecurity.com/blog/top-examples-of-phishing-emails>

# Mini Quiz: Practice Spotting Phishing

You receive an email from "support@paypaI.com" asking for your password. (Notice: the "I" in "PayPal" is actually a capital "i", not "L".)

**Is it phishing or not?**

* **Real**
* **Phishing**

**Here’s an interactive quiz to test your ability to identify phishing attempts.**

<https://phishingquiz.withgoogle.com/>

**Why it was phishing?**

# This is phishing. Here's why:

1. **Suspicious Sender Address**:
   * **The email comes from "support@paypaI.com" (with a capital "I" instead of an "l").**
   * **The legitimate PayPal domain is "paypal.com", not "paypaI.com". Scammers often use lookalike characters (e.g., "I" vs. "l") to trick users.**
2. **Password Request**:
   * **Legitimate companies like PayPal will NEVER ask for your password via email. This is a classic phishing tactic to steal credentials.**
3. **Urgency or Fear Tactics:**
   * **Phishing emails often pressure you to act quickly (e.g., "Your account will be locked!"). Check for alarming language.**

# What To Do If You Clicked on a Phishing Email

* **Immediately change your passwords**.
* **Use two-factor authentication** (like phone verification).
* **Scan your device** with antivirus software.
* **Report the phishing email** to your email provider.

**Here’s guidance on immediate steps to take after clicking a phishing link:**

<https://www.youtube.com/watch?v=B06nvFCyBFs>