**Sample Phishing Email**

**Subject:** Immediate Action Required: Your Account Will Be Suspended

From: security-alerts@accounts-support.com

To: user@example.com

Dear Customer,

We noticed unusual sign-in activity on your account and to protect your data, you must verify your account immediately by clicking the link below:

[Secure Your Account]

Failure to verify within 24 hours will result in permanent account suspension.

Thank you for your prompt attention,

Security Support Team

## Phishing Warning Signs

1. **Suspicious Sender Address**

* The email originates from a questionable domain like accounts-support.com instead of a trusted official domain (e.g. @yourbank.com or @platformname.com)

2. **Generic Greeting**

* Uses “Dear Customer” instead of your name, indicating it may be a mass-mailed phishing attempt.

**3. Urgent, Threatening Language**

* Creates pressure by stating the account will be suspended within 24 hours unless action is taken immediately—common phishing tactic to trigger panic and override rational thought.

4. **Links That Aren’t Transparent**

* The link text says “Secure Your Account,” but hovering over it often reveals a suspicious or unrelated URL, not matching the claimed domain or organization.

5. **Unexpected Request**

* You didn’t request any verification or initiate suspicious activity—legitimate services rarely ask you to verify account access out of the blue.

6. **No Contact Details Provided**

* Legitimate emails usually include real contact info, sometimes reply-to addresses. Here, there's no way to verify the sender or respond securely.

7. **Attachments or Links with Potential Malware**

* Criminals might include attachments disguised as invoices, forms, or document files that install malware on your device when opened.

## How to Protect Yourself

* **Verify sender email** by checking domain spelling and comparing with previous legitimate communications.
* **Hover over links** (without clicking) to inspect their destination URLs.
* **Don’t click links or download attachments** unless you’re expecting them, and instead access services directly via known URLs.
* **Watch for urgency**; legitimate providers rarely threaten immediate suspension.
* **Use two-factor authentication (2FA)** to protect your accounts even if passwords get compromised.
* **Report phishing attempts** to your security team or email provider immediately.