

### 1. What is phishing?

Phishing is a cyberattack where attackers impersonate trusted organizations (like Microsoft) through fake emails or messages to trick users into revealing sensitive data such as usernames, passwords, or financial information.  
👉 In your email, the attacker pretends to be Microsoft to steal login credentials.

### 2. How to identify a phishing email?

From the attached email, signs include:

Suspicious sender: support@msupdate.net (not a Microsoft domain).

Generic greeting: Doesn’t use the recipient’s real name.

Urgency: Claims "Your password changed" to scare you.

Fake links: “Reset your password” likely redirects to a phishing site.

### 3. What is email spoofing?

Email spoofing is when attackers forge the “From” address so the email looks like it’s from a trusted source.  
👉 In your case, it looks like Microsoft support, but actually comes from @msupdate.net.

### 4. Why are phishing emails dangerous?

They can steal your login credentials if you click the fake links.

Attackers could then access your Microsoft account, emails, files, or even use your account for further attacks.

It may also install malware if links or attachments are clicked.

### 5. How can you verify the sender’s authenticity?

Check the **email address/domain** (@msupdate.net ≠ Microsoft).

Hover over links (without clicking) to see if the URL matches Microsoft’s real website.

Log in directly via account.microsoft.com, not through email links.

### 6. What tools can analyze email headers?

**MxToolbox**

**Google Admin Toolbox Messageheader**

**Microsoft Message Header Analyzer**  
These reveal the actual sending server, SPF/DKIM/DMARC checks, and if the domain is spoofed.

### 7. What actions should be taken on suspected phishing emails?

**Do not click** any links.

Report it (forward to phish@office365.microsoft.com).

Mark it as spam in your email client.

Delete it after reporting.

If clicked, immediately **change your password** and run a malware scan.

### 8. How do attackers use social engineering in phishing?

**Fear/urgency**: Claiming “Your password changed” pressures you into quick action.

**Impersonation**: Pretending to be Microsoft for credibility.

**Technical details**: Adding IP, browser, and location info to make it look legitimate.