

Email Headers for CTF Challenge 3

Raw Email Headers

Delivered-To: victim@school-ctf.com
Received: by 10.100.10.10 with SMTP id abcd1234
for victim@school-ctf.com; Thu, 5 Feb 2026 10:30:45 +0000 (UTC)
Received: from mail-serverexample.com (mail-serverexample.com. [203.0.113.89])
by mx.school-ctf.com with SMTP id xyz789
for victim@school-ctf.com; Thu, 5 Feb 2026 10:30:40 +0000 (UTC)
Received: from attacker-pc.local ([192.168.1.100])
by mail-serverexample.com; Thu, 5 Feb 2026 10:30:35 +0000
From: "IT Support" support@fake-domain.com
To: victim@school-ctf.com
Subject: Urgent: Password Reset Required
Date: Thu, 5 Feb 2026 10:30:00 +0000
Message-ID: 12345@fake-domain.com
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 7bit
X-Mailer: PhishMailer 2.0
X-Originating-IP: [203.0.113.89]
Return-Path: support@fake-domain.com

Email Body

Dear User,

We have detected suspicious activity on your account. For security purposes, you must reset your password immediately by clicking the link below:

<http://fake-domain.com/reset-password?token=abc123xyz>

If you do not reset your password within 24 hours, your account will be permanently suspended.

Thank you for your cooperation.

IT Support Team
School CTF Security