Analyzer a Email Phishing Report

---

1. Email Metadata Section

Include basic details about the email:

Field	Example
Sender Name	Coursera sales **Department**
Sender Email	Coursera@m.learn.coursera.org>
Recipient	Coursera@m.learn.coursera.org>
Date Received	2025-05-27
Subject Line	Revamped Meta courses are here

---

2. Phishing Indicators Section

Analyze and list any red flags under the following categories:

A. Sender Information

- ⛔ Domain spoofing (32.51.54998.11749286@i-061d73a1544757ab2.mta1vrest.sd.prd.sparkpost)

⛔ Public domain used (v=DKIM1; k=rsa; h=sha256; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDy51SK8L1L99MHiKejCaQ1NiB9+omaX9Q4az1El
n4g4bGfkfXfxX9ra2tNXG1iW4aPjU5/bIgvGKiJul59tB6+liNiz1NhpRWcyQpwtXtvofIHDdYUQubknNaCKkv8/RqdZWI1BfezG4DPmCSYLR6cgaErEDU9pdDt298jMds+hwIDAQAB)

- ⛔ Display name and email mismatch Coursera@m.learn.coursera.org

B. Email Content

- ⛔ Generic greeting (e.g., “Dear User”)
- ⛔ Spelling/grammar errors
- ⛔ Urgent or threatening tone (“Immediate Action Required”)

C. Links and Attachments

- ⛔ Mismatched URLs (Coursera@m.learn.coursera.org)

⛔ Suspicious attachment type (`v=spf1 exists:%{i}._spf.sparkpostmail.com ~all`

D. Requests

- ⛔ Asks for sensitive info (password, SSN)

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:d@rua.agari.com,mailto:yfy3q-9359@rua.dmarc.emailanalyst.com	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto:d@ruf.agari.com	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.

	Test	Result
✅	DMARC Record Published	DMARC Record found
✅	DMARC Syntax Check	The record is valid
✅	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✅	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✅	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.

Your DNS hosting provider is "NS1". Need Bulk Dns Provider Data?

---

3. Screenshots or Raw Email Header (Optional)

Include:

- Screenshot of the full email (with header)

SPF and DKIM Information

dmarc:m.learn.coursera.org Show Solve Email Delivery Problems

DMARC Record for m.learn.coursera.org

No DMARC Record found for sub-domain.

Organization Domain of this sub-domain is: coursera.org Inbox Receivers will apply coursera.org DMARC record to mail sent from m.learn.coursera.org

SP Tag '' found: Inbox Receivers will treat all mail sent from m.learn.coursera.org that fails DMARC as suspicious.

DMARC Record for coursera.org (organizational domain)

v=DMARC1; p=reject; rua=mailto:dmarc-reports@coursera.org; ruf=mailto:dmarc-reports@coursera.org; fo=0; pct=100

- Full email headers (for advanced analysis)

Headers Found

Header Name	Header Value

Delivered-To	asurajkumar8535@gmail.com
X-Google-Smtp-Source	AGHT+IHQZi4thJdYfQKm0H9BmNNTP1gYiPqUEVk99x3KBrbduGfaDREZe5V3lrbwRukLf6DKfeqM
X-Received	by 2002:a05:6902:2b07:b0:e76:5fb9:9f48 with SMTP id 3f1490d57ef6-e7b6a318343mr11005088276.3
ARC-Seal	i=1; a=rsa-sha256; t=1747535634; cv=none; d=google.com; s=arc-20240605; b=MWW6CyIMOSABQoV BM8YAttr/askRt/j6O4ARl1sqM0crfRrtzKBkX/4pQ6BOmY3H/ 5pMwFvSFddNx3ssbG2CTa7v2aw5YMJ4lf Yc/eGqIcG0+nns8k3DAhkDugsXmYfJX2 V36GaWnskAYkdNYxItyMX1067KLUhSjmqvgUqMQ+W3qOJBZS
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=list-unsubscribe:subject:list-u ga3LWAbMdWyjdQ/vq4LIKhzkxPbeR5xhddH0=; fh=KbR/Cr0BEP4BU1uKW5IDVL+YeyxpnCcUAERxt4Dnf EvTm TwBcihvdpdDHvp7uUmm8RH3FPlUl7fPMJvL2MTOfCQxq8CpOFkCuBIPL7cOm9CC1nX/u FD7tG8B AuG21XLBJlXRe5igcbLQGOXXJdAhrxauAwWQyuPEdU6amxfrjDCp4INJS o0RnIwcCvjmSVryYHzLP0p5AE4
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@m.learn.coursera.org header.s=scph0823 header.b=pB4Zo9 @m.learn.coursera.org designates 137.22.225.86 as permitted sender) smtp.mailfrom="msprvs1=2023 REJECT dis=NONE) header.from=coursera.org
Return-Path	<msprvs1=20233g7Q1iHvl=bounces-266693-993@m.learn.coursera.org>
Received-SPF	pass (google.com: domain of msprvs1=20233g7q1ihvl=bounces-266693-993@m.learn.coursera.org de
Authentication-Results	mx.google.com; dkim=pass header.i=@m.learn.coursera.org header.s=scph0823 header.b=pB4Zo9np; earn.coursera.org designates 137.22.225.86 as permitted sender) smtp.mailfrom="msprvs1=20233g7C T dis=NONE) header.from=coursera.org
X-MSFBL	/4KfckhUoDk4Bmpfi7iAqYhbQRgV6N/bzOC+yYdSQY4=|eyJjdXN0b21lcl9pZCI 6IjI2NjY5MyIsIm1lc3NhZ2 0ZW5hbnRfaWQiOiJzcGMiLCJyIjoiYXN1cmF qa3VtYXI4NTM1QGdtYWlsLmNvbSJ9
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=m.learn.coursera.org; s=scph0823; t=1747535633; i=@m.lear ssage-ID:Date:Content-Type:From:List-Unsubscribe-Post: Subject:List-Unsubscribe:From:To:Cc:Subject IIjekYgxQAIQbIZaijQ6lO3LwUKxWnTBE6bgrKDXI9SDijjLGIwwseSM5DuK1Ep9I q2t7YkmcTT0Mb3bM29lc
To	asurajkumar8535@gmail.com
Message-ID	<32.51.54998.11749286@i-061d73a1544757ab2.mta1vrest.sd.prd.sparkpost>

Date	Sun, 18 May 2025 02:33:53 +0000
Content-Type	multipart/alternative; boundary="_----0PXxECfiuRpF52+wiyL6/w===_B1/51-54998-11749286"
MIME-Version	1.0
From	Coursera <Coursera@m.learn.coursera.org>
List-Unsubscribe-Post	List-Unsubscribe=One-Click
Subject	Revamped Meta courses are here!
List-Unsubscribe	<https://05.emailinboundprocessing.com/enc_user/list_unsubscribe?d=%241%24KGsJ5%2BSPuNzyrJB O%2BSbcmeV5t3%0Ak1AEquLhWXNSZKzyG%2B0jlDXIe9y18IB2%2B7CmMMTtocBvtR3xbVLvOodkpGU 1f%0Ajje4kRjj78ZMCRm5ZjOxWm11qhEPhQus5FjWUE6gn1FbS1ml9v9gdRMQ5z%2Fq%0AkYZC4d1%2F l9TSPpRf99LlEP6Fkbl1uuNz0vVZndp1xfe%2BygZI6suh%2BA%2B5%0Acvtkvy00AN6%2FmkrCOKg1uqZK8 ubscribe-05.emailinboundprocessing.com?subject=Unsubscribe%20pnrcgsq4fpu3za16yh9ua3gt4ele6fa hkyvqmg3pbdqkw8kz7mbs5uy9opxnudsvb8ib2ctuo2rxk61a58mddesodyh6gb6ul-DO_NOT_DELETE>

-

---

4. Verdict & Actions Taken

Field	Example
Verdict	Likely Phishing
Action Taken	Reported to IT and marked as phishing
User Clicked Link?	No
Malware Detected?	No

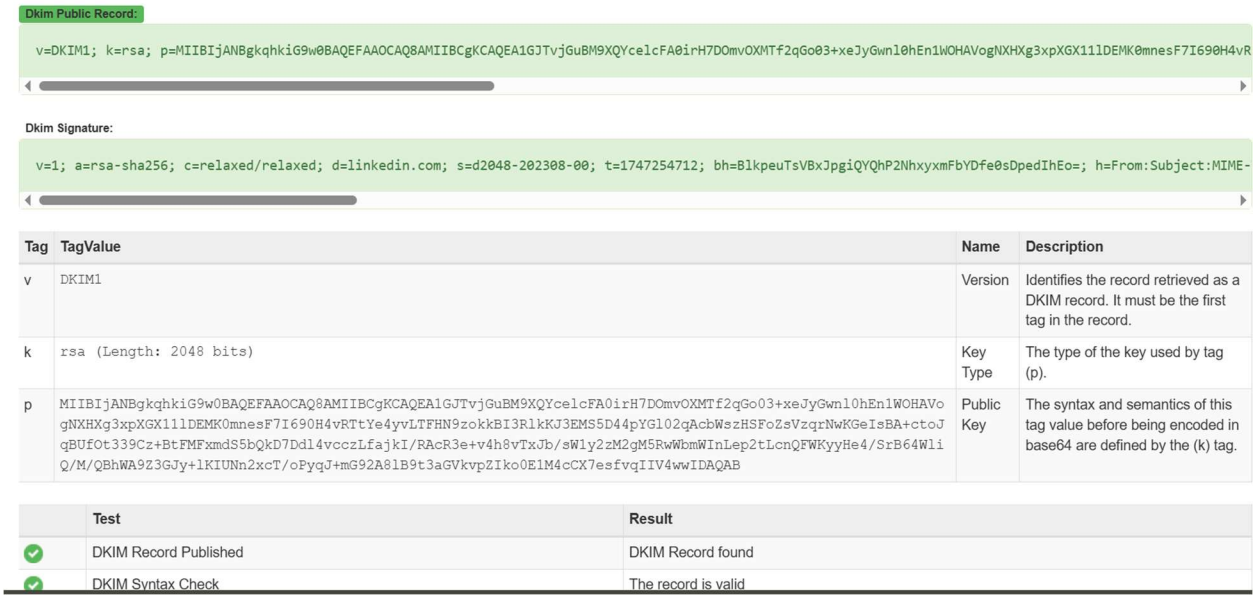
Sample Template (Editable for Training or Real Reports)

Suspicious Email Report

Date: 2025-05-27
Reported by: John Doe (Coursera@m.learn.coursera.org)

Email Summary:

"You must update your to avoid service suspension. Click here toCoursera@m.learn.coursera.org resolve."



Dkim Public Record:

```
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1GJTvjGuBM9XQYcelcFA0irH7DOmvOXMTf2qGo03+xeJyGwnl0hEn1WOHAVogNXHXg3xpXGX11lDEMK0mnesF7I690H4vR
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; d=linkedin.com; s=d2048-202308-00; t=1747254712; bh=BlkpeuTsVBxJpgiQYQhP2NhxyxmFbYDfe0sDpedIhEo=; h=From:Subject:MIME-
```

Tag	TagValue	Name	Description
v	DKIM1	Version	Identifies the record retrieved as a DKIM record. It must be the first tag in the record.
k	rsa (Length: 2048 bits)	Key Type	The type of the key used by tag (p).
p	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1GJTvjGuBM9XQYcelcFA0irH7DOmvOXMTf2qGo03+xeJyGwnl0hEn1WOHAVogNXHXg3xpXGX11lDEMK0mnesF7I690H4vRTtYe4yvLTFHN9zokkBI3RlkKJ3EMS5D44pYGl02qAcbWszHSFoZsVzqrNwKGeIsBA+ctoJqBUfOt339Cz+BtFMFxmdS5bQkD7Ddl4vcczLfajkI/RAcR3e+v4h8vTxJb/sW1y2zM2gM5RwWbmWInLep2tLcnQFWKyyHe4/SrB64WliQ/M/QBhWA9Z3GJy+lKIUNn2xcT/oPyqJ+mG92A8lB9t3aGVkvpZIko0ElM4cCX7esfvqIIV4wwIDAQAB	Public Key	The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.

	Test	Result
✓	DKIM Record Published	DKIM Record found
✓	DKIM Syntax Check	The record is valid

Sender Coursera@m.learn.coursera.org

Subject Line: "Action Required: Account Suspension Notice"

Red Flags Identified:

Domain resembles Coursera@m.learn.coursera.org is actually "paypa1-secure.com"

Action Taken:

- Marked as phishing in Outlook

-
- Reported to IT security team
- No link clicked