📨 Lecture 27 — Email Analysis

1️⃣ What is Email Analysis?

Email Analysis means investigating emails to detect malicious intent such as phishing, spam, spoofing, or data theft.
Security analysts analyze:

- Sender details
- Email headers (SPF, DKIM, DMARC)
- Attachments
- URLs
- Message body & tone

The goal is to identify fake or suspicious emails before users interact with them.

2️⃣ What is Phishing Email? 🎣

Definition:
Phishing is a cyberattack technique where attackers trick users into sharing sensitive data (like passwords, OTPs, or credit card details) by pretending to be a trusted entity (like banks, delivery companies, or government).

Common signs of a phishing email: 🚨

1. ⚠️ **Threat or Urgency:** “Your account will be suspended in 2 hours!” – creates panic.
2. 📝 **Grammar & Spelling Errors:** Poorly written emails are red flags.
3. 📎 **Suspicious Attachments:** .exe, .zip, .scr, or unexpected invoices can carry malware.
4. 🔑 **Requesting Login Info:** Fake login pages mimic real websites to steal credentials.
5. 🎁 **Too Good To Be True Offers:** “You won $1000!” – lure you into clicking malicious links.

3️⃣ How Data Sharing Causes Phishing (Truecaller Example) 🧩

- **Truecaller** collects contact numbers and names from users who grant permissions.
- If an app like Truecaller has *read and write* SMS permissions, it can see OTPs, message content, or marketing details.
- Scammers can misuse this data to craft *personalized phishing emails* or SMS scams (e.g., fake offers from "RummyCircle", banking scams, etc.).
- ⚙️ **Tip:** Never give message access permission to apps that don't need it.

4️⃣ Email Authentication Mechanisms 🔐

These are the **three main protocols** used to verify whether an email really comes from the domain it claims to be from:

🧩 (1) SPF — *Sender Policy Framework*

📘 **Definition:**
SPF is a **TXT record** stored in the domain's **DNS (Domain Name System)**.
It lists which mail servers (IP addresses) are authorized to send emails on behalf of that domain.

⚙️ **How it works:**

1. You receive an email from, say, support@bank.com.
2. Your mail server checks the **SPF record** of bank.com.
3. If the sender's IP matches the list in that SPF record → ✅ **SPF Pass**
   Otherwise → ❌ **SPF Fail**

🔍 **Example SPF record:**

v=spf1 ip4:192.0.2.0/24 include:_spf.google.com -all

Meaning → Only IPs from that range or Google servers can send mail for this domain.

💡 **Why it's used:**
To prevent **email spoofing** — attackers cannot send fake emails pretending to be from your domain.

🧩 **(2) DKIM — *DomainKeys Identified Mail***

📘 **Definition:**
DKIM adds a **digital signature** to each outgoing email to prove it wasn't modified during transit.

⚙️ **How it works:**

1. The sending mail server signs the email with a **private key**.
2. The recipient's mail server retrieves the **public key** from the sender's DNS record.
3. The email's DKIM signature is verified —
    - If **matches** → ✅ DKIM Authenticated (email is genuine)
    - If **does not match** → ❌ DKIM Fail (possibly tampered or spoofed)

🔍 **Example DKIM DNS record:**

v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3...

💡 **Why it's used:**
To ensure message integrity — that no one altered or forged the email content after it left the sender's domain.

🧩 **(3) DMARC — *Domain-based Message Authentication, Reporting & Conformance***

📘 **Definition:**
DMARC sits **on top of SPF and DKIM**.
It decides what to do if SPF or DKIM fails — should the email go to inbox, spam, or be rejected?

⚙️ **How it works:**

1. The recipient's mail server checks both SPF & DKIM results.

2. DMARC policy defines the action if one or both fail.

🔍 **Example DMARC record:**

v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@domain.com; adkim=s; aspf=s;

🧠 **Interpretation:**

- p=quarantine → send failed emails to spam
- p=reject → block them completely
- p=none → just monitor/report

💡 **Why it's used:**
To protect the domain's reputation and users from phishing/spoofed emails.

5️⃣ How SPF, DKIM & DMARC Work Together 🔄

Step	Mechanism	Function	Result
1	**SPF**	Checks if sender's IP is allowed	IP verified ✅
2	**DKIM**	Checks if email content is signed & valid	Integrity verified ✅
3	**DMARC**	Checks SPF + DKIM results → decides inbox/spam/reject	Policy enforced ✅

🧩 **Combined Benefit:** Prevents attackers from sending fake emails using your domain name.

6️⃣ How to Analyze an Email Header (with MXToolbox) 🧰

When you suspect a phishing email, analyze its header:

Steps:

1. Open the email → click on **3 dots (⋮)** → select **"Show Original"**.
2. Copy the full header text (contains SPF, DKIM, DMARC results).
3. Go to 🌐 mxtoolbox.com → select "Analyze Header."

4. Paste the header → click **Analyze**.

You'll see results like:

Field	Description
DMARC Compliant ✅	Email passed both SPF & DKIM; domain policy satisfied.
SPF Alignment ⚠️	The domain in the "From" field and SPF domain don't match perfectly.
SPF Authenticated ✅	Sender's IP is listed in SPF record.
DKIM Alignment ⚠️	The DKIM domain differs from "From" domain (not ideal).
DKIM Authenticated ✅	DKIM signature matched successfully.
Return Path 📩	Actual email address used to send the message — can differ from "From:" (check for mismatch → may indicate spoofing).

7️⃣ Understanding the Return Path 📬

Definition:
Return Path is the address where *bounced or failed* emails are returned.
It's usually hidden from the user but visible in the email header.

Why important:

- Attackers often use a **different Return Path** than the visible sender address (From:).
- If the Return Path domain doesn't match the From domain → it's a strong sign of spoofing or phishing.

Example:

From: support@paypal.com

Return-Path: hacker@fake-domain.ru

🚨 **Red Flag!** — the real sender is not PayPal.

8️⃣ Practical Example 📄

Imagine an email claims to be from bankofsecure.com.
You run a header analysis:

Check	Result	Meaning
SPF	✅ Pass	IP authorized
DKIM	❌ Fail	Signature invalid or missing
DMARC	⚠️ Quarantine	Policy applied — email sent to spam

Return Path suspicious@malicious.org Mismatch detected

👉 Conclusion: **Spoofed email — likely phishing.**

9️⃣ Why Email Analysis is Important 🧠

- Prevents **phishing and fraud**.
- Detects **email spoofing** before users fall victim.
- Ensures **domain reputation** (so your genuine mails don't go to spam).
- Provides **forensic evidence** during cyber investigations.

🔟 Tips to Stay Safe 🛡️

✅ Check sender domain carefully (not just display name).
✅ Don't open unknown attachments.
✅ Hover over links before clicking — check if URL matches legitimate domain.
✅ Use **SPF, DKIM, and DMARC** on your organization's mail servers.
✅ Use **MXToolbox** or **Google Postmaster Tools** to monitor your email security setup.

⚙️ Bonus: Quick Reference Table

Mechanism	Type	Stored In	Checks	Prevents
SPF	TXT Record	DNS	Authorized sender IP	Spoofing
DKIM	TXT Record	DNS	Signature verification	Tampering
DMARC	TXT Record	DNS	SPF/DKIM policy enforcement	Fraud/Phishing

📜 Summary in One Line:

“SPF confirms the sender, DKIM confirms integrity, and DMARC confirms policy — together, they protect you from phishing and spoofed emails.” 💪