Computer Skills 2nd year

Email threats

Hussam Numan
Assistant Lecturer

Objectives

By the end of this workshop, students will be able to:

- Recognize common email threats (phishing, scams, malware).
- Secure their Gmail account with strong passwords and 2-Step Verification.
- Identify suspicious messages and report them.
- Use Gmail's built-in security tools effectively.

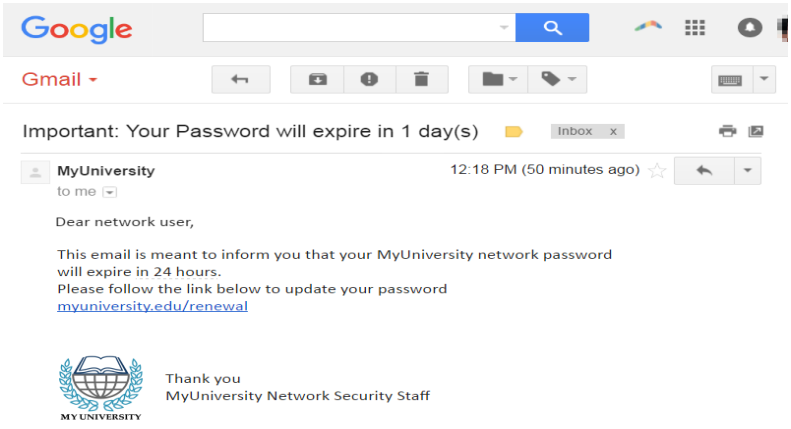
1. Introduction – Why Gmail Security Matters

- Gmail is one of the most used email platforms worldwide.
- Hackers often target Gmail accounts to steal information or spread scams.
- A single mistake (like clicking a fake link) can expose your entire account.

2. Common Gmail Threats

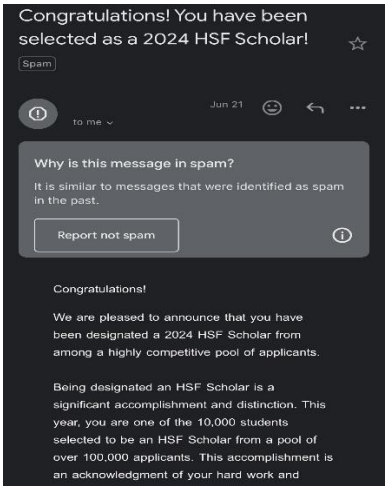
a. Phishing Emails

- Fake messages pretending to be from Google, banks, or friends.
- Example: "Your Gmail account will be deactivated — click here to verify."
- Always check the sender address and the URL before clicking.



b. Scam Emails

- Promise money, scholarships, or prizes.
- Ask for your personal information or payment details.



c. Malicious Attachments

- Files that install malware or spyware when opened.
- Never open unknown attachments, even from known senders.

3. Securing Your Gmail Account

a. Use a Strong, Unique Password

- At least 12 characters, mix of letters, numbers, and symbols.
- Avoid using names, birthdays, or “123456.”

- Use a password manager if needed.

b. Turn On 2-Step Verification (2FA)

- Go to: myaccount.google.com/security → *"2-Step Verification."*
- Adds a code sent to your phone or via Google Prompt when signing in.

c. Check Account Security Settings

- Visit: https://myaccount.google.com/security-checkup
- Review connected devices, third-party apps, and recovery options (phone/email).

d. Use Recovery Options

- Add your phone number and backup email to recover your account if lost.

e. Keep Your Browser and Apps Updated

- Security updates protect against new threats.

4. How to Recognize and Report Suspicious Emails

a. Warning Signs of a Fake Email:

- Urgent or threatening tone ("Your account will be deleted!")
- Grammar mistakes or weird spelling
- Sender's email doesn't match the company's official domain
- Links that don't lead to Google (hover to check)

b. How to Report in Gmail:

1. Open the suspicious email.
2. Click the **three dots (⋮)** on the top right.
3. Choose **"Report phishing."**
4. Delete the email — never reply or click links.

c. Block or Unsubscribe Safely:

- Use Gmail's **"Block sender"** or **"Unsubscribe"** buttons instead of random links.

5. Quick Tools and Habits

- Review your **recent account activity**: https://myaccount.google.com/device-activity
- Don't share passwords with anyone.
- Sign out on public computers (e.g., school labs).
- Avoid saving passwords on shared devices.
- Don't reuse the same password for social media and Gmail.

Gmail Safety Checklist:

- Strong password
- 2-Step Verification enabled
- Recovery email & phone added
- Regular security checkup
- Report phishing and block suspicious senders
- Never click unknown links or open weird attachments

Mini Quiz:

1. What is phishing?
2. What does 2-Step Verification do?
3. How can you report a suspicious email in Gmail?
4. Should you click "verify" links from strange messages? (Why not?)
5. Where can you check your Gmail account security?