Phishing Email Example 1: Banking Scam

From: security@yourbankalerts.com
Subject: Urgent: Unauthorised Login Attempt Detected

Dear Customer,

We have detected an unauthorised login attempt on your online banking account. For your safety, please log in using the link below to verify your identity.

[Secure Your Account](fake-link-bank.com)

Failure to verify your identity within 24 hours will result in your account being suspended.

Thank you for your prompt attention to this matter.

Sincerely,
Your Bank Security Team

Phishing Email Example 2: Fake Job Offer

From: careers@global-jobs.com
Subject: Exclusive Job Opportunity – Immediate Hire

Dear Candidate,

We are excited to offer you a high-paying remote job opportunity with our global team. Please click the link below to provide your personal details and CV to begin your onboarding process.

[Submit Your Details](phishing-link-jobs.com)

We are only selecting a few qualified individuals, so please complete this form within 24 hours to secure your spot.

Best regards,
Global Jobs Recruitment Team

Phishing Email Example 3: Fake Tax Refund

From: refunds@hmrctax.com
Subject: Tax Refund Notification

Dear Taxpayer,

We have calculated that you are eligible for a tax refund of £1,250. To claim this refund, please click the secure link below to verify your banking information.

[Claim Refund](fake-tax-refund.com)

Please note: This link will expire in 48 hours. Failure to claim the refund will result in the funds being forfeited.

Regards,
HMRC Tax Department

Phishing Email Example 4: Social Media Account Lock

From: support@instagramhelpdesk.com
Subject: Your Instagram Account Has Been Temporarily Locked

Dear User,

Due to suspicious activity on your Instagram account, we have temporarily locked your account for security reasons. Please click the link below to verify your identity and regain access.

[Verify Now](fake-link-instagram.com)

If you do not verify within 24 hours, your account may be permanently disabled.

Thank you,
Instagram Security Team

Phishing Email Example 5: Package Delivery Scam

From: tracking@delivery-service.com
Subject: Your Package Delivery is on Hold

Dear Customer,

Your recent order is being held due to incomplete shipping details. Please click the link below to confirm your delivery address and avoid delays.

[Update Delivery Info](scam-link-delivery.com)

If we do not receive confirmation within 48 hours, your package will be returned to the sender.

Sincerely,
Delivery Service Support

Phishing Email Example 6: Charity Donation Scam

From: donations@globalcharity.org
Subject: Emergency Relief Fund – Donate Now to Help!

Dear Supporter,

We are currently raising urgent funds to help victims of the recent natural disaster. Please consider donating to provide much-needed aid. Every penny counts.

[Donate Now](fake-charity-link.com)

Your generous donation will make a significant impact in helping those in need. Thank you for your support.

Warm regards,
Global Charity Fundraising Team

Phishing Email Example 7: Fake E-Commerce Promotion

From: offers@onlineshopworld.com
Subject: Exclusive Offer – 50% Off on Your Next Purchase!

Dear Valued Customer,

We're offering you an exclusive 50% discount on your next purchase! Click the link below to redeem your coupon code and start saving on the best deals.

[Claim Discount](phishing-link-shop.com)

Hurry, this offer expires in 24 hours!

Best regards,
Online Shop World Customer Support

Phishing Email Example 8: Fake Security Alert

From: alerts@antivirusprotection.com
Subject: Virus Detected – Immediate Action Required

Dear User,

We have detected a severe virus on your computer that could compromise your data. To prevent further damage, please click the link below to download our virus removal tool.

[Remove Virus Now](fake-antivirus-link.com)

Failure to act may result in permanent data loss. Thank you for using our security services.

Best regards,
Antivirus Protection Support Team

2. Social Engineer Role Card

This is the role card for the student acting as the “secret” Social Engineer. Print and hand it out discreetly to the selected student before the main activity begins.

Social Engineer Role Instructions Card:

Your Role: Social Engineer

Your task is to secretly use social engineering tactics to manipulate your group into sharing information with you.

You can use the following tactics:
- Blagging: Pretend to need personal information to complete a task.
- Shoulder Surfing: Try to peek at private information (like usernames or passwords).
- Pretexting: Create a believable fake story to gain trust and extract sensitive information.

Do not reveal your role to anyone! At the end of the activity, the class will try to guess who the Social Engineer was and how you used manipulation tactics.

Phishing and Social Engineering Reflection Worksheet

Learning Objectives:

- I can identify phishing attempts in emails and online communications.
- I can explain how social engineering manipulates individuals into sharing sensitive information.
- I can recognize social engineering tactics when they are used in everyday situations.

Success Criteria:

- All: Recognize basic phishing indicators and describe social engineering tactics like shoulder surfing and blagging.
- Most: Explain how phishing and social engineering tactics work together to deceive individuals.
- Some: Develop strategies for preventing both phishing and social engineering attacks.

Questions:

1. What red flags did you notice in the phishing emails you analysed?
   (List specific details such as fake URLs, spelling errors, or an urgent tone.)

---

2. How did the Social Engineer in your group try to manipulate others?
   (Describe the tactics they used, such as blagging, shoulder surfing, or pretexting. What was effective?)

---

3. What steps can you take in the future to avoid falling for phishing or social engineering tactics?
   (List practical strategies, such as verifying email addresses, not sharing personal details easily, etc.)

---

4. Group Analysis Worksheet (For Phishing Emails)

Each group will need to complete an analysis of the phishing emails they receive. Here's a Group Phishing Email Analysis Worksheet:

Phishing Email Analysis Worksheet

Group Members:

Phishing Email Number:

---

1. What did you identify as the major red flags in the phishing email?

(Examples: Spelling mistakes, fake URL, urgency, etc.)

---

2. What was the phishing tactic used to try and deceive the recipient?

(Examples: Fear of account lockout, promise of rewards, impersonation of a company, etc.)

---

3. How could someone have avoided falling for this phishing email?

(List strategies: Checking the sender’s email address, not clicking links, contacting the company directly, etc.)

---

4. How might phishing and social engineering work together in this example?

(Explain how someone could follow up with a phone call, pretexting, or blagging after the email.)

---

5. Social Engineering Tactics Overview Handout

This resource provides students with an overview of the social engineering tactics they'll be discussing and encountering. You can hand this out after the starter activity to solidify their understanding of each term:

Social Engineering Tactics: An Overview

- Blagging: This involves pretending to be someone else (e.g., a company employee or authority figure) to extract personal information from a victim.

- Shoulder Surfing: A form of information theft where the attacker looks over someone’s shoulder to steal personal details, such as passwords or usernames.
- Pretexting: This involves creating a fake story or scenario to trick someone into giving personal information. The attacker often uses an elaborate excuse to gain trust.
- Phishing: The practice of sending fake emails or messages that appear legitimate to trick individuals into clicking on malicious links or sharing personal details.
