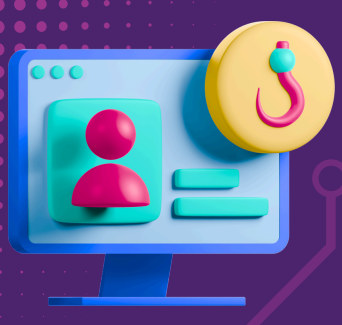
PHISHING AWARENESS

DO NOT TAKE THE BAIT!



PHISHING

is a cyberattack where scammers pretend to be trusted individuals or organizations to trick you into giving personal information, clicking harmful links, or downloading malware.

COMMON EXAMPLES OF PHISHING

FAKE BANK ALERTS
asking you to "verify your account."

DELIVERY SERVICE NOTIFICATIONS
saying your package can't be delivered.

TECH SUPPORT SCAMS
claiming your device has a virus.

EMAIL FROM A "BOSS"
requesting urgent gift card purchases.

SOCIAL MEDIA MESSAGES
asking you to click a suspicious link.

EXAMPLES EMAIL GALLERY (PHISHING)

FAKE BANK ALERT
Subject: URGENT: Account Locked
Body: Your account has been suspended. Verify now: asking you to click a suspicious link.

Suspicious Parts:
- Urgent tone
- Strange link
- Non-official domain
- Grammar errors

DELIVERY SCAM
Subject: Package Delivery Failed
Please pay the ₱30 redelivery fee: Subject: URGENT: Account Locked
Body: Your account has been suspended. Verify now: asking you to click a suspicious link.

Suspicious Parts:
- Unexpected fee
- Unfamiliar website
- Vague sender info

BOSS GIFT CARD SCAM
Can you buy 5 Apple gift cards urgently? I need them for clients.

Suspicious Parts:
- Urgent request
- Abnormal behavior from your boss
- Sent from a personal email

Suspicious Parts:
- Shortened link
- No company branding
- Generic message

FAKE PASSWORD RESET
We detected unusual activity. Reset your password here: bit.ly/password-help

COMPARISON: FAKE VS. REAL EMAIL

REAL EMAIL

- Uses your actual name
- Professional grammar and formatting
- Legitimate domain name
- No pressure tactics
- Doesn't ask for sensitive info
- You can verify sender through official channels

FAKE EMAIL

- "Dear Customer" (generic greeting)
- Wrong grammar/spelling
- Suspicious links
- Unverified sender
- Threats/urgency
- Requests personal data

10 TIPS FOR AWARENESS

1.CHECK THE SENDER'S EMAIL ADDRESS.

2. HOVER OVER LINKS BEFORE CLICKING.

3. NEVER SHARE PASSWORDS OR OTP CODES.

4. IGNORE EMAILS ASKING FOR URGENT ACTION.

5. DON'T DOWNLOAD ATTACHMENTS FROM UNKNOWN SOURCES.

6. ENABLE MULTI-FACTOR AUTHENTICATION (MFA).

7. VERIFY THROUGH OFFICIAL CHANNELS (CALL THE BANK/COMPANY).

8. UPDATE ANTIVIRUS AND DEVICE SOFTWARE.

9. USE STRONG, UNIQUE PASSWORDS.

10. REPORT SUSPICIOUS EMAILS IMMEDIATELY.

"PHISHING WORKS ONLY WHEN YOU LET YOUR GUARD DOWN—STAY ALERT."

phishing attacks succeed when we stop being careful. Staying alert and double-checking messages helps prevent scammers from tricking us.