Final Assessment Question Bank (40 Questions)

Part A: Final Assessment Content and Question Design

Module 1: Foundations & Psychology (8 Questions)

1. A person receives a text message stating: "Your BPI account has been flagged for a suspicious transaction. To avoid suspension, please log in immediately via this link: [bit.ly/bpi-secure-login-check]." This message primarily preys upon which two psychological principles?

A. Authority and Liking
B. Urgency and Social Proof
C. Authority and Urgency
D. Liking and Scarcity

2. A key distinction of social engineering is its focus on the "human element." Why is this considered a significant threat even to organizations with strong technical security like firewalls?

A. Because social engineers can physically disable firewalls without being detected.
B. Firewalls are not effective against modern malware.
C. A social engineer can persuade a legitimate user to perform actions that bypass all technical defenses.
D. Because the "human element" is only a weakness in small companies, not large ones.

3. An attacker creates a fake social media profile impersonating a popular influencer. They host a "giveaway" requiring participants to share the post and enter their email and password on a fake website. The attack's high participation rate is most likely due to the exploitation of:

A. Authority and Urgency
B. Scarcity and Liking
C. Liking and Social Proof
D. Urgency and Scarcity

4. Which of the following scenarios is the CLEAREST example of exploiting the principle of Authority?

A. An email from a "friend" asking for a small amount of money via GCash.
B. A pop-up ad claiming "Only 3 items left in stock!" for a popular product.
C. A phone call from someone claiming to be a PNP Anti-Cybercrime Group agent, demanding personal information for an "ongoing investigation."
D. A website that shows testimonials from hundreds of "satisfied customers."

5. A social engineering attack is fundamentally an act of:

A. Technical exploitation
B. Psychological manipulation
C. Network intrusion
D. Software piracy

6. An email promises a free, exclusive in-game item to the "first 100 students" who log in with their school credentials on a linked website. This tactic heavily relies on the principle of:

A. Authority
B. Social Proof
C. Liking
D. Scarcity

7. Why is social engineering often preferred by cybercriminals over purely technical hacking methods?

A. It requires more advanced programming skills, making it a greater challenge.
B. It is generally easier and more effective to exploit human trust and psychological biases than to find and exploit a complex software vulnerability.
C. It guarantees that the attack will never be detected by security software.
D. It can only be performed by people who are naturally very friendly and charismatic.

8. A scammer sends a message pretending to be from a well-known charity, telling a compelling, emotional story about a recent disaster and asking for donations. This approach is primarily leveraging which psychological principle?

A. Authority
B. Urgency

C. Liking/Empathy
D. Scarcity

Module 2: Attack Tactics (8 Questions)

9. An employee finds a USB drive in the office parking lot labeled "Executive Salary Bonuses Q3." Curious, they plug it into their work computer, which then installs malware. This attack is a prime example of:

A. Pretexting
B. Baiting
C. Tailgating
D. Shoulder Surfing

10. An attacker calls a company's front desk, impersonates a known IT vendor, and uses technical jargon to explain a fake "urgent system upgrade." They convince the receptionist to reveal the internal Wi-Fi password. This attack's success relies on a well-crafted:

A. Phishing link
B. Bait
C. Pretext
D. Tailgate

11. While a student is typing their password at a crowded library computer, another person stands nearby, pretending to read a book, but is actually watching the student's keystrokes. This is a classic example of:

A. Vishing
B. Baiting
C. Tailgating
D. Shoulder Surfing

12. What is the primary difference between a generic phishing attack and a pretexting attack?

A. Phishing uses email, while pretexting only uses phone calls.
B. Phishing attacks are always for financial gain, while pretexting is for information.

C. Pretexting involves creating a detailed, fabricated scenario to build trust, while phishing is often a less-targeted, broader attempt.
D. Pretexting uses malware, whereas phishing only uses malicious links.

13. A person wearing a delivery uniform is standing by a secure office door with their hands full of packages. They make eye contact with an employee and ask, "Could you please get the door for me?" The employee swipes their card and holds the door open. This is a security breach known as:

A. Baiting
B. Pretexting
C. Tailgating
D. Shoulder Surfing

14. An email sent to all students contains a link to a "mandatory student satisfaction survey" with a chance to win a new laptop. The link leads to a fake login page designed to steal credentials. This entire scheme is best described as:

A. A phishing attack using bait.
B. A pretexting attack using a tailgate.
C. A shoulder surfing attack using social proof.
D. A vishing attack using scarcity.

15. Which of the following is an example of a PHYSICAL social engineering tactic?

A. Sending a fraudulent email with an urgent request for a password reset.
B. Calling a user and pretending to be from tech support.
C. Watching someone enter their ATM PIN from a short distance away.
D. Creating a fake social media profile to befriend a target.

16. "Vishing" is a specific type of social engineering attack that is conducted via:

A. Email
B. Voice calls
C. Text messages
D. Malicious USB drives

Module 3: Proactive Defense (8 Questions)

17. A student uses a very strong, unique password for their MMDC email and has Multi-Factor Authentication (MFA) enabled. A hacker successfully steals their password from a breach on a completely unrelated gaming website. Why is the hacker still very unlikely to access the student's MMDC email?

A. Because the school's firewall will recognize the password came from a breach.
B. Because MFA requires a second, separate verification factor (like a phone code) that the hacker does not possess.
C. Because the hacker will not know the student's email address.
D. Because MFA automatically changes the password after a known breach.

18. When analyzing a URL like https://mmdc-edu.ph.account-services.com/login, what is the most significant red flag?

A. The URL uses "https."
B. The URL contains the letters "mmdc."
C. The true top-level domain is "account-services.com," not "mmdc-edu.ph."
D. The URL path includes the word "login."

19. What is the primary security risk of "oversharing" personal information like your full birthdate, mother's maiden name, and first pet's name on public social media?

A. It can cause your friends to become jealous.
B. It consumes too much mobile data.
C. It provides attackers with the answers to common security questions used for account recovery.
D. It automatically makes your accounts non-compliant with privacy laws.

20. A password manager's primary function is to solve which core cybersecurity problem?

A. The difficulty of creating and remembering multiple, strong, unique passwords for every online account.
B. The need to scan all incoming emails for potential phishing links.
C. The requirement to have Multi-Factor Authentication on every account.
D. The risk of physical shoulder surfing in public places.

21. Before clicking a link in an unsolicited email, the "hover to verify" technique is crucial. This technique allows you to:

A. Activate a security scan of the link before opening it.

B. Preview the actual destination URL to see if it matches the link's text and looks legitimate.
C. See a screenshot of the destination website without actually visiting it.
D. Automatically report the link to IT if it is deemed suspicious.

22. Which of the following passwords is the strongest according to the principles taught in the module?

A. P@ssword2025
B. Mmdc-student-123
C. Manok!Pusa;Daga_Baka?
D. MyBdayIs08152005

23. Setting your social media profile to "Private" is a key defense. Its main purpose is to:

A. Prevent your account from ever being hacked.
B. Ensure your posts get more engagement from friends.
C. Allow you to control who can see your personal information, thus shrinking your vulnerable digital footprint.
D. Block all advertisements from appearing on your feed.

24. In the context of website security, what does the "s" in "https://" signify?

A. The website is "special" and for members only.
B. The website has a "simple" design for fast loading.
C. The connection to the website is "secure" and encrypted.
D. The website is a "static" page with no interactive elements.

Module 4: Incident Response (8 Questions)

25. You realize you have just entered your school portal credentials into a convincing phishing site. You do not have immediate access to another "clean" device. What is the BEST sequence of actions?

A. Report to IT, disconnect from the internet, then run an antivirus scan.
B. Disconnect from the internet, run an antivirus scan, then change your password from the same device.

C. Immediately open a new browser tab, go to the official school portal, change your password, then report the incident to IT.
D. Wait to see if any suspicious activity occurs before taking any action.

26. In the context of incident response, what is the primary purpose of "containment" (e.g., disconnecting from the internet)?

A. To automatically delete any malware that has been downloaded.
B. To prevent the threat from spreading further or exfiltrating more data.
C. To help the IT department trace the physical location of the attacker.
D. To reset your device to its factory settings.

27. Your friend's social media account sends you a message with a suspicious link. You suspect their account has been hacked. What does the principle of "Digital Bayanihan" suggest you do?

A. Click the link to investigate where it goes.
B. Ignore the message and block your friend's account.
C. Immediately contact your friend through a different, trusted method (like a phone call) to warn them their account is compromised and not to click the link yourself.
D. Post on your own social media that your friend's account was hacked.

28. After regaining access to a compromised email account, why is it critical to review account activity logs and connected third-party apps?

A. To see if the hacker read any of your old emails.
B. To identify and remove any backdoors (like a malicious app) the hacker may have set up to regain access later.
C. To delete all emails the hacker may have sent.
D. To report all third-party apps to the police.

29. You receive a credible threat of harassment from another student via your MMDC email. According to the MMDC Reporting Protocol, which office is the most appropriate primary contact for this specific issue?

A. The MMDC IT Helpdesk
B. Your course professor
C. The Opisina ng Estudyante (Student Affairs Office)
D. The campus security office

30. What is the most significant risk of NOT reporting a compromised school account to the IT department?

A. You might be fined for violating school policy.
B. The attacker could use your account to launch attacks against other students and faculty, and IT will be unaware of the threat to the network.
C. You will not be able to change your password without their help.
D. Your academic records might be deleted permanently.

31. The "Recovery Toolkit" emphasizes using a "clean device" to change passwords after a compromise. A device is considered "clean" if:

A. It has recently been physically wiped down.
B. It has all its software updated to the latest versions.
C. You can be reasonably sure it is free from malware or keyloggers that could capture your new password.
D. It has never been used to access the internet before.

32. After discovering a financial scam, the module suggests reporting to the PNP Anti-Cybercrime Group with guidance from MMDC staff. Why is involving the school recommended?

A. Because the school can provide legal representation for you.
B. To ensure the report is filed correctly and to provide institutional support, as the incident may affect the broader school community.
C. Because the school is legally required to pay back any financial losses.
D. To get the scammer expelled from the school.

Module 5: Advanced Threats & Cyber Defender Mindset (8 Questions)

33. An attacker uses an AI tool to analyze a student's public LinkedIn profile, noting their career interests and recent project involvements. They then craft a hyper-realistic phishing email from a "recruiter" with specific details about a job that perfectly matches the student's profile. This is an example of:

A. Quishing
B. AI-powered spear phishing
C. A deepfake audio attack

D. An Advanced Persistent Threat (APT)

34. A finance employee receives a video call on Microsoft Teams from their CFO, who instructs them to make an urgent, confidential wire transfer. The video looks and sounds exactly like the CFO, but it is actually a real-time AI-generated impersonation. This attack is known as a:

A. Quishing attack
B. Smishing attack
C. Deepfake scam
D. Baiting attack

35. You see a QR code sticker on a table at a popular coffee shop advertising a "Free Coffee Refill." The most secure course of action is to:

A. Scan it immediately to see if the offer is real.
B. Ask another customer if they have used the code successfully.
C. Avoid scanning it, as it could be a malicious "Quishing" attempt leading to a scam website.
D. Take a picture of the QR code and try to analyze it later.

36. The concept of "continuous learning" in cybersecurity is essential because:

A. Cybersecurity certifications expire every year.
B. Attackers' tools, tactics, and procedures (TTPs) are constantly evolving, and yesterday's defense may not be effective against tomorrow's threat.
C. You need to memorize the name of every new virus that is discovered.
D. The fundamental principles of social engineering change completely every few months.

37. Which of the following best embodies the "Cyber Defender Mindset" as a proactive community member?

A. Keeping your knowledge of cybersecurity to yourself to maintain a personal advantage.
B. Helping a less tech-savvy family member understand the risks of phishing and set up Multi-Factor Authentication on their accounts.
C. Assuming that since you are knowledgeable, you are immune to all social engineering attacks.
D. Only reporting security incidents after you have personally lost money or data.

38. An "Advanced Persistent Threat" (APT) often begins with a simple social engineering trick. What is the primary goal of an APT attacker after gaining initial access?

A. To cause as much immediate and visible damage as possible.
B. To announce their presence to the network administrators.
C. To remain undetected within the network for a long period to quietly exfiltrate sensitive data.
D. To steal a single password and then immediately exit the network.

39. You are in a group chat, and a classmate shares a link to a website offering "free answers" to an upcoming exam. Recognizing this as both an academic integrity issue and a probable security risk (baiting/phishing), what is the most responsible action?

A. Silently leave the group chat to avoid involvement.
B. Click the link to confirm it's a scam before warning others.
C. Publicly call out the classmate for cheating.
D. Privately message the classmate about the risks, advise others in the chat not to click the link, and report the situation to a professor or relevant authority.

40. The ultimate goal of the "Digital Bayanihan" concept is to:

A. Create a formal neighborhood watch group to patrol for cybercriminals.
B. Foster a culture of shared responsibility and collective defense, making the entire community more resilient to cyber threats.
C. Ensure that every student becomes a professional cybersecurity expert.
D. Replace the need for an official IT department by crowdsourcing security.

Part B: Answer Sheet, including Automated Feedback and Concluding Message

Feedback for Each Question:

1. **Correct (C):** "Correct! The message impersonates an authority (BPI) and creates a false sense of urgency (account suspension) to provoke a hasty, unthinking response."
   Incorrect (A, B, D): "Incorrect. While it uses Authority, the primary pressure tactic here is the time limit ('immediately'), which is Urgency, not Liking or Social Proof."

2. **Correct (C):** "Correct! This is the core concept of the human firewall. Technical controls can be rendered useless if an attacker tricks an authorized person into misusing their legitimate access."
   Incorrect (A, B, D): "Incorrect. The 'human element' is a universal vulnerability because social engineers manipulate trust, which exists in organizations of all sizes, to bypass technology."

3. **Correct (C):** "Correct! The attack leverages the Liking of a popular influencer and the Social Proof of seeing many others participating to lower the target's guard."
   Incorrect (A, B, D): "Incorrect. The main psychological hooks are the appeal of the influencer (Liking) and the perception that 'everyone is doing it' (Social Proof)."

4. **Correct (C):** "Correct! This scenario uses the perceived power and legitimacy of a law enforcement agency to intimidate the target into complying with a request for information."
   Incorrect (A, B, D): "Incorrect. This is the clearest example of Authority because it impersonates an organization with official power, making the request seem non-negotiable."

5. **Correct (B):** "Correct! At its core, social engineering bypasses technology to exploit human psychology, trust, fear, and curiosity."
   Incorrect (A, C, D): "Incorrect. While an attack might involve technical elements, the fundamental method of social engineering is the manipulation of a person."

6. **Correct (D):** "Correct! The 'first 100 students' creates a sense of limited availability, or Scarcity, designed to make people act quickly without thinking."
   Incorrect (A, B, C): "Incorrect. The primary motivator here is the fear of missing out on a limited offer, which is the definition of Scarcity."

7. **Correct (B):** "Correct! Exploiting human nature is often less complex and more reliable for criminals than finding a zero-day exploit in constantly updated software."
   Incorrect (A, C, D): "Incorrect. Cybercriminals often choose social engineering because it is the path of least resistance—targeting predictable human behavior is often easier than breaking complex code."

8. **Correct (C):** "Correct! The attacker is building rapport and appealing to the target's empathy and desire to help (Liking) through a fabricated emotional story."
   Incorrect (A, B, D): "Incorrect. The appeal is emotional and relational, designed to make you like or sympathize with the cause, which is a form of the Liking principle."

9. **Correct (B):** "Correct! The USB drive is the 'bait,' using curiosity and a provocative label ('Executive Salary Bonuses') to lure the victim into taking the unsafe action of plugging it in."
   Incorrect (A, C, D): "Incorrect. This is not Pretexting (a fabricated story) or a physical breach like Tailgating. The attack relies on a tempting object to exploit the victim's curiosity, which is the definition of Baiting."

10. **Correct (C):** "Correct! The attacker fabricated a believable identity (IT vendor) and scenario (urgent upgrade) to build trust and achieve their goal. This detailed story is a pretext."
    Incorrect (A, B, D): "Incorrect. The success of this attack hinges entirely on the detailed, made-up story, which is the definition of a pretext."

11. **Correct (D):** "Correct! This is the exact definition of shoulder surfing: surreptitiously observing someone to steal their confidential information as they type it."
    Incorrect (A, B, C): "Incorrect. This is a physical, observational attack. Vishing, Baiting, and Tailgating involve different methods of deception or physical access."

12. **Correct (C):** "Correct! Pretexting is typically a more targeted and elaborate attack that relies on a well-researched, believable story to manipulate the victim."
    Incorrect (A, B, D): "Incorrect. The key differentiator is the depth and customization of the story used. Pretexting is a deep, convincing narrative, while phishing can be a wide, generic net."

13. **Correct (C):** "Correct! This is a classic tailgating tactic that exploits a person's natural tendency to be polite and helpful to gain unauthorized physical access."
    Incorrect (A, B, D): "Incorrect. The goal is to gain unauthorized physical entry by following an authorized person, which is the definition of tailgating."

14. **Correct (A):** "Correct! The overall scheme is phishing (stealing credentials via a fake login page), and it uses bait (the chance to win a laptop) to entice users to click."
    Incorrect (B, C, D): "Incorrect. The attack's method is phishing, and its lure is the bait of a potential prize. The other terms do not fit the scenario."

15. **Correct (C):** "Correct! Shoulder surfing requires the attacker to be physically present to observe the victim, unlike the other options which are digital."
    Incorrect (A, B, D): "Incorrect. The other options describe attacks that occur over digital channels (email, phone, social media). Shoulder surfing happens in the physical world."

16. **Correct (B):** "Correct! 'Vishing' is a portmanteau of 'voice' and 'phishing,' referring specifically to phishing attacks conducted over the phone."
    Incorrect (A, C, D): "Incorrect. Vishing is exclusively voice-based. Phishing via text is 'Smishing,' and email is just 'phishing'."

17. **Correct (B):** "Correct! This question tests the core function of MFA. Even with the password ('something you know'), the hacker lacks the second factor ('something you have,' like a code from the user's phone)."
    Incorrect (A, C, D): "Incorrect. The strength of MFA is that it requires a separate

verification factor. A firewall wouldn't know where the password came from, and MFA doesn't automatically change passwords."

18. **Correct (C):** "Correct! This is a critical URL analysis skill. The text before the top-level domain (.com, .org, etc.) is the true domain. In this case, the user is connecting to 'account-services.com,' not an official MMDC site."
    Incorrect (A, B, D): "Incorrect. The most critical part of a URL to inspect for authenticity is the true top-level domain, which reveals the actual owner of the site."

19. **Correct (C):** "Correct! This information is frequently used in 'Forgot Password' security questions, and providing it publicly makes it easy for an attacker to impersonate you and reset your passwords."
    Incorrect (A, B, D): "Incorrect. While there are many risks to oversharing, giving away the answers to common security questions is a direct and severe threat to your account security."

20. **Correct (A):** "Correct! Password managers are designed to eliminate the need for humans to remember dozens of complex, unique passwords, thereby improving overall password hygiene."
    Incorrect (B, C, D): "Incorrect. While other tools handle those functions, a password manager's specific and primary purpose is to manage credentials securely."

21. **Correct (B):** "Correct! This simple action reveals the link's true destination before you navigate to it, allowing you to spot deceptive URLs designed to look legitimate."
    Incorrect (A, C, D): "Incorrect. The 'hover' technique is a manual inspection tool for you, the user. It does not trigger any automated scans or reporting."

22. **Correct (C):** "Correct! This password is long, complex (using uppercase, lowercase, numbers, and symbols), and avoids predictable dictionary words or personal information."

Incorrect (A, B, D): "Incorrect. The other options are either too short, use predictable patterns (dictionary words, personal info), or lack sufficient complexity."

23. **Correct (C):** "Correct! A private profile limits who can view your data, which reduces the information available to scammers for pretexting and makes it harder for them to target you."
    Incorrect (A, B, D): "Incorrect. A private profile is a powerful tool for controlling your digital footprint and minimizing the data available to attackers."
24. **Correct (C):** "Correct! HTTPS (Hypertext Transfer Protocol Secure) indicates that the data transmitted between your browser and the website is encrypted and secure."
    Incorrect (A, B, D): "Incorrect. The 's' is a critical indicator of a secure, encrypted connection, which is a key part of website verification."

25. **Correct (C)**: "Correct! The immediate threat is the compromised password. Changing it instantly from the official site contains the damage. The other actions are important but secondary to locking the attacker out."
    Incorrect (A, B, D): "Incorrect. Disconnecting first would prevent you from changing your password online. The highest priority is to invalidate the stolen password immediately by changing it on the official site."

26. **Correct (B):** "Correct! Containment is about damage control. Disconnecting stops malware from 'calling home' or spreading across a network and prevents an active attacker from stealing more data."
    Incorrect (A, C, D): "Incorrect. The goal of containment is purely defensive: to stop the attack from progressing and to limit the total impact."

27. **Correct (C):** "Correct! This action protects your friend by alerting them to the hack through a secure channel and protects the community by preventing the spread of the malicious link."
    Incorrect (A, B, D): "Incorrect. This is a perfect application of Digital Bayanihan: taking a responsible action that protects both an individual and the wider community from a threat."

28. **Correct (B):** "Correct! Hackers often grant permissions to malicious third-party apps or set up forwarding rules to maintain persistent access even after a password change. This step is crucial for complete cleanup."
    Incorrect (A, C, D): "Incorrect. While seeing what the hacker did is useful, the most critical security action is to find and remove any backdoors they may have left behind."

29. **Correct (C):** "Correct! The Student Affairs Office is designated to handle issues related to student welfare, conduct, harassment, and cyberbullying, whereas the IT Helpdesk handles technical issues."
    Incorrect (A, B, D): "Incorrect. The reporting protocol directs different types of issues to the appropriate office. Harassment and threats are a student affairs matter, not a technical one."

30. **Correct (B):** "Correct! A single compromised account can be a gateway for an attacker to target the entire institution. Reporting allows IT to mitigate this larger threat."
    Incorrect (A, C, D): "Incorrect. The most significant risk is not personal but communal. Your compromised account becomes a threat to the entire school network and its users."

31. **Correct (C):** "Correct! The purpose of using a 'clean' device is to ensure that no keylogging malware is present that could steal the new password as you type it."
    Incorrect (A, B, D): "Incorrect. A 'clean' device in a cybersecurity context specifically means one that is trusted to be free of malware that could compromise your recovery efforts."

32. **Correct (B):** "Correct! Involving the school ensures the report is handled correctly and leverages the institution's resources, especially since the scam might be targeting other students."
    Incorrect (A, C, D): "Incorrect. The school's role is to provide guidance and support, recognizing that a threat against one student may be a threat against many."

33. **Correct (B):** "Correct! This is a highly targeted form of phishing (spear phishing) that uses AI to craft a personalized and extremely convincing lure based on the victim's own publicly available data."
    Incorrect (A, C, D): "Incorrect. The use of AI to create a highly personalized email for a specific target is the definition of AI-powered spear phishing."

34. **Correct (C):** "Correct! A deepfake scam involves using AI to create a convincing but fake video/audio impersonation of someone, often a person in a position of authority."
    Incorrect (A, B, D): "Incorrect. This advanced attack, which uses AI-generated video in real-time to impersonate someone, is a clear example of a deepfake scam."

35. **Correct (C):** "Correct! Unverified QR codes in public spaces are a significant vector for 'Quishing.' The safest approach is to assume they are malicious unless you can verify their source."
    Incorrect (A, B, D): "Incorrect. Given the rise of Quishing, the most secure action is to be skeptical of all unverified, public QR codes."

36. **Correct (B):** "Correct! Cybersecurity is a dynamic field. New vulnerabilities and attack methods emerge constantly, requiring continuous learning to maintain an effective defense."
    Incorrect (A, C, D): "Incorrect. The core reason for continuous learning is that the threats themselves are constantly changing, so our defenses must adapt."

37. **Correct (B):** "Correct! The Cyber Defender Mindset extends beyond personal security to protecting the community. Sharing knowledge and helping others improve their security is a core tenet of Digital Bayanihan."
    Incorrect (A, C, D): "Incorrect. A true Cyber Defender is proactive and community-oriented, understanding that shared knowledge leads to collective strength."

38. **Correct (C):** "Correct! The 'Persistent' in APT means the attacker's goal is long-term, low-and-slow access to gather as much valuable data as possible without being detected."
    Incorrect (A, B, D): "Incorrect. APTs are defined by their stealth and long-term goals, not by causing immediate and loud disruption."

39. **Correct (D):** "Correct! This response is the most responsible as it addresses the security risk without causing a panic, deals with the academic issue privately, and reports it to the proper channels."
    Incorrect (A, B, C): "Incorrect. The most mature and effective response involves handling the situation discreetly while ensuring the threat is contained and reported."

40. **Correct (B):** "Correct! Digital Bayanihan is about creating a resilient community where every member feels a sense of ownership over security, making the group as a whole much harder to attack."
    Incorrect (A, C, D): "Incorrect. The goal is cultural—to build a community with a proactive, collective defense mindset, not to replace formal security structures."

Part C: Final Messages

Final Message (If Score >= 80% - PASS):

Congratulations, Cyber Defender!

You have successfully passed the Final Assessment and demonstrated a strong, practical understanding of social engineering threats and defenses. Your high score proves you have the skills to protect yourself and the knowledge to help protect our entire community.

You have officially earned the title of MMDC Cyber Defender.

You may now proceed to generate your Certificate of Completion. Wear it with pride—you are a crucial part of our collective digital defense.

Final Message (If Score < 80% - FAIL):

Keep Going, Future Defender!

It looks like you didn't reach the 80% passing score on this attempt. That's okay—this is a challenging and critical subject, and the most important thing is to master the material, not just to pass. True defenders are built through persistence.

We strongly encourage you to review the modules again, paying close attention to the topics where you felt unsure.

When you are ready, you can take the assessment again. You will be presented with a different set of questions to ensure a comprehensive understanding.

We are confident that with a little more review, you will succeed. You can do this