CRICOS Provider No. 00103D | RTO Code 4909 | TEQSA No. PRV12151 (Australian University)

## ITECH1502 Cybersecurity Fundamentals

## Week 3 Lab Activities

# Human Factors in Cybersecurity

**Lab Overview:**

This week’s lab series explores how **human psychology** and behavioral manipulation contribute to cyber threats. Students will examine how **social engineering tactics** exploit trust, curiosity, authority, and routine, often bypassing even the most secure technical controls.

The three lab tasks are designed to:

1. Develop an in-depth understanding of **social engineering attack types and psychological triggers**.
2. Enable critical analysis of **real-world incidents** to identify security gaps and human vulnerabilities.
3. Encourage students to apply **defensive thinking** by proposing behavior-based security strategies and reflecting on personal and organizational awareness.

**Learning Outcomes Assessed:**

1. Critically evaluate how psychological manipulation techniques and cognitive biases contribute to real-world cybersecurity breaches and reflect on behavioral vulnerabilities in personal or organizational contexts.
2. Critically evaluate how social engineering exploits psychological triggers and behavioral patterns to compromise cybersecurity and propose awareness-based defense strategies.
3. Critically evaluate common social engineering tactics by analyzing real-world attack scenarios and synthesizing practical defense strategies tailored to organizational and individual vulnerabilities.

### ****🔐 Lab Task 1: Cyber Threat Analysis of a Real-World Incident (1 Mark)****

In this task, you will investigate how **human behavior, psychological biases**, and **social manipulation** contribute to successful cyberattacks. By analyzing a real-world incident and reflecting on human vulnerabilities, you will understand why attackers target people—not just systems.

#### ****Step 1: Choose One Real-World Case****

Pick **one high-profile cybersecurity breach** where human behavior played a key role. Choose from the list below or find your own:

* Twitter breach (2020)
* RSA spear-phishing attack (2011)
* Sony Pictures hack (2014)
* Colonial Pipeline ransomware (2021)
* Medibank or Optus data breach (Australia)

#### ****Step 2: Complete the Human Vulnerability Table****

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident** | **Manipulated Bias** | **Type of Social Engineering** | **Point of Failure (Human Action)** |
| Medibank | Trust bias | Phishing, | Employee trusted a fraudulent request and clicked a sketchy link |

#### ****Step 3: Write a 200–250 Word Reflection****

Respond to the following:

1. **How did human behavior contribute to the breach?**
2. **What cognitive or emotional trigger was exploited?**
3. **If you were the employee in that scenario, how could you have responded differently?**

Human behaviour contributed to the breach through misplaced trust and failure to verify the source of a communication. The attacker exploited authority bias, making the employee more likely to comply with a request that appeared to come from a powerful figure. Emotional triggers like urgency and trust also played a role, clouding judgment. If I were the employee, I would have paused to verify the sender’s identity through a separate channel before acting.

### 📘 ****Marking Criteria (1 mark)****

|  |  |
| --- | --- |
| Criteria | Description |
| 1 mark | Completed table and thoughtful reflection showing understanding of human vulnerabilities in cyberattacks |
| 0.5 mark | Partial completion or surface-level reflection |
| 0 mark | Not submitted or lacks relevance to human factors |

### ****Lab Task 2: Psychology of Cyberattacks and Social Engineering (1 Mark)****

This task invites you to apply your understanding of **psychological manipulation in cyberattacks** by analyzing real-world social engineering examples and reflecting on how cognitive and emotional biases influence user behavior.

#### ****1. Analyze Real-World Social Engineering Examples****

Choose **any two** of the social engineering attack types and find **real-world incidents** where they were used:

* Phishing (e.g., credential harvesting via fake email)
* Baiting (e.g., USB or malware-laced downloads)
* Impersonation (e.g., CEO fraud or tech support scam)
* Tailgating (e.g., unauthorized physical access)

Complete the following table for each case:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Attack Type** | **Incident Summary (max 100 words)** | **Psychological Triggers** | **Manipulation Tactics Used** | **Why Did It Work?** |
| Phishing | The incident of the Medibank breach was most likely was phishing as the company received a suspicious email which there got tricked by which caused the whole incident | fear, urgency,trust | pretexting | The employee responded without verifying the sender |

#### ****2. Critical Reflection (200–250 words)****

In a short reflection, respond to the following:

* Technical security frequently fails to protect against social engineering because it focuses on systems rather than human behavior. Attackers use emotions such as fear, speed, and trust to influence others into circumventing protocols. In Medibank's situation, phishing most likely tricked an employee into providing access. Better awareness training, such as spotting pretexts and confirming requests, may have prevented this. Personally, I'd avoid deception by slowing down, confirming sources across other channels, and consulting with colleagues.
* Why do you think **technical security measures often fail** against social engineering attacks?
* How could better **awareness training or communication design** have prevented the incidents you analyzed?
* What would you personally do to **resist psychological manipulation** in a high-pressure cyber scenario?

## ✅ ****Marking Guide – Lab Task 2: Psychology of Cyberattacks and Social Engineering (1 Mark)****

|  |  |  |  |
| --- | --- | --- | --- |
| ****Criteria**** | ****Excellent (Full Mark)****<br>****1.0**** | ****Satisfactory (Partial Mark)****<br>****0.5**** | ****Unsatisfactory (No Mark)****<br>****0.0**** |
| **Analysis of Two Social Engineering Incidents** | Clear, relevant real-world examples selected; all columns in table are thoroughly and accurately completed with strong insight into psychological manipulation. | Examples are relevant but partially developed or missing some detail; shows basic understanding of tactics used. | Examples are vague, missing, or irrelevant; table is incomplete or shows minimal effort. |
| **Critical Reflection** | Thoughtful, well-written reflection that critically examines why users are manipulated and offers practical ideas for improvement and personal defense strategies. | General reflection with basic understanding of concepts; lacks depth or specificity. | Missing, too brief, or lacks any critical analysis or connection to content. |

### ****Lab Task 3:**** Social Engineering Awareness & Defense Strategy Design ****(1 Mark)****

This lab requires students to apply their understanding of **phishing**, **baiting**, **impersonation**, and **tailgating** to real-life situations. By analyzing scenarios and designing defense strategies, students will gain insight into the **human vulnerabilities** targeted by attackers and how to respond effectively.

Students will:

* Examine **real-world social engineering cases** or hypotheticals.
* Identify **psychological tactics** used in each case.
* Reflect on how different security awareness or procedural measures could prevent such attacks.
* Propose **awareness-based countermeasures** using behaviorally informed strategies.

#### ****Step 1: Scenario Analysis (Choose ONE Scenario)****

Select one of the following **real-world or hypothetical scenarios**:

1. A university finance officer receives a fake invoice email from a “vendor” and unknowingly transfers $15,000.
2. A USB stick labeled “confidential payroll” is found in a car park and plugged into a HR workstation.
3. A stranger follows a staff member into a secure building by pretending to be a delivery courier.
4. An employee receives a spear phishing email mimicking the CEO’s tone requesting login credentials.

#### ****Step 2: Complete the Table Below****

|  |  |
| --- | --- |
| ****Aspect**** | ****Your Response**** |
| Type of Social Engineering | (e.g., phishing, baiting, etc.) |
| Psychological Triggers Used | (e.g., urgency, curiosity, authority bias) |
| Attack Vector | (e.g., email, USB, physical access) |
| Targeted Individual Role | (e.g., HR staff, IT technician) |
| Potential Impact | (financial, reputational, operational) |
| Missed Safeguards | (what was lacking?) |
| Recommended Awareness Measures | (e.g., phishing drills, posters, simulations) |

#### ****Step 3: Short Reflection (150–200 Words)****

In your own words, answer the following:

* What psychological vulnerability made this attack effective?
* How could this incident have been prevented through awareness or behavior change?
* Why is it important to address human factors alongside technical controls?

### ✅ ****Marking Guide – Lab Task 3 (1 Mark Total)****

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Weight** | **High (Full Mark)** | **Medium (0.5)** | **Low/None (0)** |
| **Scenario Analysis Table** | 0.5 | All fields completed with relevant, specific analysis | Most fields completed with some relevance | Incomplete, missing fields or vague answers |
| **Reflection Quality (150–200 words)** | 0.4 | Clear, critical reflection with relevant insights | Some reflection and insights, but lacks depth | Minimal or no reflection; lacks relevance |
| **Presentation & Clarity (Spelling, Formatting, Clarity)** | 0.1 | Professionally presented, well-structured, easy to read | Some errors, minor issues in structure or clarity | Poor formatting, difficult to read or disorganized |

## Lab Submission Guidelines

1. Students might use AI tools. However, they must have to demonstrate their understanding of contents through oral questions or presentation.
2. All students are required to submit their completed **Week 3 Lab** tasks via **Moodle** by **Sunday, 10 August 2025** 23:59 (local time). Late submissions are not accepted.
3. Navigate to **Week 3 > Active Learning** in Moodle to access the submission link.