UNIT - 1 NOTES

Ethics of Ethical Hacking

What is Ethical Hacking?

Ethical hacking means legally testing computers, networks, or websites to find security problems before real hackers can attack them.

An ethical hacker works with permission and helps improve cyber security.

Example:
A company hires a hacker to test its website security. The hacker finds weaknesses and reports them instead of stealing data.

Ethics of Ethical Hacking

Ethics means the rules and moral values an ethical hacker must follow while doing hacking activities.

Main Ethical Rules

1. Take Permission First

An ethical hacker must always get official permission before testing any system.

Without permission, hacking becomes illegal.

---

2. Protect Privacy

Ethical hackers should never misuse personal or confidential information.

They must keep user data safe and secret.

---

3. Do Not Damage Systems

The goal is to identify problems, not to destroy files, crash servers, or harm networks.

---

4. Report Vulnerabilities Honestly

After testing, ethical hackers should clearly report all security weaknesses to the organization.

They should not hide or misuse vulnerabilities.

---

5. Follow Laws and Rules

Ethical hackers must obey cyber laws, company policies, and security regulations.

---

6. Maintain Confidentiality

Sensitive information discovered during testing should never be shared with unauthorized people.

---

7. Use Skills for Good Purpose

Ethical hacking knowledge should be used to protect systems, not for cybercrime or illegal activities.

Importance of Ethics in Ethical Hacking

- Protects organizations from cyber attacks
- Builds trust between companies and hackers
- Prevents misuse of hacking skills
- Helps maintain privacy and security
- Supports legal and responsible cyber security practices

VULNERABILITY ASSESSMENT AND PENETRATION TESTING(23CY701)

ETHICS OF ETHICAL HACKING

HACK RESPONSIBLY. PROTECT EVERYONE.

WHAT IS ETHICAL HACKING?

Ethical hacking means legally testing computers, networks, or websites to find security problems before real hackers can attack them.

An ethical hacker works with permission and helps improve cyber security.

EXAMPLE:

A company hires a hacker to test its website security. The hacker finds weaknesses and reports them instead of stealing data.

ETHICS OF ETHICAL HACKING

Ethics means the rules and moral values an ethical hacker must follow while doing hacking activities.

1	TAKE PERMISSION FIRST	An ethical hacker must always get official permission before testing any system. Without permission, hacking becomes illegal.
2	PROTECT PRIVACY	Ethical hackers should never misuse personal or confidential information. They must keep user data safe and secret.
3	DO NOT DAMAGE SYSTEMS	The goal is to identify problems, not to destroy files, crash servers, or harm networks.
4	REPORT VULNERABILITIES HONESTLY	After testing, ethical hackers should clearly report all security weaknesses to the organization. They should not hide or misuse vulnerabilities.
5	FOLLOW LAWS AND RULES	Ethical hackers must obey cyber laws, company policies, and security regulations.
6	MAINTAIN CONFIDENTIALITY	Sensitive information discovered during testing should never be shared with unauthorized people.
7	USE SKILLS FOR GOOD PURPOSE	Ethical hacking knowledge should be used to protect systems, not for cybercrime or illegal activities.

ETHICAL HACKER vs MALICIOUS HACKER

ETHICAL HACKER	VS	MALICIOUS HACKER
Works legally		Works illegally
Takes permission		No permission
Protects systems		Damages systems
Reports vulnerabilities		Exploits vulnerabilities
Follows ethics		Breaks laws

IMPORTANCE OF ETHICS IN ETHICAL HACKING

- Protects organizations from cyber attacks
- Builds trust between companies and hackers
- Prevents misuse of hacking skills
- Helps maintain privacy and security
- Supports legal and responsible cyber security practices

SIMPLE CONCLUSION

Ethical hacking is useful only when it is done legally, responsibly, and honestly.
Ethical hackers use their knowledge to improve security and protect people from cyber threats.

Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing.

In cyber security, defenders must think like attackers to protect systems properly. Ethical hackers and security professionals study hacker techniques to understand how cyber attacks happen.

Reasons to Understand Hacker Tactics

1. Identify Weaknesses Before Attackers Do

By understanding hacking methods, organizations can discover vulnerabilities early and fix them before criminals exploit them.

Example:
If a hacker commonly uses phishing emails, companies can train employees to recognize fake messages.

---

2. Improve Security Defenses

Knowing attacker strategies helps build stronger firewalls, authentication systems, and monitoring tools.

Security teams can prepare defenses against:

- Malware attacks
- Phishing
- Password attacks
- Network intrusions
- Social engineering

---

3. Predict Future Attacks

Hackers constantly change their methods. Studying their behavior helps organizations stay prepared for new cyber threats.

---

4. Perform Better Penetration Testing

Ethical hackers simulate real-world attacks during penetration testing. Understanding enemy tactics makes testing more realistic and effective.

Recognizing the Gray Areas in Security

Not everything in cyber security is completely right or wrong. Some situations fall into "gray areas," where ethical and legal decisions become difficult.

Examples of Gray Areas

1. Unauthorized Testing

A person may test a system to "help" find vulnerabilities but without permission. Even with good intentions, this can still be illegal.

---

2. Disclosure of Vulnerabilities

If a researcher finds a security flaw:

- Should they tell the company privately?
- Should they publish it publicly?
- What if the company ignores the issue?

These situations create ethical dilemmas.

---

3. Dual Use of Hacking Tools

Many tools used by ethical hackers can also be used by cybercriminals.

Example:
Password cracking tools help:

- Ethical hackers test password strength
- Attackers steal accounts

The tool itself is not illegal; how it is used matters.

Vulnerability Assessment and Penetration Testing (VAPT)

What is Vulnerability Assessment?

Vulnerability Assessment is the process of scanning systems to identify security weaknesses.

It answers:
"What vulnerabilities exist?"

Features

- Finds known weaknesses
- Uses automated tools
- Focuses on detection
- Lower risk

What is Penetration Testing?

Penetration Testing is the process of actively exploiting vulnerabilities to test how dangerous they are.

It answers:
"How much damage can an attacker do?"

Features

- Simulates real attacks
- Tests security defenses
- Requires skilled ethical hackers
- More practical and realistic

NARSIMHA REDDY ENGINEERING COLLEGE

NRCM
your roots to success.
Estd.2007

An Autonomous Institution| Affiliated to JNTUH | Approved by AICTE
Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING(23CY701)

WHY YOU NEED TO UNDERSTAND YOUR ENEMY'S TACTICS

In cyber security, defenders must think like attackers to protect systems properly. Ethical hackers and security professionals study hacker techniques to understand how cyber attacks happen.

1 IDENTIFY WEAKNESSES BEFORE ATTACKERS DO

Understand hacking methods to discover vulnerabilities early and fix them before criminals exploit them.

EXAMPLE:
If a hacker commonly uses phishing emails, companies can train employees to recognize fake messages.

2 IMPROVE SECURITY DEFENSES

Knowing attacker strategies helps build stronger defenses and security controls.

Prepare defenses against:
- Malware attacks
- Phishing
- Password attacks
- Network intrusions
- Social engineering

3 PREDICT FUTURE ATTACKS

Hackers constantly change their methods. Studying their behavior helps organizations stay prepared for new cyber threats.

4 PERFORM BETTER PENETRATION TESTING

Ethical hackers simulate real-world attacks during penetration testing. Understanding enemy tactics makes testing more realistic and effective.

RECOGNIZING THE GRAY AREAS IN SECURITY

Not everything in cyber security is completely right or wrong. Some situations fall into "gray areas," where ethical and legal decisions become difficult.

1 UNAUTHORIZED TESTING

A person may test a system to "help" find vulnerabilities but without permission. Even with good intentions, this can still be illegal.

2 DISCLOSURE OF VULNERABILITIES

If a researcher finds a security flaw:
- Should they tell the company privately?
- Should they publish it publicly?
- What if the company ignores the issue?

These situations create ethical dilemmas.

3 DUAL USE OF HACKING TOOLS

Many tools used by ethical hackers can also be used by cybercriminals.

EXAMPLE:
Password cracking tools help:
✓ Ethical hackers test password strength
✗ Attackers steal accounts

The tool itself is not illegal; how it is used matters.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

WHAT IS VULNERABILITY ASSESSMENT?

Vulnerability Assessment is the process of scanning systems to identify security weaknesses.

It answers: "What vulnerabilities exist?"

FEATURES
- Finds known weaknesses
- Uses automated tools
- Focuses on detection
- Lower risk

VS

WHAT IS PENETRATION TESTING?

Penetration Testing is the process of actively exploiting vulnerabilities to test how dangerous they are.

It answers: "How much damage can an attacker do?"

FEATURES
- Simulates real attacks
- Tests security defenses
- Requires skilled ethical hackers
- More practical and realistic

DIFFERENCE BETWEEN VULNERABILITY ASSESSMENT AND PENETRATION TESTING

VULNERABILITY ASSESSMENT	ASPECT	PENETRATION TESTING
Identifies weaknesses	GOAL	Exploits weaknesses
Mostly automated	APPROACH	Mostly manual
Detection focused	FOCUS	Attack simulation focused
Lower risk	RISK LEVEL	Higher controlled risk
Provides vulnerability list	OUTPUT	Shows real-world impact

IMPORTANCE OF VAPT

- Improves cyber security
- Protects sensitive information
- Prevents cyber attacks
- Helps organizations meet security standards
- Builds trust with customers and users

SIMPLE CONCLUSION

Understanding hacker tactics helps security professionals protect systems more effectively.

Ethical hacking requires balancing legal, ethical, and technical responsibilities.

Vulnerability Assessment and Penetration Testing are important methods used to identify and reduce cyber security risks before attackers can exploit them.

Penetration Testing and Tools:

Social Engineering Attacks:

What is Social Engineering?

Social Engineering is a trick used by hackers to fool people into giving:

- Passwords
- Bank details
- Personal information
- Access to systems or devices

Instead of hacking computers directly, attackers **hack human emotions** like:

- Trust
- Fear
- Curiosity
- Urgency

Common Types of Social Engineering Attacks

1. Phishing

Fake emails or messages pretending to be from banks, companies, or trusted people.

Example:

You receive:

> "Your bank account will be blocked. Click here immediately."

You click the link and enter your password.
The attacker steals it.

2. Vishing (Voice Phishing)

Attackers call people pretending to be:

- Bank officers
- Police
- Technical support

Example:

"Your ATM card is blocked. Tell us the OTP."

They steal money using the OTP.

---

3. Smishing (SMS Phishing)

Fake SMS messages with malicious links.

Example:

"You won ₹50,000! Click this link to claim."

---

4. Pretexting

The attacker creates a fake story to gain trust.

Example:

Someone pretends to be an IT employee and asks:

"We need your password to update the system."

---

5. Baiting

Attackers offer something attractive to trap victims.

Example:

A USB drive labeled:

"Salary Details"

Someone plugs it into the office computer, and malware installs automatically.

6. Tailgating

Unauthorized people enter secure places by following authorized employees.

Example:

An attacker says:

"I forgot my ID card. Please open the door."

Why Social Engineering is Dangerous

- Humans are easier to trick than computers
- No advanced hacking skills needed
- Can cause:
  - Data theft
  - Financial loss
  - Identity theft
  - System compromise

How to Protect Yourself

✅ Never share passwords or OTPs
✅ Verify emails and phone calls
✅ Avoid clicking unknown links
✅ Use two-factor authentication (2FA)
✅ Think before trusting urgent messages
✅ Keep software updated

SOCIAL ENGINEERING ATTACKS
IN SIMPLE LANGUAGE

Social Engineering is a trick used by attackers to fool people into giving away sensitive information or access to systems.

Attackers don't hack computers, they hack human emotions.

TRUST | FEAR | CURIOSITY | URGENCY

COMMON TYPES OF SOCIAL ENGINEERING ATTACKS

1 PHISHING
Fake emails or messages that look real, sent to steal your information.

Example:
You receive an email saying "Your account will be blocked. Click here immediately." You click the link and enter your password. The attacker steals it.

2 VISHING (VOICE PHISHING)
Attackers call you pretending to be from a trusted organization.

Example:
They call and say your card is blocked and ask for OTP or card details. They use it to steal money.

3 SMISHING (SMS PHISHING)
Fake SMS messages with malicious links.

Example:
You get a message saying you won a prize. You click the link and your personal information is stolen.

4 PRETEXTING
The attacker creates a fake story to gain your trust and information.

Example:
Someone pretends to be an IT employee and asks for your password or access.

5 BAITING
Offering something attractive to lure you into a trap.

Example:
You find a USB drive labeled "Salary Details". You plug it in and malware installs automatically.

6 TAILGATING
Gaining unauthorized access to restricted areas by following authorized people.

Example:
An attacker follows you into a secure area like office or server room.

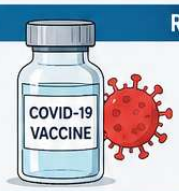
WHY IS IT DANGEROUS?

- Humans are easier to trick than computers.
- No advanced hacking skills needed.
- Can cause:
  - Data theft
  - Financial loss
  - Identity theft
  - System compromise

HOW TO PROTECT YOURSELF

- Never share passwords or OTPs.
- Verify emails, SMS, and phone calls.
- Avoid clicking on unknown links or attachments.
- Use two-factor authentication (2FA).
- Think before you trust urgent requests.
- Keep your software and devices updated.

REAL-LIFE EXAMPLE



During the COVID-19 pandemic, attackers sent fake vaccine and health-related emails and SMS pretending to be from health organizations to steal personal information and money.

ONE-LINE CONCLUSION

"Social engineering attacks target human psychology rather than technology.

BE AWARE. BE CAUTIOUS. THINK BEFORE YOU CLICK, SHARE OR TRUST.

How a Social Engineering Attack Works

A social engineering attack usually follows a simple step-by-step process where attackers manipulate human behavior instead of hacking technology directly.

Step-by-Step Process

1. Information Gathering

The attacker collects information about the victim from:

- Social media
- Emails
- Websites
- Phone numbers
- Company details

Example:

The attacker learns your:

- Name
- Workplace
- Friends
- Email address

2. Building Trust

The attacker pretends to be someone trusted such as:

- Bank employee
- IT support
- Police officer
- Friend or colleague

Goal:

Make the victim feel safe and trust the attacker.

Example:

"Hello, I am calling from your bank security team."

3. Creating Urgency or Fear

Attackers pressure victims emotionally using:

- Fear
- Panic
- Excitement
- Curiosity

Example:

"Your account will be blocked in 10 minutes!"

This makes people act quickly without thinking.

4. Victim Takes Action

The victim may:

- Click a fake link
- Share passwords
- Reveal OTPs
- Download malware
- Open infected attachments

Example:

The victim enters login details on a fake website.

5. Attacker Gains Access

Now the attacker can:

- Steal money
- Access accounts
- Hack systems
- Steal confidential data

NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution| Affiliated to JNTUH | Approved by AICTE

Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING(23CY701)

HOW A SOCIAL ENGINEERING ATTACK WORKS

Attackers don't hack systems, they hack people.

STEP	WHAT HAPPENS?	EXAMPLE	ATTACKER'S GOAL
1 INFORMATION GATHERING	The attacker collects information about the victim from various sources. • Social media • Websites • Emails • Phone numbers • Company details	The attacker learns your: ✓ Name ✓ Workplace ✓ Friends ✓ Email address ✓ Phone number	Collect enough details to make the attack convincing and personalized.
2 BUILDING TRUST	The attacker pretends to be someone you trust. • Bank employee • IT support • Police officer • Friend or colleague • Company representative	They use details collected about you to sound real and believable.	Gain your trust so you let your guard down.
3 CREATING URGENCY OR FEAR	The attacker pressures you emotionally so you act quickly without thinking. • Fear • Panic • Excitement • Curiosity	Examples of messages: "Your account is locked. Verify now!" "Unusual activity detected. Confirm your details." "You won a prize! Click now to claim."	Make you feel pressured so you don't think clearly.
4 VICTIM TAKES ACTION	The victim follows the attacker's instructions. • Clicks a fake link • Shares passwords • Reveals OTPs • Downloads malware • Opens infected attachments	The victim enters login details on a fake website or shares an OTP.	Get you to share sensitive information or perform a dangerous action.
5 ATTACKER GAINS ACCESS	Now the attacker can misuse the stolen information. • Steal money • Access accounts • Hack systems • Steal confidential data • Commit identity theft	The attacker logs in to your account and changes your password, or makes unauthorized transactions.	Use the access to steal, damage, or commit fraud for profit.

THE ENTIRE PROCESS IN A SIMPLE FLOW

1. Collect Information → 2. Build Trust → 3. Create Fear / Urgency → 4. Victim Makes Mistake → 5. Attacker Steals Data or Gains Access

REAL-LIFE EXAMPLE

A scammer sends an email pretending to be from Google:

"Your Gmail account is hacked. Reset password now."

The victim clicks the fake link, enters the password, and the attacker steals the account.

Google

Your account has been disabled.

Please verify your account immediately.

RESET PASSWORD

FAKE

WHY IT WORKS?

- Humans are naturally trusting
- We fear problems and act fast
- We want to help
- We are curious about offers
- Attackers use our emotions against us

STAY ALERT!

- ✓ Verify before you trust.
- ✓ Never share passwords or OTPs.
- ✓ Don't click on unknown links.
- ✓ Check sender's email carefully.
- ✓ Report suspicious messages.

THINK. VERIFY. PROTECT. Your awareness is your best defense against social engineering attacks.

Conducting a Social Engineering Attack

Social Engineering Attack Lifecycle (For Awareness)

1. Reconnaissance
   Collecting publicly available information about targets.
2. Trust Building
   Pretending to be a trusted person or service.
3. Manipulation
   Creating urgency, fear, or curiosity.
4. Exploitation
   Getting the victim to reveal information or perform an action.
5. Exit/Cover Tracks
   Using stolen access while avoiding detection.

Defensive Measures

- Security awareness training
- Multi-factor authentication (MFA)
- Verification procedures
- Email filtering
- Incident reporting systems
- Zero-trust access policies

Common Types Used in Security Training

- Phishing emails
- Vishing calls
- Smishing texts
- USB baiting
- Tailgating simulations

VULNERABILITY ASSESSMENT AND PENETRATION TESTING(23CY701)

CONDUCTING A SOCIAL ENGINEERING ATTACK

Attackers don't break in through the system, they walk in through you.

THE SOCIAL ENGINEERING ATTACK LIFECYCLE

1 RECONNAISSANCE
The attacker collects information about the target from publicly available sources.

- Social media profiles
- Company websites
- News & press releases
- Employee directory
- Public documents

GOAL Gather as much information as possible to create a convincing approach.

2 BUILD TRUST
The attacker poses as someone trustworthy to establish a connection.

- Use of real names & details
- Professional tone & appearance
- Impersonating a trusted person or organization

GOAL Gain the victim's trust and lower their guard.

3 MANIPULATION
The attacker uses psychological triggers to influence the victim to act quickly.

- Create urgency or fear
- Offer something attractive
- Appeal to curiosity
- Use authority or pressure

GOAL Manipulate emotions to bypass rational thinking.

4 EXPLOITATION
The victim is tricked into revealing information or performing an action.

- Clicking malicious links
- Sharing passwords / OTPs
- Downloading malware
- Providing confidential data
- Authorizing payments

GOAL Obtain the information or access needed.

5 EXIT / COVER TRACKS
The attacker uses the access silently and tries to avoid detection.

- Maintain access
- Escalate privileges
- Cover tracks & logs
- Monetize or cause damage

GOAL Achieve the objective without being detected.

COMMON SOCIAL ENGINEERING ATTACKS

PHISHING


Fake emails designed to steal credentials or sensitive information.

Example: "Your account will be suspended. Click here to verify."

VISHING (VOICE PHISHING)


Fraudulent phone calls pretending to be from trusted organizations.

Example: "This is your bank. Please share the OTP to secure your account."

SMISHING (SMS PHISHING)


Malicious SMS or messages with fake links.

Example: "Click here to claim your reward!"

BAITING


Offering something attractive to lure victims (e.g., free downloads, USB drives).

Example: A USB labeled "Salary Details" contains malware.

PRETEXTING


Creating a fabricated scenario to obtain information.

Example: "IT team needs your password to fix an issue."

TAILGATING


Following an authorized person into a restricted area.

Example: "Sorry, I forgot my ID card."

RED FLAGS – BE ALERT!

- Unexpected or unusual requests
- Urgent or threatening language
- Requests for passwords or OTPs
- Poor grammar or suspicious links
- Too good to be true offers
- Pressure to act immediately

HOW TO PROTECT YOURSELF

- Verify before you trust – independently confirm requests.
- Never share passwords, OTPs, or sensitive data.
- Hover over links before clicking.
- Use multi-factor authentication (MFA).
- Keep software and systems updated.
- Report suspicious messages or activities.
- Stay informed and attend security awareness training.

IMPACT OF SUCCESSFUL ATTACKS

- Financial loss
- Data breaches
- Reputation damage
- Identity theft
- Operational disruption

REAL-LIFE EXAMPLE

A company employee received an email appearing to be from the CEO, requesting an urgent wire transfer to a vendor. The employee, trusting the request, transferred $100,000. It was later discovered that the email was from an attacker who had spoofed the CEO's email.

KEY TAKEAWAY

"Technology can have all the defenses, but a single human mistake can open the door."

THINK. VERIFY. PROTECT. | AWARENESS TODAY, SECURITY TOMORROW.

Common Attacks Used in Penetration Testing

Penetration testing (ethical hacking) uses controlled and authorized techniques to identify security weaknesses before real attackers can exploit them.

---

1. Phishing Simulation

Security testers send fake emails to check whether users:

- Click malicious links
- Share passwords
- Download unsafe files

Goal:

Test employee awareness and email security.

2. Password Attacks

Testing weak passwords using:

- Brute force
- Dictionary attacks
- Password spraying

Goal:

Find weak or reused passwords.

3. SQL Injection (SQLi)

Attackers insert malicious SQL queries into login forms or websites.

Example:

Trying to bypass login authentication.

Goal:

Access or steal database information.

4. Cross-Site Scripting (XSS)

Injecting malicious scripts into websites.

Goal:

Steal cookies, sessions, or user data.

5. Network Scanning

Using tools to discover:

- Open ports
- Active devices
- Vulnerable services

Common Tool:

Nmap

6. Man-in-the-Middle (MITM)

Testing whether attackers can intercept communication between two systems.

Goal:

Check network encryption and security.

7. Malware Simulation

Security professionals safely simulate malware behavior to test defenses.

Goal:

Evaluate antivirus and monitoring systems.

8. Social Engineering Tests

Authorized testing of human awareness through:

- Fake calls
- Fake emails
- USB baiting

Goal:

Measure employee security awareness.

9. Wireless Attacks

Testing Wi-Fi security such as:

- Weak passwords
- Rogue access points
- Weak encryption

10. Privilege Escalation

Checking whether a low-level user can gain administrator access.

Goal:

Identify improper permissions.

Common Penetration Testing Tools

- Metasploit
- Wireshark
- Burp Suite

NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution| Affiliated to JNTUH | Approved by AICTE
Accredited by NBA & NAAC with 'A' Grade

NRCM
your roots to success.
Estd.2007

VULNERABILITY ASSESSMENT AND PENETRATION TESTING(23CY701)

- Nmap
- John the Ripper

Preparing Yourself for Face-to-Face Social Engineering Attacks

Face-to-face social engineering attacks happen when attackers physically interact with people to gain:

- Information
- Building access
- Passwords
- Trust

These attacks often occur in:

- Offices
- Colleges
- Banks
- Hospitals
- Public places

Step 1: Stay Aware of Your Surroundings

Always observe:

- Unknown visitors
- Suspicious behavior
- People without ID cards
- Unusual questions

Why?

Attackers often look confident and act normal to avoid suspicion.

Example:

Someone wandering around office areas pretending to be staff.

Step 2: Verify Identity Properly

Never trust someone only because:

- They wear formal clothes
- They speak confidently
- They know company names

What to Do:

✓ Ask for:

- ID card
- Authorization
- Employee verification

Example:

A fake technician says:

"I' m from IT support."

Verify with the actual IT department first.

Step 3: Do Not Share Sensitive Information

Never share:

- Passwords
- OTPs
- Access cards
- Internal information

Even if the person seems urgent or friendly.

Example:

"Please tell me the Wi-Fi password quickly."

Step 4: Be Careful with Tailgating

Tailgating means an unauthorized person follows you into a restricted area.

What to Do:

✅ Ensure everyone uses their own access card.

❌ Do not hold doors open for unknown people.

Step 5: Watch for Emotional Manipulation

Attackers may use:

- Fear
- Sympathy
- Urgency
- Authority

Example:

"Please help me quickly, my boss is waiting."

What to Do:

Pause and verify before helping.

Step 6: Protect Devices and Documents

Never leave:

- Laptops unlocked
- ID cards unattended
- Confidential files open

Why?

Attackers can quickly photograph or steal information.

Step 7: Report Suspicious Activity

Inform:

- Security team
- IT department
- Management

Report if someone:

- Asks unusual questions
- Tries entering restricted areas
- Behaves suspiciously

Step 8: Attend Security Awareness Training

Learn about:

- Common attack techniques
- Scam behavior
- Verification methods
- Emergency procedures

Goal:

Build confidence in recognizing threats.

PREPARING YOURSELF FOR FACE-TO-FACE ATTACKS

Simple steps to stay safe from face-to-face social engineering attacks.

1 STAY AWARE OF YOUR SURROUNDINGS

- Observe unknown visitors and suspicious behavior.
- Notice people without ID cards.
- Be alert to unusual questions.

Example:
Someone wandering around office areas pretending to be staff.

2 VERIFY IDENTITY PROPERLY

What to do:
- ✓ Ask for ID card.
- ✓ Check authorization.
- ✓ Verify with the department.

Example:
A fake technician says, "I'm from IT support." Verify with the IT department.

3 DO NOT SHARE SENSITIVE INFORMATION

Never share:
- Passwords
- OTPs
- Access cards
- Internal information

Even if the person seems urgent or friendly.

Example:
"Please tell me the Wi-Fi password quickly."

4 BE CAREFUL WITH TAILGATING

- Tailgating means an unauthorized person follows you into a restricted area.
- Ensure everyone uses their own access card.
- Do not hold doors open for unknown people.

5 WATCH FOR EMOTIONAL MANIPULATION

Attackers may use:
- Fear
- Sympathy
- Urgency
- Authority

Pause and verify before helping.

6 PROTECT DEVICES AND DOCUMENTS

Never leave:
- Laptops unlocked
- ID cards unattended
- Confidential files open

Attackers can quickly photograph or steal information.

7 REPORT SUSPICIOUS ACTIVITY

Report if someone:
- Asks unusual questions
- Tries entering restricted areas
- Behaves suspiciously

8 ATTEND SECURITY AWARENESS TRAINING

Learn about:
- Common attack techniques
- Scam behavior
- Verification methods
- Emergency procedures

Build confidence in recognizing threats.

COMMON FACE-TO-FACE ATTACK METHODS

TAILGATING	IMPERSONATION	SHOULDER SURFING	DUMPSTER DIVING	BAITING
				
Following authorized people into secure areas.	Pretending to be staff, technician or someone authorized.	Watching your screen or password while you type.	Searching thrown away documents for sensitive info.	Leaving infected USB drives or items to lure victims.

QUICK SAFETY CHECKLIST

- ✓ Verify identities
- ✓ Protect passwords
- ✓ Lock devices
- ✓ Question unusual requests
- ✓ Follow company security rules
- ✓ Report suspicious people

ONE-LINE CONCLUSION: Awareness, verification, and caution are the best defenses against face-to-face social engineering attacks.

Defending Against Social Engineering Attacks

Social engineering attacks target human behavior instead of technology.
The best defense is awareness, verification, and safe security practices.

1. Verify Before Trusting

Always confirm:

- Emails
- Phone calls
- Messages
- Visitors

Example:

If someone claims to be from IT support, verify with the actual department first.

2. Never Share Passwords or OTPs

Do not share:

- Passwords
- OTPs
- PINs
- Access credentials

Even trusted organizations usually never ask for them directly.

3. Be Careful with Emails and Links

Avoid:

- Unknown attachments
- Suspicious links
- Urgent messages

Check for:

- Fake email addresses
- Spelling mistakes
- Unusual requests

4. Use Multi-Factor Authentication (MFA)

MFA adds extra security by requiring:

- Password + OTP
- Password + biometric verification

Benefit:

Even if a password is stolen, attackers may still be blocked.

5. Protect Personal Information

Do not overshare information on:

- Social media
- Public websites
- Online profiles

Attackers use personal details to build trust.

6. Stay Alert for Emotional Manipulation

Attackers often use:

- Fear
- Urgency
- Curiosity

- Sympathy

Example:

"Your account will be blocked immediately!"

Pause and verify before acting.

7. Keep Software Updated

Update:

- Operating systems
- Antivirus software
- Browsers
- Applications

Why?

Updates fix security vulnerabilities.

8. Lock Devices and Secure Documents

Always:

- Lock computers when away
- Protect ID cards
- Secure confidential files

9. Attend Security Awareness Training

Learn about:

- Phishing attacks
- Fake calls
- Scam techniques
- Security best practices

Training improves threat recognition.

10. Report Suspicious Activity Immediately

Report:

- Suspicious emails
- Unknown visitors
- Unusual requests
- Fake calls

Quick reporting helps stop attacks early.

NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution| Affiliated to JNTUH | Approved by AICTE

Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING(23CY701)

DEFENDING AGAINST SOCIAL ENGINEERING ATTACKS

Attackers trick people, not technology.
Stay aware. Verify. Protect. Report.

1 VERIFY BEFORE TRUSTING

Always verify the identity of people or organizations before sharing information or taking any action.

Example: If someone claims to be from IT support, verify with the official department first.

2 NEVER SHARE PASSWORDS OR OTPS

Do not share your passwords, OTPs, PINs or any access credentials with anyone.

Remember: Legitimate organizations never ask for your passwords or OTPs.

3 BE CAREFUL WITH EMAILS AND LINKS

Avoid unknown attachments, suspicious links and urgent or unusual requests.

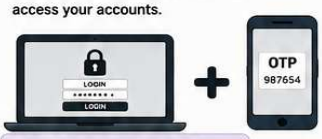
Check for:

- Fake email addresses
- Spelling mistakes
- Unusual requests

When in doubt, don't click. Verify first.

4 USE MULTI-FACTOR AUTHENTICATION (MFA)

MFA adds an extra layer of security. It makes it harder for attackers to access your accounts.



Even if your password is stolen, MFA can still stop attackers.

5 PROTECT PERSONAL INFORMATION

Do not overshare personal details on social media or public websites.

Attackers use your personal information to build trust and trick you.

6 STAY ALERT FOR EMOTIONAL MANIPULATION

Attackers use emotions like fear, urgency, curiosity or sympathy to trick you.

Stay calm. Pause. Verify before you act.

7 KEEP SOFTWARE UPDATED

Regularly update your operating system, antivirus, browsers and applications.

Updates fix security flaws and help protect you.

8 LOCK DEVICES AND SECURE DOCUMENTS

Lock your devices when not in use and keep documents and ID cards in a safe place.

Small actions prevent big problems.

9 ATTEND SECURITY AWARENESS TRAINING

Learn about the latest threats, scam techniques and best security practices.

Knowledge is your best defense.

10 REPORT SUSPICIOUS ACTIVITY IMMEDIATELY

Report suspicious emails, calls, visitors or unusual requests to your organization.

Quick reporting helps stop attacks and protects everyone.

QUICK DEFENSE CHECKLIST

- Verify identities
- Protect passwords and OTPs
- Use multi-factor authentication
- Avoid suspicious links and emails
- Keep systems updated
- Lock devices and secure information
- Report suspicious behavior

AWARENESS. CAUTION. VERIFICATION.

STAY SAFE, STAY SECURE!

ONE-LINE CONCLUSION:

Awareness, caution and verification are the strongest defenses against social engineering attacks.

Be Aware | Verify Always | Protect Yourself | Report Immediately