



DAY 3

Threat Types: Malware, Phishing, Social Engineering & Insider Threats

Knowing the enemy

Cybersecurity Track · Week 1
Figure Academy Learner Portal

STUDENT COPY

1. Learning Objectives

By the end of this session, you should be able to distinguish between the major categories of cyber threats, recognize common attack techniques within each category, and connect each threat type back to the CIA triad pillar it most directly endangers.

2. Malware

Malware, short for malicious software, is any program designed to damage, disrupt, or gain unauthorized access to a system. It remains one of the most common tools attackers use, and it primarily threatens integrity and availability, and often confidentiality as well.

Common malware types

- **Virus** — malicious code that attaches itself to a legitimate file or program and spreads when that file is run or shared.
- **Worm** — similar to a virus but self-replicating; it spreads across networks without needing a human to open a file.
- **Trojan** — malware disguised as legitimate software, named for the Trojan Horse; it tricks the user into installing it voluntarily.
- **Ransomware** — encrypts a victim's files and demands payment for the decryption key; a major and growing threat to businesses and hospitals worldwide, covered in depth in Week 6.
- **Spyware** — secretly monitors user activity and harvests data such as keystrokes or login credentials.

3. Phishing

Phishing is a form of social engineering in which an attacker sends fraudulent communications, most often email, that appear to come from a trusted source, in order to steal credentials, deliver malware, or trick the victim into an action such as a wire transfer. It remains, by a wide margin, the most common way attackers gain initial access to a target.

Variants worth knowing

- **Spear phishing** — a highly targeted phishing attempt aimed at a specific individual, often using personal details from social media to make it convincing.
- **Whaling** — spear phishing aimed specifically at senior executives or high-value targets.
- **Business Email Compromise (BEC)** — an attacker impersonates an executive or vendor to trick an employee into wiring funds or sharing sensitive data.
- **Vishing** — voice phishing, conducted over a phone call rather than email.
- **Smishing** — phishing carried out via SMS text message.

Spot the red flags

When you receive a suspicious email, look for: a sender domain that does not match the organization it claims to be, urgency and pressure language ("act now or your account will be closed"), generic greetings ("Dear customer"), and links whose real destination (hover to check) is not what it claims.

4. Social Engineering (Beyond Phishing)

Social engineering is the broader category of manipulating people, rather than machines, into breaking normal security procedures. Phishing is the most common form, but there are others you should recognize.

- **Pretexting** — the attacker invents a fabricated scenario (a pretext) to convince the target to hand over information, for example impersonating IT support to "verify" a password.
- **Baiting** — leaving a malware-infected USB drive somewhere it will be found and plugged in out of curiosity.
- **Tailgating / piggybacking** — physically following an authorized person through a secure door without their own access credentials.

The common thread across all social engineering is that it exploits human psychology, trust, urgency, fear, curiosity, rather than a technical flaw. This is precisely why cybersecurity is as much a people problem as a technology problem.

5. Insider Threats

An insider threat is harm caused by someone who already has legitimate authorized access to an organization's systems, whether that harm is intentional or accidental. Insider threats are uniquely dangerous because traditional perimeter defenses, firewalls, intrusion detection, are built to keep outsiders out, and are far less effective against someone who is already inside.

Categories of insider threat

- **Pawns** — well-meaning employees manipulated into causing harm, often via social engineering or spear phishing.
- **Goofs** — employees who bypass security policy out of convenience, believing the rules do not apply to them.
- **Collaborators** — insiders who knowingly work with an external attacker, usually for financial gain.
- **Turncloaks** — insiders who act alone against their employer, whether for personal gain or grievance.

6. Mapping Threats to the CIA Triad

Connecting today's threats back to the CIA triad from Day 2 is exactly the kind of thinking that strong security professionals, and certification exam candidates, need to practice.

- Ransomware primarily attacks availability (data becomes inaccessible), though it may also threaten confidentiality if data is stolen before encryption.
- Phishing that steals login credentials primarily threatens confidentiality, but can lead to integrity or availability damage once the attacker is inside.
- An insider quietly altering financial records is an integrity attack.
- A disgruntled insider deleting critical files on their way out is an availability attack.

7. Questions to Reflect On

- Describe a suspicious message you personally have received. What made it suspicious in hindsight?
- Why do you think phishing remains effective even though awareness of it is now widespread?
- Which insider threat category, pawn, goof, collaborator, or turncloak, do you think is the most common in most organizations, and why?

8. Key Terms Introduced Today

- **Malware, virus, worm, trojan, ransomware, spyware** — categories of malicious software.
- **Phishing, spear phishing, whaling, vishing, smishing** — email, voice, and text-based social engineering attacks.
- **Social engineering** — manipulating people rather than systems to breach security.
- **Insider threat** — harm caused by someone with legitimate authorized access.

9. Looking Ahead

Day 4 shifts from theory to hands-on practice: you will begin building your own cybersecurity home lab using Oracle VirtualBox. This lab will be the sandbox for practical exercises throughout the rest of the course, so a clean, careful setup this week pays off for the next eleven.