**Five common information security threats**

Here are **five common information security threats**, each explained with examples and how they impact individuals or organizations:

**1. Phishing Attacks**

**What it is:**  
Phishing is a type of **social engineering** where attackers impersonate trusted entities (like banks, IT admins, or coworkers) to trick users into revealing sensitive information like passwords, credit card numbers, or login credentials.

**Example:**  
You receive an email that looks like it’s from Microsoft asking you to reset your Office 365 password. Clicking the link leads you to a fake login page that captures your credentials.

**Impact:**

* Credential theft
* Unauthorized access
* Financial loss
* Identity theft

**2. Malware (Malicious Software)**

**What it is:**  
Malware refers to **software designed to harm** or exploit devices, services, or networks. Common types include viruses, worms, trojans, spyware, and ransomware.

**Example:**  
An employee downloads a PDF attachment that contains a hidden trojan. It silently installs and records keystrokes to steal login information.

**Impact:**

* Data corruption or loss
* Device hijacking
* Ransom demands (in case of ransomware)
* Unauthorized surveillance

**3. Denial-of-Service (DoS) / Distributed Denial-of-Service (DDoS)**

**What it is:**  
A DoS/DDoS attack floods a system, server, or network with traffic to **exhaust its resources**, making it **unavailable** to legitimate users.

**Example:**  
A botnet of infected machines sends thousands of requests per second to a company’s e-commerce site, crashing the site during a sales event.

**Impact:**

* Business downtime
* Revenue loss
* Brand reputation damage

**4. Insider Threats**

**What it is:**  
An insider threat comes from **employees, contractors, or partners** who misuse their access, intentionally or accidentally, to harm the organization.

**Example:**  
A disgruntled employee downloads sensitive HR files and leaks them to a competitor.

**Impact:**

* Data breaches
* Legal and compliance issues
* Loss of intellectual property

**5. Man-in-the-Middle (MitM) Attacks**

**What it is:**  
In a MitM attack, the attacker **intercepts and possibly alters communications** between two parties without them knowing.

**Example:**  
Using an unsecured public Wi-Fi, an attacker intercepts the data between your device and your online banking session, capturing login credentials.

**Impact:**

* Credential and session hijacking
* Data manipulation
* Loss of confidentiality

**🔐 Summary Table**

| **Threat Type** | **Attack Method** | **Potential Damage** |
| --- | --- | --- |
| **Phishing** | Deceptive emails/websites | Credential theft, financial fraud |
| **Malware** | Infected files or software | Data loss, surveillance, extortion |
| **DoS/DDoS** | Traffic flooding attacks | Service downtime, revenue loss |
| **Insider Threats** | Misuse of internal access | Data leaks, regulatory fines |
| **Man-in-the-Middle** | Traffic interception | Unauthorized access, data theft |

**🛡️ Common Information Security Threats**

| **Threat** | **How It Works** | **Potential Impact** | **Real-World Example** |
| --- | --- | --- | --- |
| **1. Phishing** | Attackers impersonate legitimate sources (e.g., emails or websites) to trick users into revealing sensitive info like passwords or credit card numbers. | Credential theft, financial loss, identity theft, unauthorized access. | In 2020, Twitter was breached via a phishing attack targeting employees’ credentials. |
| **2. Malware** | Malicious software (e.g., viruses, worms, Trojans) installed on a device to disrupt, spy, or gain control of systems. | System corruption, data theft, financial fraud, ransom demands. | The WannaCry ransomware in 2017 affected 200,000+ computers across 150 countries. |
| **3. DDoS (Distributed Denial of Service)** | Attackers flood a server/network with traffic from multiple sources to make it unavailable. | Service disruption, revenue loss, brand damage. | GitHub was hit by a massive 1.35 Tbps DDoS attack in 2018, temporarily taking it offline. |
| **4. Insider Threats** | A current or former employee misuses access to compromise data, either intentionally or accidentally. | Data leaks, intellectual property theft, reputational harm. | In 2014, a Morgan Stanley employee stole client data and posted it online. |
| **5. SQL Injection** | An attacker injects malicious SQL queries into input fields to manipulate databases and gain unauthorized access. | Data breaches, database corruption, system takeover. | In 2012, LinkedIn suffered a breach (partially through SQLi), exposing 117M user accounts. |