**Key Information Security Controls & Mitigate Common Threats**

Here’s a clear outline of **key information security controls** and how they mitigate the **common threats** we discussed earlier (phishing, malware, DoS, insider threats, MitM):

**🔐 Information Security Controls & Corresponding Threat Mitigation**

| **Security Threat** | **Security Controls** | **How It Mitigates the Threat** |
| --- | --- | --- |
| **1. Phishing Attacks** | - Email filtering (e.g., **Microsoft Defender for 365**)- User awareness training- Multi-Factor Authentication (**MFA**)- Domain-based Message Authentication (**DMARC/DKIM/SPF**) | Filters phishing emails, educates users, and ensures compromised credentials alone aren't enough. |
| **2. Malware Infections** | - Endpoint Detection & Response (EDR)- Antivirus/anti-malware software- Application whitelisting- Network segmentation- Secure email/file scanning | Detects and blocks malicious files and behaviour before execution or spreading. |
| **3. Denial-of-Service (DoS)** | - **Web Application Firewall (WAF)-** Rate limiting- **Load balancing**- Auto-scaling- Cloud CDN (e.g., Cloudflare)- **Network firewall rules** | Prevents overload on services by filtering malicious traffic and distributing legitimate requests. |
| **4. Insider Threats** | - **Role-Based Access Control (RBAC)-** **Least Privilege Principle**- **Activity monitoring (e.g., Microsoft Sentinel)- Data Loss Prevention (DLP)- Segregation of duties** | Limits what insiders can access, and monitors/logs unusual behaviour or data exfiltration. |
| **5. Man-in-the-Middle (MitM)** | - **TLS/SSL encryption- Secure Wi-Fi configurations- VPN usage- Certificate pinning- DNS Security Extensions (DNSSEC)** | Encrypts communications to prevent interception or tampering during transit. |

**🔐 Security Controls and Their Effectiveness**

| **Security Control** | **How It Works** | **Why It’s Effective / What It Mitigates** |
| --- | --- | --- |
| **1. Firewalls** | Monitors and filters incoming/outgoing network traffic based on predefined rules. | Blocks unauthorized traffic and mitigates **malware spread**, **DDoS**, and **intrusions**. |
| **2. Encryption** | Converts sensitive data into unreadable code unless a decryption key is used. | Protects **data confidentiality** during transit and storage, even if intercepted (e.g., by **phishing** or **insiders**). |
| **3. Access Control** | Restricts access to systems or data based on roles (RBAC) or identity verification (MFA). | Prevents **insider threats** and limits damage from compromised accounts (**phishing**). |
| **4. Intrusion Detection and Prevention Systems (IDPS)** | Monitors network/system activity for malicious behaviour and can block or alert on threats. | Detects and responds to **malware**, **SQL injection**, and **unauthorized access attempts** in real time. |
| **5. Web Application Firewalls (WAF)** | Filters and monitors HTTP traffic to and from a web application. | Specifically defends against **SQL injection**, **XSS**, and **other web-based attacks**. |

**✅ Control-to-Threat Mapping Summary**

| **Threat** | **Key Control** | **Mitigated By** |
| --- | --- | --- |
| **Phishing** | Email filtering + MFA | Access Control (MFA), Encryption, IDPS |
| **Malware** | Firewalls, IDPS, Endpoint Security | EDR + Application Whitelisting |
| **DDoS** | Firewalls, Network Load Balancers, Rate Limiting | WAF + Rate Limiting |
| **Insider Threats** | Access Control, Encryption, Monitoring Tools | RBAC + Audit Logs |
| **SQL Injection** | WAF, IDPS, Secure Coding Practices | WAF, IDPS, Secure Coding Practices |
| **Man-in-the-Middle (MITM)** | Encryption, Securing Wi-Fi, keeping software updated | TLS Encryption + VPN, WPA3, MFA |

**🧱 Additional Universal Controls**

| **Control** | **Purpose** |
| --- | --- |
| **Patch Management** | Fixes known vulnerabilities before attackers exploit them |
| **Security Awareness Training** | Reduces human error — the weakest link in most breaches |
| **Security Incident & Event Management (SIEM)** | Provides centralized monitoring, detection, and alerting (e.g., Microsoft Sentinel) |
| **Backups & Recovery Plans** | Helps recover from ransomware, DoS, or accidental deletions |
| **Access Reviews & Audits** | Ensures permissions remain appropriate over time |