Network Security Fundamentals

Week 1: Exploring current cybersecurity threats, network vulnerabilities, attack types, and practical mitigation strategies for IT professionals.

What is Network Security?

Network security protects networks and data from unauthorized access, misuse, disruption, and destruction. Modern threats—phishing, ransomware, DDoS, and supply-chain attacks—exploit trusted services and living-off-trusted-sites techniques.

Confidentiality

Restrict data access to authorized users only

Integrity

Ensure data remains accurate and unaltered

Availability

Keep systems accessible to legitimate users

Top Current Threats

Understanding today's most prevalent attack vectors helps organizations prioritize defenses effectively.

Phishing & Social Engineering

Most security incidents begin with phishing attacks targeting employee credentials and trust.

Ransomware

Highly disruptive attacks encrypting critical data; targets organizations of all sizes and industries.

DDoS Attacks

Record-breaking distributed denial-of-service attacks now exceed 37+ Tbps, causing massive outages.

Supply-Chain Compromises

Attackers exploit trusted third-party services to gain access and hide malicious activity.

Web Application Attacks

SQL injection, cross-site scripting (XSS), and other vulnerabilities expose sensitive databases.

Network Spoofing

ARP and DNS spoofing enable attackers to intercept traffic and redirect users to malicious sites.

Common Network Vulnerabilities

These weaknesses provide attackers initial footholds to gain access, escalate privileges, move laterally, and exfiltrate data.

Weak or Reused Passwords

Lack of multi-factor authentication (MFA) leaves accounts exposed to brute force and credential stuffing.

Unpatched Software & Firmware

Outdated systems contain known vulnerabilities that attackers exploit systematically.

Unsecured Networks

Open Wi-Fi and poorly segmented networks lack proper access controls and traffic isolation.

Misconfigured Firewalls

Poorly managed firewall rules and exposed management services create unnecessary entry points.

Missing Encryption

Data transmitted without TLS or stored without encryption remains readable to attackers.

Phishing & Social Engineering

How It Happens

Attacker sends a convincing email appearing from company HR with a link to a fake login page. User enters credentials, and the attacker gains account access to move laterally through the network.

Business Impact

- Credential theft and account takeover
- Lateral movement within networks
- Data breaches and intellectual property loss
- Regulatory violations and fines

Practical Mitigations

01

User Training & Testing

Run regular security awareness training and conduct simulated phishing tests to measure susceptibility.

02

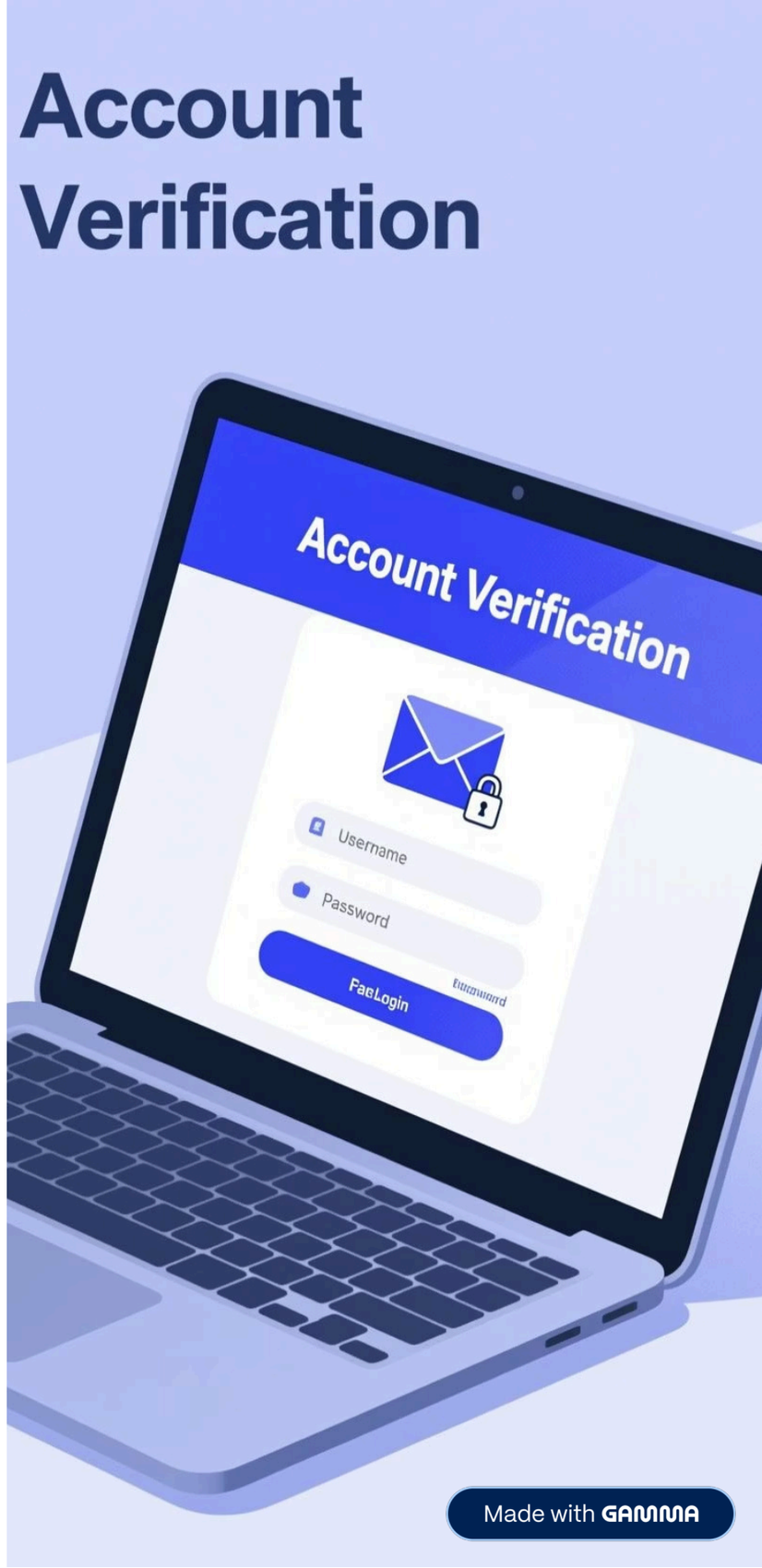
Enforce MFA Everywhere

Require multi-factor authentication (TOTP tokens, hardware keys) on all critical accounts.

03

Email Security

Deploy spam/phishing filters, DMARC/DKIM/SPF authentication, URL rewriting, and risky attachment blocking.



Ransomware Attacks

How It Happens

Initial access through phishing or exposed RDP enables attackers to deploy ransomware across file servers, backups, and critical infrastructure, then demand payment for decryption.

Business Impact

- Encryption of critical business data
- Extended downtime and operational disruption
- Ransom demands and potential data leaks
- Revenue loss and regulatory penalties

Practical Mitigations

01

Offline Backups

Maintain regular, tested offline encrypted backups and immutable snapshots isolated from production networks.

02

Access Controls

Patch systems promptly, reduce exposed RDP ports, and use VPN or zero-trust architecture for management access.

03

Detection & Response

Deploy EDR tools and network segmentation to contain spread; maintain a tested incident response plan.

DDoS & Web Application Attacks

DDoS: Distributed Denial of Service

How: Botnets flood services with massive traffic (37+ Tbps recorded). **Impact:** Outages, revenue loss, distracted defenses. **Mitigate:** Use CDN/DDoS scrubbing services, rate limiting, geo-blocking, and scalable cloud resources.

SQL Injection

How: Attacker injects SQL via form fields (e.g., `' OR '1'='1`) to bypass authentication. **Impact:** Full database compromise and data leaks. **Mitigate:** Use parameterized queries, input validation, WAF rules, and regular code reviews.

Network-Layer Attacks

Man-in-the-Middle (MitM)

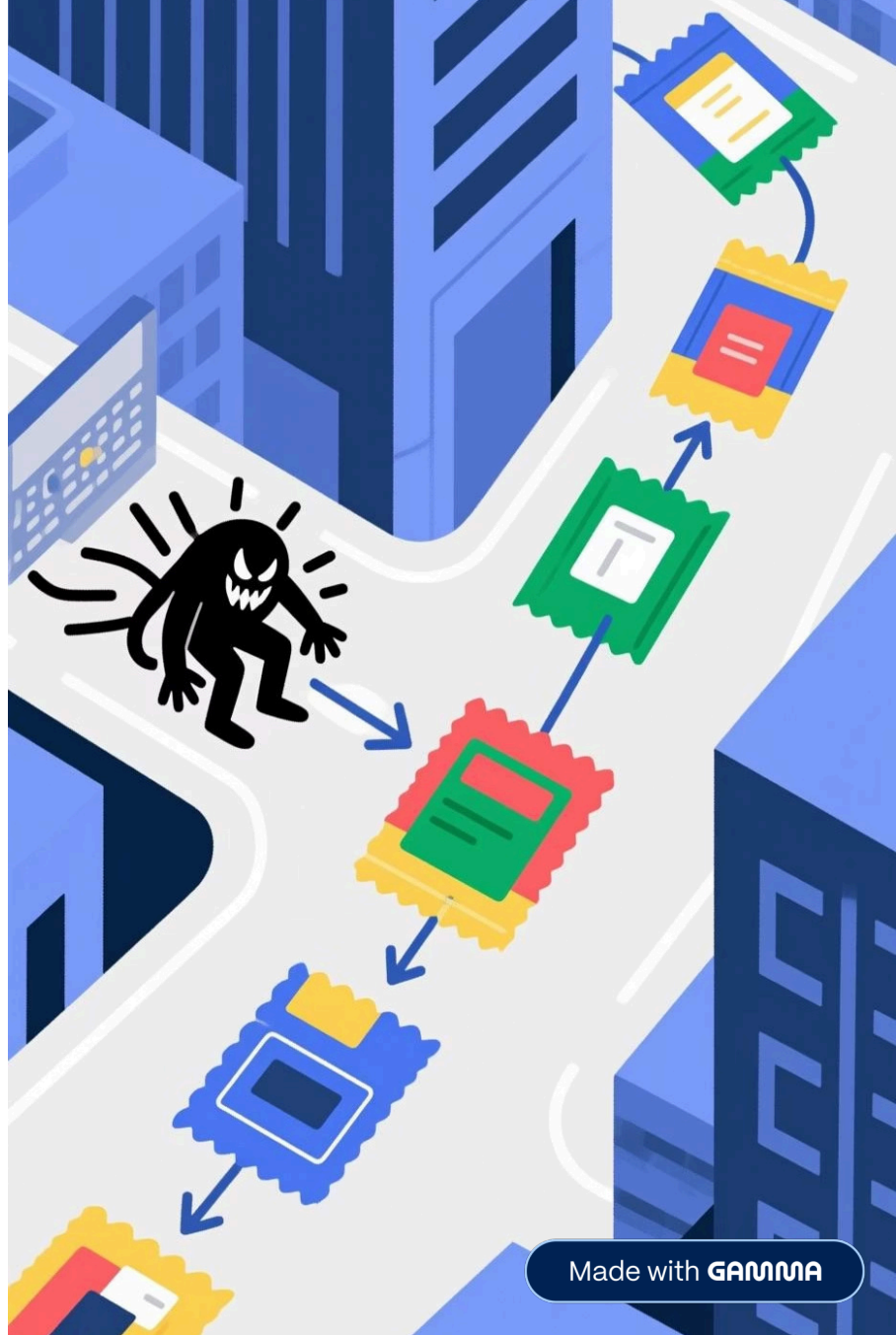
How: Attacker intercepts unencrypted traffic on shared Wi-Fi or downgrades TLS. **Mitigate:** Enforce TLS 1.2/1.3, use HSTS, deploy VPN on untrusted networks, enable WIDS.

ARP Spoofing

How: Forged ARP replies redirect traffic through attacker device. **Mitigate:** Use static ARP entries, Dynamic ARP Inspection, 802.1X, and network access control (NAC).

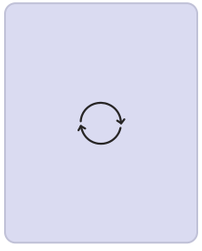
DNS Spoofing

How: Poisoned DNS redirects users to phishing sites despite correct domain entry. **Mitigate:** Enable DNSSEC, use trusted DNS providers, enforce HTTPS, and monitor anomalies.



Cross-Cutting Security Controls

These foundational practices protect against all attack types and form the backbone of a comprehensive security program.

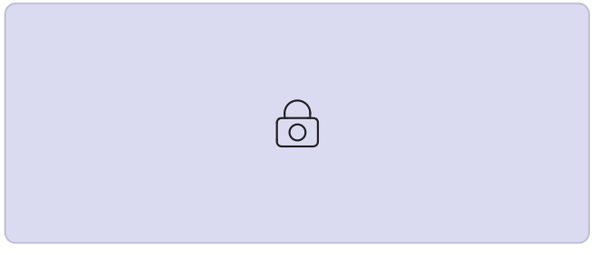


Patch & Vulnerability Management

Maintain inventory, prioritize CVEs by risk, and patch critical issues promptly to eliminate known exploits.

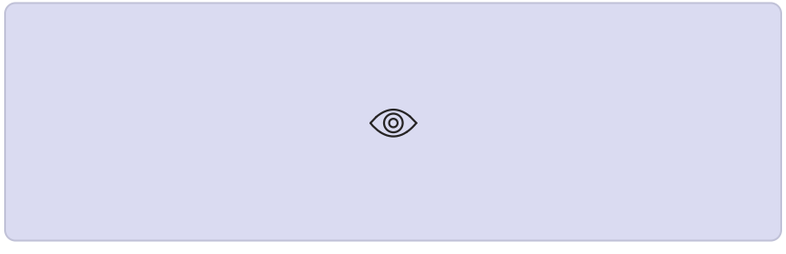
Identity & Access Management

Enforce MFA, least-privilege access controls, and centralized SSO/IdP for stronger authentication.



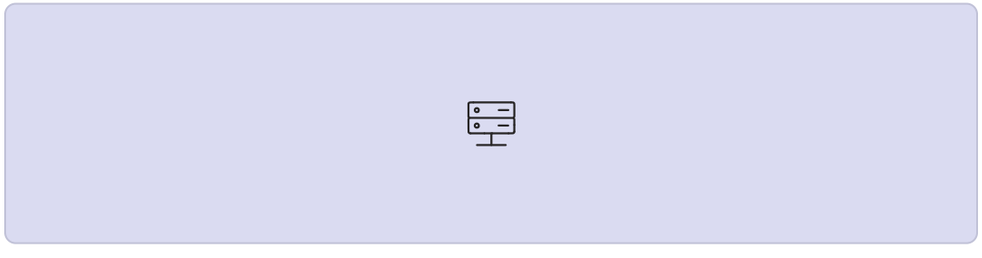
Encryption & Key Management

Deploy TLS 1.2/1.3 everywhere, full-disk encryption, encrypted backups, and secure key lifecycle processes.



Monitoring & Detection

Use SIEM, EDR, IDS/IPS, and NetFlow to correlate logs, detect anomalies, and trigger rapid alerts.



Backups & Disaster Recovery

Maintain encrypted offline backups and test recovery procedures regularly to ensure business continuity.

Key Recommendations & Next Steps

1 Prioritize High-Impact Controls

MFA, patching, and offline backups stop most high-impact attacks. Implement these first.

2 Combine Technical & Human Controls

Layer EDR, WAF, and SIEM with security training, policies, and tabletop incident response exercises.

3 Maintain Visibility & Threat Intelligence

Deploy continuous monitoring, subscribe to external threat feeds, and conduct regular vulnerability scans and penetration tests.

4 Build Resilience

Document an incident response plan, define roles and responsibilities, and stay informed of emerging threats.