TOP TEN CYBER ATTACKS OF 2025

1	**PHISHING AND SOCIAL ENGINEERING** Attackers trick users into revealing credentials or executing malicious content. Implement continuous user awareness training, strong email filtering, and multifactor authentication. Verify sensitive requests out of band before acting.
2	**RANSOMWARE AND EXTORTION** Attackers encrypt and steal data, then threaten to leak or destroy it to coerce payment. Maintain tested offline backups, segment critical systems, harden remote access, and account for Ransomware threats in incident response processes.
3	**EXPLOITATION OF PUBLIC-FACING APPLICATIONS** Vulnerabilities and misconfigurations in public facing applications, VPNs, and APIs allow attackers to gain access. Rigorously patch and remediate vulnerabilities, expose only necessary services, use web application firewalls, and perform regular penetration tests.
4	**REMOTE ACCESS ABUSE** Insecure remote management tools provide attackers with access and cloak their presence. Enforce multifactor authentication on all remote access, implement network controls and instrumentation on remote entities.
5	**CLOUD MISCONFIGURATION AND INTRUSION** Misconfigured cloud resources, over-privileged identities, and exposed access keys allow direct compromise of data stores and cloud workloads at scale. Manage IAM under least-privileged access and enforce configuration management. Leverage native security controls and instrumentation to identify and protect against threats.
6	**SOFTWARE AND SUPPLY CHAIN COMPROMISE** Compromised supply chains allow attackers to distribute malicious updates or abuse trusted access to downstream victims en masse. Organizations should inventory critical suppliers and require robust security controls and disclosure practices.
7	**INFORMATION THEFT OR LEAKAGE** Data breaches fuel criminal markets to perpetrate later intrusions and fraud. Organizations should manage points of compromise aggressively through endpoint protection, restricted rights, credential rotation, and user awareness training. Consider proactive controls such as dark-web monitoring and DLP.
8	**DISTRIBUTED DENIAL OF SERVICE (DDoS)** DDoS attacks overwhelm online services with malicious traffic, causing outages or degraded services. Make use of DDoS-resilient hosting with elastic capacity and rate limiting. Pre-establish response playbooks with upstream providers.
9	**INSIDER AND ACCOUNT-TAKEOVER MISUSE** Legitimate accounts may be used to abuse existing privileges to exfiltrate data or sabotage systems without detection. Strict access governance, least privileged access, and intelligent monitoring can help protect organizations against malicious activity from legitimate accounts.
10	**AI-ENHANCED AND DEEPFAKE-DRIVEN ATTACKS** AI tools and deepfakes make phishing, fraud, and impersonation more convincing and scalable through automation and deep-fake audio or video. Mitigating this threat requires intelligent monitoring and ongoing user vigilance.