Top 50 Cybersecurity Threats of 2025

#	Threat Name	Description	Mitigation
1	Account Takeover	Attackers gain unauthorized access to user accounts, often via stolen credentials.	Implement strong IAM, use MFA, adopt zero trust, monitor for anomalies, review access controls.
2	Advanced Persistent Threat (APT)	Stealthy, prolonged attacks for espionage or data theft, often by nation-states.	Network segmentation, monitor for lateral movement, patch systems, EDR/XDR, phishing training.
3	AWS Attacks	Exploiting vulnerabilities in Amazon Web Services environments.	Follow shared responsibility, secure S3 buckets, monitor access, limit/audit permissions.
4	Application Access Token Abuse	Using stolen OAuth tokens to access cloud/email services.	Monitor token usage, revoke suspicious tokens, educate users on app permissions.
5	Bill Fraud	Fraudulent transactions diverting funds from consumers.	User education, transaction monitoring, anti-phishing tools, verify payment requests.
6	Brute Force Attack	Automated guessing of passwords or PINs.	Strong passwords, rate limiting, account lockout, monitor login activity.
7	Business Email Compromise (BEC)	Impersonating business contacts to trick victims into transferring funds.	Employee training, DMARC/SPF/DKIM, verify payment requests, monitor email activity.
8	Cloud Cryptomining	Hijacking cloud resources for unauthorized cryptocurrency mining.	Monitor usage, restrict permissions, alert on anomalies.
9	Command & Control (C2) Attack	Malware establishes a channel to receive attacker commands.	EDR, network monitoring, block malicious domains, segmentation.
10	Compromised Credentials	Use of stolen passwords or keys to access systems.	Unique passwords, MFA, monitor for leaks, user education.
11	Credential Dumping	Extracting credentials from compromised systems.	Patch systems, limit privileges, monitor for dumping tools, EDR.
12	Credential Reuse Attack	Using stolen credentials on multiple sites.	Unique passwords, password managers, monitor for stuffing.
13	Cross-Site Scripting (XSS)	Injecting malicious scripts into trusted websites.	Sanitize input, Content Security Policy, app testing.
14	Cryptojacking Attack	Malware hijacks devices to mine cryptocurrency.	Monitor CPU usage, patch software, anti-malware.
15	DNS Amplification	DDoS attack using DNS servers to amplify traffic.	Secure DNS, block spoofing, rate limiting.

#	Threat Name	Description	Mitigation
15	DNS Amplification	DDoS attack using DNS servers to amplify traffic.	Secure DNS, block spoofing, rate limiting.
16	DNS Hijacking	Remiting.	Remiting.
32	Phishing Payloads	Malicious attachments or links in phishing emails.	Block attachments, sandboxing, user education.
33	Spear Phishing	Targeted phishing attacks on specific individuals.	Train high-risk users, advanced email security, verify info.
34	Whale Phishing (Whaling)	Phishing attacks targeting high-profile individuals.	Executive education, targeted anti-phishing, strict checks.
35	Privileged User Compromise	Abuse of accounts with elevated privileges.	Limit privileges, monitor activity, just-in-time access.
36	Ransomware	Encrypt data and demand ransom for decryption.	Offline backups, patching, anti-malware, user education.
37	Router/Infrastructure Attacks	Compromise network devices to control/intercept traffic.	Change defaults, update firmware, monitor for changes.
38	Shadow IT	Use of unauthorized IT resources by employees.	Monitor for unauthorized use, employee education, policies.
39	Simjacking	Hijack phone numbers via SIM swap scams.	App-based MFA, user education, monitor account changes.
40	Social Engineering	Manipulate people to divulge confidential information.	Security awareness, verification, monitor for anomalies.
41	Spyware	Software that secretly gathers user data.	Anti-spyware, patching, user education.
42	SQL Injection	Inject malicious SQL queries to manipulate databases.	Sanitize input, parameterized queries, app testing.
43	Supply Chain Attack	Compromise third-party vendors to breach customers.	Vet vendors, monitor activity, limit vendor access.
44	Suspicious Cloud Storage	Exploit misconfigured/vulnerable cloud storage.	Secure storage, monitor logs, encrypt sensitive data.
45	Typosquatting	Register misspelled domains to trick users.	Register similar domains, user education, monitor domains.
46	Watering Hole Attack	Compromise websites frequented by targets.	Monitor for compromised sites, web filtering, user education.
47	Web Session Cookie Theft	Steal authentication cookies to hijack sessions.	Secure/HTTP-only cookies, session timeouts, monitor sessions.
48	Zero-Day Exploit	Exploit previously unknown vulnerabilities.	Prompt patching, IDS/IPS, monitor for abnormal behavior.