# Sobulachi Wanjoku

# 2022 Finnish Parliament attack

**1. How the attack happened**

* The attackers launched a Distributed Denial-of-Service (DDoS) attack by flooding the Finnish parliament’s website with massive amounts of fake traffic.
* The traffic overwhelmed the servers, making the website inaccessible during a live parliamentary session.
* Responsibility was claimed by a pro-Russian hacktivist group, likely as retaliation for Finland’s stance on joining NATO.

**2. Damage caused**

* Website outage: The parliament’s website went offline, disrupting access to official information.
* Public trust impact: While core parliamentary operations weren’t compromised, the attack highlighted vulnerabilities in critical government infrastructure.
* Political signal: It served as a cyber show of force, meant to intimidate Finland during a politically sensitive period.

**3. How it could’ve been prevented**

* DDoS Mitigation Services: Using cloud-based services (e.g., Cloudflare, Akamai) that absorb and filter malicious traffic before it reaches the target.
* Rate Limiting & Traffic Filtering: Setting rules to block abnormal traffic spikes.
* Redundant Infrastructure: Deploying load balancers and backup servers across multiple data centers.
* Continuous Monitoring: Early detection systems to flag unusual traffic patterns in real time.
* Incident Response Preparedness: Having contingency plans so that official communication can continue through alternative channels (e.g., social media, backup portals).

# 2023 MGM Resorts phishing attack

**1. How the attack happened**

* The attack began with social engineering: hackers impersonated an employee and contacted MGM’s IT help desk.
* Using information they gathered (likely from LinkedIn or data brokers), they convinced the help desk to reset account credentials.
* With this access, attackers infiltrated MGM’s systems, locking employees out of internal networks and causing ransomware-style disruptions.
* The attack was linked to the Scattered Spider group, known for highly effective phishing and social engineering techniques.

**2. Damage caused**

* Operational disruption: Slot machines, ATMs, room key cards, and online booking systems were taken offline for days.
* Financial impact: MGM reported losses exceeding $100 million from the attack (including revenue loss and recovery costs).
* Data breach: Customer data (including personal info of guests) was reportedly exposed.
* Reputation hit: Affected trust among guests and highlighted MGM’s weak internal security practices.

**3. How it could’ve been prevented**

* Stronger Authentication: Enforce multi-factor authentication (MFA) on all critical accounts so that stolen/reset credentials alone can’t grant access.
* Employee Awareness Training: Regular phishing and social engineering awareness training for both staff and IT support teams.
* Help Desk Verification Protocols: Strict identity verification (e.g., requiring multiple proofs of identity) before resetting credentials.
* Privileged Access Management (PAM): Limit high-level access accounts and monitor their use closely.
* Zero Trust Security Model: Assume no request is trustworthy by default—always verify.
* Continuous Monitoring & Detection: Use AI/EDR tools to detect unusual login behavior or privilege escalation quickly.

# 2024 Synnovis Lab Attack

**1. How the attack happened**

* The attack was carried out by a Russian-linked ransomware group (Qilin).
* Hackers gained access to Synnovis’s systems—likely through phishing, stolen credentials, or unpatched software vulnerabilities—and deployed ransomware.
* Once inside, they encrypted critical lab data and systems, making them inaccessible to staff.
* The attackers then demanded a ransom for decryption and threatened to leak sensitive patient information.

2. Damage caused

* Healthcare disruption: Thousands of hospital appointments, cancer treatments, and surgeries across London had to be postponed.
* Operational paralysis: Blood test services and diagnostic labs were offline, crippling clinical workflows.
* Patient impact: Delayed treatments posed serious risks to patient health and safety.
* Data exposure: Sensitive medical records of patients were allegedly stolen.
* Financial + reputational loss: NHS partners and Synnovis faced huge recovery costs and public scrutiny over their cybersecurity readiness.

3. How it could’ve been prevented

* Regular Patching & System Updates: Ensure critical systems (including lab software) are not running outdated or vulnerable versions.
* Network Segmentation: Separate lab networks from hospital IT systems to contain damage if one is compromised.
* Backup & Disaster Recovery Plans: Keep offline, immutable backups to quickly restore services without paying ransom.
* Strong Access Controls: Use multi-factor authentication and least privilege principles for all staff accounts.
* 24/7 Monitoring & Threat Detection: Deploy EDR/XDR systems to detect unusual activity (e.g., mass file encryption).
* Employee Security Training: Since healthcare is a major phishing target, continuous training is essential to reduce human error.
* Incident Response Drills: NHS and private partners should rehearse cyberattack scenarios to minimize downtime during real incidents.