Hospital Ransomware

Victim: Regional Hospital
Impact: Doctors lose access to patient records; surgeries delayed; ambulances diverted.
Vulnerability: Employee clicked a phishing email carrying ransomware.
Diagnostic Clues: Files renamed, ransom note appears, unusual file access from one user.
Prevention: Email filtering, security awareness, MFA, offline backups.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?

Airline Reservation System

Victim: Major Airline
Impact: Reservation system offline; thousands of delayed flights.
Vulnerability: Administrator reused a password from another breach.
Diagnostic Clues: Successful login from overseas; new admin account created.
Prevention: Unique passwords, MFA, login alerts.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?

Personal Savings Account

Victim: College Student
Impact: Savings account emptied.
Vulnerability: Fake banking website (phishing).
Diagnostic Clues: Login from unfamiliar location; password reset email; unusual transfers.
Prevention: MFA, password manager, verify URLs.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?

High School Grades

Victim: High School
Impact: Student grades changed.
Vulnerability: Teacher password left on a sticky note.
Diagnostic Clues: After-hours grade changes; login from classroom computer.
Prevention: Strong password practices, auto-lock screens.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?

City Water Utility

Victim: Water Treatment Plant
Impact: Chemical settings modified; public safety risk.
Vulnerability: Remote access exposed with weak credentials.
Diagnostic Clues: Remote login followed by configuration changes.
Prevention: VPN, MFA, disable unused remote access.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?

Online Store

Victim: Small Business
Impact: Customer credit cards stolen.
Vulnerability: Unpatched web server.
Diagnostic Clues: Exploit attempts in web logs; unusual database queries.
Prevention: Patch management, web application firewall.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?

Smart Home

Victim: Family Home
Impact: Security cameras viewed by strangers.
Vulnerability: Default admin password never changed.
Diagnostic Clues: Overseas logins; unknown devices.
Prevention: Change default passwords, firmware updates.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?

Factory

Victim: Manufacturing Plant
Impact: Production halted.
Vulnerability: Infected USB drive connected to engineering workstation.
Diagnostic Clues: Malware immediately after USB insertion.
Prevention: USB controls, endpoint protection.
Discussion: What happened? How did they get in? What clues reveal it? How could it have been prevented?