THE ESSENTIAL 6 CYBERSECURITY CHECKLIST

PHISHING-RESISTANT MFA

Enforce Multi-Factor Authentication across all accounts, prioritizing hardware keys or biometrics over SMS codes to defeat AI-driven session hijacking.

ZERO TRUST ACCESS

Implement the "Principle of Least Privilege," ensuring users and devices are continuously verified and granted only the minimum access necessary for their specific roles.

AUTOMATED PATCH MANAGEMENT:

Enable automated updates for all operating systems, third-party applications, and firmware to close vulnerabilities before they can be exploited by automated AI scanners.

IMMUTABLE BACKUPS (3-2-1-1 RULE)

Maintain three copies of data on two different media, with one offsite and one immutable (uneditable/air-gapped) copy to ensure recovery from ransomware.

CONTINUOUS MONITORING & LOGGING:

Deploy AI-enhanced Endpoint Detection and Response (EDR) to monitor for "Living off the Land" attacks and suspicious behavioral anomalies in real-time.

THE "HUMAN FIREWALL" PROTOCOL

Conduct monthly simulation-based training and establish "Out-of-Band" verification procedures (like the Safe Word protocol) for all high-stakes financial or data requests.