WHAT DOES A SMALL BUSINESS DO ON A RANSOMWARE OR ACCOUNT LOCKOUT DAY?

Follow your written response checklist. CISA's #StopRansomware Guide recommends encrypted offline backups that you test, and an offline copy of your incident response plan. Ready.gov adds: consider turning off the affected device, change passwords, notify system owners and report the incident.

THE STEPS

01 Open the offline copy of your incident response plan.

02 Consider turning off the affected device, as Ready.gov advises.

03 Change account passwords and check for unrecognized charges.

04 Tell your system owners, banks and card companies what happened.

05 File a report with local police, and submit a complaint to the FBI's IC3, per Ready.gov.

06 Restore from the encrypted offline backup you tested. CISA says to keep and test them.

THE CHECKLIST

- ☐ Encrypted offline backups, tested
- ☐ Offline incident response plan
- ☐ Call list on paper
- ☐ Multifactor on every account
- ☐ A paper way to take sales

Sources: CISA, #StopRansomware Guide; Ready.gov, Cybersecurity; CISA, Cyber Essentials. Last reviewed November 17, 2026. General planning information, not medical, legal or financial advice.