-

-

RANSOMWARE RECOVERY GUIDE

A Step-by-Step Framework for Responding to Ransomware Attacks

Created by Jamola Cybersec Services Limited

INTRODUCTION

Ransomware attacks are one of the most significant threats facing businesses today. This guide provides a structured framework for responding to ransomware attacks to minimise damage and maximise recovery.

CRITICAL: DO NOT PAY THE RANSOM

Paying ransomware does not guarantee:

- **That you will get your data back**
- **That the attackers will not hit you again**
- **That your data has not been copied/stolen**
- **That you are not funding criminal organisations**

IMMEDIATE RESPONSE (FIRST 30 MINUTES)

□ 1. ISOLATE AFFECTED SYSTEMS

- **Disconnect infected devices from network immediately**
- **Disable Wi-Fi and Bluetooth on affected devices**
- **Unplug network cables**
- **Do NOT restart or shutdown devices (this can destroy evidence)**

□ 2. CONTAIN THE ATTACK

- **Block ransomware communication domains at firewall**
- **Disable email for affected users if spreading via email**
- **Lock down network shares and drives**
- **Implement firewall rules to block malicious traffic**

□ 3. ACTIVATE INCIDENT RESPONSE TEAM

- Alert key personnel and management
- Activate external support if needed
- Establish communication channels
- Document everything

ASSESSMENT (FIRST 1-2 HOURS)

□ 4. DETERMINE SCOPE

- Identify which systems are affected
- Determine what data has been encrypted
- Identify if backups are affected
- Check if data has been exfiltrated

□ 5. IDENTIFY RANSOMWARE TYPE

- Check for ransom note and extension
- Use online tools to identify ransomware family
- Check for known decryption tools
- Document ransomware information

□ 6. VERIFY BACKUPS

- Check if backups are intact
- Determine if backups were affected
- Locate clean backup copies
- Test backup integrity

INVESTIGATION (FIRST 2-4 HOURS)

□ 7. DETERMINE INFECTION VECTOR

- Review email logs for phishing
- Check for compromised remote access
- Review vulnerability scans
- Identify initial entry point

□ 8. EVIDENCE PRESERVATION

- Capture memory images of affected systems
- Collect encrypted files
- Save ransom note and contact details
- Record all timestamps

□ 9. DECISION MAKING

- Can you restore from backups?
- Is there a decryption tool available?
- Do you need external support?
- Should you involve law enforcement?

RECOVERY OPTIONS

OPTION A: RESTORE FROM BACKUPS

□ 10. BACKUP RESTORATION

- Verify backup integrity
- Isolate backup restore environment
- Restore systems from clean backups
- Apply all security patches
- Change all passwords

□ 11. POST-RESTORE ACTIONS

- Scan for remaining malware
- Update security controls
- Implement additional protections
- Monitor for suspicious activity

OPTION B: USE DECRYPTION TOOLS

□ 12. DECRYPTION TOOL APPLICATION

- Identify if tool exists for ransomware variant
- Download from trusted source (NoMoreRansom.org)
- Test on a sample before full deployment
- Follow tool instructions carefully

OPTION C: SEEK PROFESSIONAL HELP

□ 13. ENGAGE INCIDENT RESPONSE FIRM

- Contact experienced incident response team
- Provide initial assessment information
- Follow professional guidance
- Support forensic investigation

POST-RECOVERY

□ 14. SYSTEM HARDENING

- **Implement MFA everywhere**
- **Update all systems and applications**
- **Install endpoint protection**
- **Configure email security**

□ 15. SECURITY IMPROVEMENTS

- **Review and update backup strategy**
- **Implement security awareness training**
- **Review and improve access controls**
- **Develop incident response plan**

□ 16. REPORTING

- **Report to information commissioner if required**
- **Notify affected parties if data breached**
- **Report to law enforcement**
- **Document lessons learned**

PREVENTION MEASURES

1. **Maintain regular, tested backups (3-2-1 rule)**
2. **Implement MFA for all accounts**
3. **Keep all software updated**
4. **Use email security solutions**
5. **Conduct security awareness training**
6. **Use endpoint protection**
7. **Implement network segmentation**
8. **Restrict admin privileges**
9. **Monitor for suspicious activity**

10. Develop and test incident response plan

EMERGENCY CONTACTS

Ransomware Response Lead: _____

Phone: _____

Backup/Recovery Lead: _____

Phone: _____

Legal Contact: _____

Phone: _____

External Support: _____

Phone: _____

USEFUL RESOURCES

- **NoMoreRansom.org (decryption tools)**
- **CISA Ransomware Guide (cisa.gov)**
- **UK National Cyber Security Centre (ncsc.gov.uk)**
- **Report ransomware to Action Fraud (actionfraud.police.uk)**

ABOUT JAMOLA CYBERSEC SERVICES LIMITED

Jamola Cybersec Services Limited provides remote cybersecurity services to SMEs worldwide. We help businesses secure their systems, protect their data, and build resilient security programmes.

Contact: info@jamolacybersec.uk

Website: https://jamolacybersec.uk