# ACE Networks

## Ransomware Response Playbook for Cyprus SMEs

2025 Edition

### Recognizing a Ransomware Attack

- Unusual file extensions appearing on documents and databases.
- Locked files with ransom notes demanding payment.
- Sudden slowdown or unresponsive systems.
- Unauthorized administrative activity on your network.

### Immediate Response Steps

- Isolate the infected machine from the network immediately.
- Disconnect shared drives, external storage, and cloud sync tools.
- Do not restart the infected system until an assessment is done.
- Preserve system logs and ransom notes for investigation.

### Why Not to Pay the Ransom

- Payment does not guarantee file recovery.
- It encourages further attacks against your business.
- You may face legal implications depending on the recipient of funds.
- Focus on recovery and prevention instead.

### Containment and Recovery

- Use clean backups to restore critical systems.
- Ensure backups are scanned for malware before restoration.
- Rebuild compromised systems with updated operating systems.
- Engage IT security specialists for forensic analysis.

### Post-Attack Actions

- Report the incident to national authorities and regulators.
- Assess GDPR obligations and notify affected parties if required.
- Communicate with clients and partners to maintain trust.

- Conduct a full review of security gaps exploited during the attack.

### Prevention Checklist

- Enable multi-factor authentication on all accounts.
- Apply patches and software updates promptly.
- Conduct quarterly cybersecurity awareness training.
- Run phishing simulations to test staff response.
- Regularly test and update your incident response plan.

### ACE Networks Support

- Ransomware is a serious and growing threat. Having a plan makes all the difference.
- ACE Networks supports Cyprus SMEs with ransomware readiness, recovery, and prevention strategies.
- For expert guidance, visit: https://acenetworks.eu/contact-ace-networks/