

How to defend against Ransomware attacks?



Keep Systems and Software Updated



- ✓ Apply patches promptly: Many ransomware strains exploit known vulnerabilities. Regularly update operating systems, applications, and firmware.
- ✓ Automate updates where possible to ensure no critical patches are missed.
- ✓ Remove or replace unsupported software that no longer receives security updates.



Use Strong Backup Practices



- ✓ Follow the 3-2-1 rule: Keep 3 copies of your data, on 2 different types of storage, with 1 copy stored offline or offsite.
- ✓ Test backups regularly to confirm they can be restored quickly and completely.
- ✓ Encrypt backup data so that even if backups are stolen, they cannot be misused.



Strengthen Access Controls



- ✓ Enable Multi-Factor Authentication (MFA) for all critical systems.
- ✓ Limit user privileges: Only give employees access to the data and tools they need.
- ✓ Use unique, strong passwords, for critical system 16+ signs.



Deploy Security Tools and Monitoring



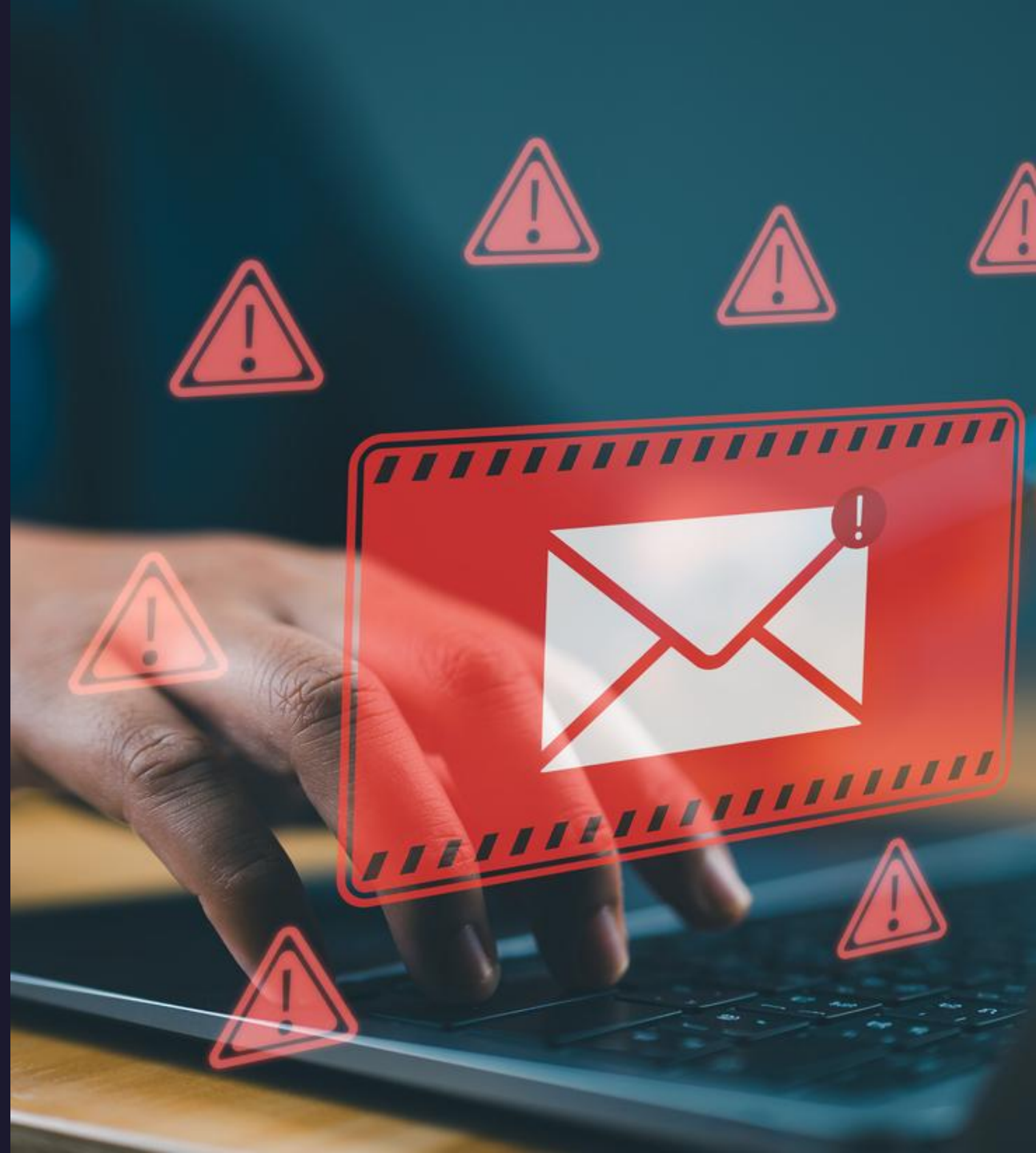
- ✓ Use reputable endpoint protection that can detect and block ransomware before it executes.
- ✓ Set up intrusion detection and monitoring to spot unusual activity early.
- ✓ Segment your network so that an infection in one area cannot spread across the entire environment.



Train Employees and Build Awareness



- ✓ Educate staff about phishing: Many ransomware attacks begin with malicious email attachments or links.
- ✓ Run regular simulations to test readiness.
- ✓ Create a clear reporting process so suspicious emails or activity are flagged immediately.



Develop and Test an Incident Response Plan

- ✓ Have a step-by-step playbook for responding to a ransomware event. Don't forget the external communication plan.
- ✓ Name the crisis team and clarify the responsibilities in the event of a crisis in advance, so that everyone knows their responsibilities and task.
- ✓ Conduct cyberattack simulations to test the plan in realistic conditions and uncover gaps before a real incident.



We recommend Zero Trust Architecture

- ✓ Verify every user and device before granting access.
- ✓ Continuously monitor trust levels to prevent lateral movement if a breach occurs.
- ✓ Apply least-privilege access by default, ensuring accounts and devices get only the minimum rights needed.



Key Takeaways

Stay updated

- Regularly patch and replace outdated systems to close common entry points for ransomware.

Back Up Smartly

- Maintain encrypted, offline backups and test them often to ensure fast recovery.

Limit Access

- Apply least-privilege access, MFA, and network segmentation to reduce the blast radius of an attack.

Plan and Train

- Build an incident response plan and train employees to recognize and report suspicious activity quickly.

Get in touch. We are happy to support.

www.patecco.com

info@patecco.com