

YOUR 4-WEEK CYBERSECURITY CHALLENGE

Small steps today = stronger security tomorrow.



WEEK 1 Secure the Basics

Day 1: Update all software and operating systems

Day 2: Turn on multi-factor authentication (MFA)

Day 3: Audit user accounts (remove old/unused access)

Day 4: Strengthen Wi-Fi passwords & router settings

Day 5: Install updates on mobile devices

Weekend Tip:
Talk to your team about common phishing red flags



WEEK 2 Safeguard Systems & Data

Day 6: Schedule a short cybersecurity training session

Day 7: Share a phishing email example with staff

Day 8: Set rules for secure remote work access

Day 9: Review permissions on shared files/folders

Day 10: Create a policy for reporting suspicious activity

Weekend Tip: Post your team's "top 3 security habits" on a visible board or Slack channel



WEEK 4 Secure the Basics

Day 16: Review access controls for sensitive data

Day 17: Draft a simple incident response checklist

Day 18: Test restoring a file from backup

Day 19: Confirm vendor security (cloud tools, apps)

Day 20: Schedule quarterly security check-ins

Weekend Tip: Celebrate your progress – small steps lead to big protection



WEEK 3 Secure the Basics

Day 11: Test your backup system

Day 12: Verify backups are stored offsite or in the cloud

Day 13: Run an antivirus/endpoint security scan

Day 14: Check firewall rules and alerts

Day 15: Patch any out-of-date apps or plugins

Weekend Tip: Ask "What happens if we're offline for 24 hours?" and discuss the plan

"Ready to go beyond 30 days? Lamb Telecom helps small organizations turn these habits into year-round protection."



LAMB TELECOM