MOGUL MEDIA
CONSULTING

Building a Culture of Cyber Awareness Implementation Checklist

Provided by Mogul Media Consulting

Phase 1: Foundation (Months 1-2)

Leadership & Planning

- [ ] Secure executive sponsorship and budget allocation
- [ ] Conduct baseline security awareness assessment
- [ ] Define clear cybersecurity roles and responsibilities
- [ ] Document current security policies and identify gaps
- [ ] Establish communication channels for security updates

Phase 2: Program Development (Months 2-3)

Core Components

- [ ] Create essential security policies (passwords, email, data handling)
- [ ] Develop role-appropriate training materials
- [ ] Design phishing simulation program
- [ ] Plan regular security communication strategy
- [ ] Establish incident reporting procedures

Phase 3: Launch & Implementation (Months 3-4)

Deployment

- [ ] Integrate security awareness into employee onboarding
- [ ] Launch initial comprehensive security training for all staff
- [ ] Begin monthly phishing simulations
- [ ] Start regular security communications (weekly tips, monthly updates)
- [ ] Identify and train security champions from each department

Phase 4: Engagement & Reinforcement (Months 4-8)
Building Momentum

- [ ] Host security awareness events and training sessions
- [ ] Implement recognition program for security-conscious behavior
- [ ] Create feedback mechanisms for employees to ask questions
- [ ] Share relevant security news and threat updates
- [ ] Conduct tabletop exercises for incident response

Phase 5: Measurement & Improvement (Months 6-12)
Tracking Progress

- [ ] Monitor key metrics (phishing click rates, incident reports, training completion)
- [ ] Conduct quarterly employee security culture surveys
- [ ] Review and update security policies based on lessons learned
- [ ] Analyze program effectiveness and adjust strategies
- [ ] Celebrate security wins and share success stories

Phase 6: Sustainability (Ongoing)
Long-term Success

- [ ] Establish annual security awareness program review
- [ ] Plan for program scalability and evolution
- [ ] Keep training content current with emerging threats
- [ ] Maintain active security champion network
- [ ] Integrate security considerations into business processes

Quick Start Actions (First 30 Days)

Week 1:

- [ ] Get leadership buy-in and assign program owner
- [ ] Assess current security awareness maturity

Week 2:

- [ ] Review existing policies and identify critical gaps
- [ ] Select training platform or approach

Week 3:

- [ ] Create basic security awareness training module
- [ ] Plan communication strategy and channels

Week 4:

- [ ] Launch pilot training with small group
- [ ] Begin weekly security tip communications

Essential Success Metrics

Track These Key Indicators:

- [ ] Phishing simulation click rates (target: <5%)
- [ ] Security training completion rates (target: 95%+)
- [ ] Employee security incident reporting frequency
- [ ] Time to detect and report security issues
- [ ] Employee satisfaction with security programs

Red Flags to Address Immediately

Take Action If You See:

- [ ] High phishing simulation click rates (>20%)
- [ ] Employees afraid to report potential security incidents
- [ ] Security training completion rates below 80%
- [ ] Multiple employees falling for same types of attacks
- [ ] Lack of security questions or engagement from staff

This checklist is designed to be flexible and scalable. Start with the essentials and build complexity as your program matures and your organization grows.