Deepfake Defense Checklist

15 Verification Protocols to Protect Your Business Today

A Comprehensive Security Guide from RedHub AI

https://www.redhub.ai

Purpose

This checklist is designed to help organizations protect themselves from AI-generated deepfake fraud, identity impersonation, and digital trust attacks.

Core Principles

1. Verify before trust
2. Slow down urgent requests
3. Train people continuously

Deepfake Defense Checklist

15 Verification Protocols to Protect Your Business Today

A Comprehensive Security Guide from RedHub AI

How to Use This Checklist

Print this checklist and distribute it to every employee who handles financial transactions, sensitive data, or executive communications. Review these protocols quarterly and update verification phrases monthly.

Risk Level Guide

- Critical: Implement immediately (this week)
- High Priority: Implement within 30 days
- Important: Implement within 90 days

SECTION 1: IDENTITY VERIFICATION PROTOCOLS

Protocol #1: Secret Verification Phrases (Critical)

What to do

- Create unique verification phrases for each team member
- Rotate phrases monthly using a secure method
- Avoid phrases that could be found on social media or public records
- Store phrases in an encrypted password manager, not email or shared documents

Example Implementation

- Finance Team Prompt: “What was our verification word for January 2026?”
- Expected Response: “Thunder” (rotated monthly)
- Incorrect answer or hesitation requires immediate stop and alternate verification

Who needs this
Anyone authorized to approve payments, access sensitive data, or make executive decisions

---

Protocol #2: Multi-Channel Confirmation (Critical)

What to do

- Never approve high-risk requests based on a single video call
- Require confirmation across at least two independent channels
- Use known, pre-verified phone numbers
- Require in-person verification when feasible

Required for

- Payments over $10,000
- Wire transfers
- Admin password resets
- Vendor payment changes

- Confidential data releases

Implementation Example

1. Receive request via video call
2. End call and phone known office number
3. Confirm verbally
4. Send encrypted confirmation via secure company messaging
5. Proceed only when all channels align

Protocol #3: Pre-Established Emergency Codewords (Critical)

What to do

- Establish codewords to distinguish real emergencies from social engineering
- Use separate codes for different threat levels
- Treat requests without codewords as suspicious
- Share codewords only in person or via encrypted calls

Codeword System Example

- Green Code ("Pineapple"): Normal operations
- Yellow Code ("Banana"): Additional verification required
- Red Code ("Strawberry"): Suspected fraud or duress

When to require
Any urgent or out-of-process request

Protocol #4: Video Call Verification Checklist (High Priority)

Before approving any request on a video call, verify:

- Background matches known location
- Lighting is consistent with time of day
- Eye movements appear natural
- Lip sync matches audio precisely
- Head movement is smooth without distortion
- Audio quality matches prior calls
- Subject can perform spontaneous actions
- Subject knows non-public personal or company details

If any item fails, require alternate verification immediately.

Protocol #5: Time-Delay Rule for Urgent Requests (Critical)

What to do

- Enforce a mandatory 15-minute delay on urgent financial requests
- Use the delay to verify through independent channels
- Train staff that legitimate emergencies tolerate verification
- Log all urgent requests for audit purposes

Red Flag Phrases

- "I need this done immediately"
- "Don't tell anyone"
- "This is confidential"
- "We'll miss the deadline"

Urgency is the attacker's primary weapon. Slowing down breaks the attack.

SECTION 2: TECHNICAL SAFEGUARDS

Protocol #6: AI Detection Software (High Priority)

What to do

- Deploy deepfake detection tools on key communication channels
- Subscribe to real-time threat intelligence feeds
- Run suspicious media through multiple detection systems
- Update detection tools weekly

Recommended Tools

- Microsoft Video Authenticator
- Sensity AI
- Deepware Scanner
- Intel FakeCatcher
- Reality Defender

Protocol #7: Video Call Recording Policy (High Priority)

What to do

- Record all video calls involving financial or sensitive decisions
- Store recordings in encrypted, tamper-proof cloud storage
- Announce recording at call start
- Retain recordings for at least 12 months

Verify compliance with local consent laws.

Protocol #8: Email Authentication Verification (Important)

What to do

- Enable SPF, DKIM, and DMARC
- Use sender-authentication tools
- Train staff to inspect headers for anomalies
- Flag lookalike email addresses

Protocol #9: Biometric Multi-Factor Authentication (High Priority)

What to do

- Require biometrics for sensitive systems
- Use behavioral biometrics where possible
- Deploy hardware security keys for critical accounts
- Never rely on passwords alone

Protocol #10: Network Traffic Analysis (Important)

What to do

- Monitor for abnormal bandwidth during video calls
- Flag unusual latency or routing
- Detect connections to known deepfake infrastructure

SECTION 3: ORGANIZATIONAL POLICIES

Protocol #11: Dual-Authorization Requirements (Critical)

What to do

- Require multiple approvers for high-value transactions
- Prevent single-person authorization technically

Recommended Thresholds

- $5,000+: Two approvals
- $25,000+: Three approvals
- $100,000+: Multi-channel verification
- Vendor changes: Always dual approval

Protocol #12: Vendor Verification Callback Process (High Priority)

What to do

- Maintain verified vendor contact records
- Call known numbers to confirm changes
- Document all verification attempts

Protocol #13: Social Media Lockdown Policy (Important)

What to do

- Reduce public exposure of executive images and voice
- Avoid posting travel or schedule details
- Monitor for misuse of employee likenesses

Protocol #14: Incident Response Plan (High Priority)

What to do

1. Stop the transaction immediately
2. Preserve all evidence
3. Contact security and IT
4. Verify through alternate channels
5. Document events
6. Notify affected parties
7. File report with FBI IC3
8. Conduct post-incident review

Protocol #15: Mandatory Deepfake Awareness Training (Critical)

What to do

- Conduct quarterly training
- Run simulated deepfake scenarios
- Test and retrain regularly
- Track completion and performance

IMPLEMENTATION ROADMAP

Week 1

- Verification phrases
- Multi-channel confirmation
- Emergency codewords
- Time-delay rule
- Dual authorization
- Training kickoff

Month 1

- Detection software
- Recording policies
- MFA rollout
- Vendor verification
- Incident response plan

Quarter 1

- Email authentication
- Network monitoring
- Social media policy
- Simulation testing

FINAL THOUGHTS

Deepfake threats evolve rapidly. This checklist reflects best practices as of January 2026 and should be reviewed quarterly.

Three principles:

1. Verify, then trust
2. Slow down
3. Train continuously

With these protocols in place, your organization dramatically reduces its exposure to deepfake fraud.

Document Version: 1.0
Last Updated: January 9, 2026
Next Review: April 9, 2026