Employee Security Awareness Training Package

Complete FTC Safeguards Rule Compliance Training Program

RebootTwice LLC
Employee Training Experts
Phone: (949) 831-8821
Email: sales@reboottwice.com
Web: www.reboottwice.com

Training Package Version: 2.0
Last Updated: January 2025
Compliance: FTC Safeguards Rule 16 CFR Part 314
Target Audience: Financial Services Organizations

TRAINING PACKAGE CONTENTS

📚 CORE TRAINING MODULES

- Module 1: FTC Safeguards Rule Overview (45 minutes)
- Module 2: Password Security & Multi-Factor Authentication (30 minutes)
- Module 3: Phishing & Social Engineering Defense (40 minutes)
- Module 4: Physical Security & Clean Desk Policies (25 minutes)
- Module 5: Customer Data Handling & Privacy (35 minutes)
- Module 6: Incident Reporting & Response (30 minutes)
- Module 7: Remote Work Security (30 minutes)
- Module 8: Vendor & Third-Party Security (20 minutes)

🎯 ROLE-SPECIFIC TRAINING

- Executive Leadership Training (60 minutes)
- IT Administrator Deep Dive (90 minutes)
- Customer Service Representative Training (45 minutes)
- Seasonal/Temporary Employee Training (30 minutes)

🏢 INDUSTRY-SPECIFIC MODULES

- Tax Preparation Services (45 minutes)
- Mortgage & Real Estate Finance (45 minutes)
- Investment Advisory Services (45 minutes)
- Debt Collection Agencies (45 minutes)

📊 ASSESSMENT & TRACKING MATERIALS

- Pre-training knowledge assessments

- Module completion quizzes
- Final certification examination
- Phishing simulation campaigns
- Training effectiveness metrics

📋 IMPLEMENTATION RESOURCES

- Training administrator guide
- Customization templates
- Compliance documentation forms
- Annual update procedures

MODULE 1: FTC SAFEGUARDS RULE OVERVIEW

Duration: 45 minutes | **Format:** Video + Slides + Quiz

Learning Objectives:

By completing this module, employees will:

- Understand FTC Safeguards Rule requirements and penalties
- Identify their role in compliance and data protection
- Recognize the business impact of security breaches
- Know reporting procedures and escalation paths

Slide Content Outline:

Slide 1-5: Introduction & Context

Slide 1: Welcome to Security Awareness Training
- RebootTwice LLC presents comprehensive security training
- Required annual training for FTC compliance
- Your role in protecting customer information

Slide 2: Why This Training Matters
- $51,744 maximum penalty PER VIOLATION in 2025
- Business reputation and customer trust at stake
- Legal and regulatory requirements
- Personal responsibility and accountability

Slide 3: FTC Safeguards Rule Overview
- Applies to financial institutions under Gramm-Leach-Bliley Act
- Protects customer personal information
- Requires written security programs and employee training
- Regular updates and compliance monitoring required

Slide 4: What is Customer Information?
- Social Security Numbers and Tax IDs
- Bank account and routing numbers
- Credit card and payment information
- Personal contact information (addresses, phone, email)
- Financial records and transaction history
- Any personally identifiable information (PII)

Slide 5: Our Organization's Commitment
- [COMPANY NAME] prioritizes customer data protection
- Investment in security technology and training
- Culture of security awareness and responsibility
- Continuous improvement and compliance monitoring

Slide 6-10: Key Requirements

Slide 6: Written Information Security Program (WISP)
- Comprehensive security plan documented
- Regular updates and board oversight
- Employee training and awareness programs
- Incident response procedures established

Slide 7: Multi-Factor Authentication (MFA)
- Required for ALL systems with customer data
- Something you know + something you have
- Protects against password compromise
- Your responsibility to set up and maintain

Slide 8: Encryption Requirements
- Customer data encrypted at rest and in transit
- Secure email for customer communications
- Encrypted storage for mobile devices
- Automatic encryption for cloud services

Slide 9: Access Controls & Monitoring
- Minimum necessary access principle
- Regular access reviews and updates
- All activities logged and monitored
- Immediate reporting of suspicious activity

Slide 10: Vendor Management
- Third-party security assessments required
- Contractual security requirements
- Regular monitoring and reviews
- Your role in vendor interactions

Slide 11-15: Employee Responsibilities

Slide 11: Your Daily Security Responsibilities
- Follow all security policies and procedures
- Protect customer information in your custody
- Report security incidents immediately
- Complete required training and updates
- Maintain confidentiality at all times

Slide 12: Password Security Requirements
- Strong, unique passwords for each system
- Password manager usage encouraged
- Never share passwords with anyone
- Regular password updates
- MFA setup and maintenance

Slide 13: Physical Security Practices
- Lock computer screens when away
- Secure sensitive documents
- Escort visitors in secure areas
- Report suspicious activities
- Clean desk policy enforcement

Slide 14: Communication Security
- Verify recipient before sending customer data
- Use encrypted email for sensitive information
- Be cautious with phone requests for information
- Avoid discussing customer data in public
- Secure disposal of printed materials

Slide 15: Incident Reporting
- What constitutes a security incident
- When and how to report incidents
- Who to contact (Qualified Individual contact info)
- No blame culture - focus on improvement
- Quick reporting minimizes damage

Video Script: "A Day in the Life of Secure Operations"

SCENE 1: MORNING ARRIVAL (3 minutes)
Narrator: "Meet Sarah, a customer service representative at [COMPANY NAME].
Let's follow her through a day of secure practices..."

[Show Sarah arriving at office]
- Badge access to building (physical security)
- Secure login with MFA (technical security)
- Review of overnight security alerts (monitoring)
- Team huddle about current threats (awareness)

Key Learning Points:
- Security starts the moment you arrive
- MFA is required for all systems
- Stay informed about current threats
- Team communication is essential

SCENE 2: CUSTOMER INTERACTIONS (5 minutes)
[Show Sarah handling customer calls and emails]
- Verifying customer identity before accessing accounts
- Using encrypted email for sensitive communications
- Handling a suspicious phone call (social engineering attempt)
- Proper documentation of customer interactions

Key Learning Points:
- Always verify customer identity
- Use secure communication channels
- Recognize social engineering attempts
- Document interactions properly

SCENE 3: INCIDENT RESPONSE (4 minutes)
[Show Sarah discovering suspicious email attachment]
- Recognition of potential phishing email
- Immediate reporting to IT team
- Isolation of potentially compromised system
- Documentation of incident details
- Communication with Qualified Individual

Key Learning Points:
- Trust your instincts about suspicious activity
- Report immediately, don't investigate alone
- Follow incident response procedures
- Document everything
- Communication is critical

SCENE 4: END OF DAY (3 minutes)
[Show Sarah's secure shutdown procedures]
- Locking computer screen
- Securing physical documents
- Proper disposal of printed materials
- Reviewing day's security practices
- Planning for tomorrow's security considerations

Key Learning Points:

- Security continues until you leave
- Clean desk policy enforcement
- Secure disposal procedures
- Daily security review
- Continuous improvement mindset

Assessment Quiz: Module 1

Question 1: What is the maximum FTC penalty per violation in 2025?
a) $25,000
b) $51,744
c) $100,000
d) $500,000
Correct Answer: b) $51,744

Question 2: Which of the following is considered customer information?
a) Social Security Numbers
b) Bank account numbers
c) Personal contact information
d) All of the above
Correct Answer: d) All of the above

Question 3: When should you report a suspected security incident?
a) After investigating it yourself
b) Only if you're certain it's a real threat
c) Immediately upon discovery
d) At the end of the day
Correct Answer: c) Immediately upon discovery

Question 4: Multi-Factor Authentication is required for:
a) Only email systems
b) Only financial systems
c) All systems containing customer data
d) Only administrative accounts
Correct Answer: c) All systems containing customer data

Question 5: What should you do if you receive a suspicious email?
a) Delete it immediately
b) Forward it to colleagues for their opinion
c) Click links to investigate
d) Report it immediately to IT
Correct Answer: d) Report it immediately to IT

Question 6: The "clean desk policy" requires:
a) Keeping your desk neat and organized
b) Securing sensitive documents when not in use
c) Using only company-provided supplies
d) Eating lunch away from your desk
Correct Answer: b) Securing sensitive documents when not in use

Question 7: Who is responsible for protecting customer information?
a) Only the IT department
b) Only management
c) Only the Qualified Individual
d) All employees
Correct Answer: d) All employees

Question 8: How often should you update your passwords?
a) Monthly
b) Quarterly
c) Annually

d) According to company policy
Correct Answer: d) According to company policy

Question 9: Before sharing customer information, you must:
a) Get supervisor approval
b) Verify the recipient's identity and authorization
c) Make a copy for your records
d) Wait 24 hours
Correct Answer: b) Verify the recipient's identity and authorization

Question 10: What is the primary purpose of the FTC Safeguards Rule?
a) To increase company profits
b) To protect customer personal information
c) To reduce paperwork
d) To improve customer service
Correct Answer: b) To protect customer personal information

MODULE 2: PASSWORD SECURITY & MFA

Duration: 30 minutes | **Format:** Interactive Demo + Slides + Hands-on Setup

Learning Objectives:

- Create strong, unique passwords for all accounts
- Set up and maintain multi-factor authentication
- Use password managers effectively
- Recognize and avoid password-related threats

Interactive Demo Script: "Password Security Best Practices"

DEMONSTRATION 1: Password Strength Testing (8 minutes)

[Live demonstration using password strength checker]

Narrator: "Let's test different password types and see their strength..."

Weak Password Examples:
- "password123" → Cracked in seconds
- "company2025" → Cracked in minutes
- "qwerty" → Cracked instantly

Strong Password Examples:
- "MyDog$Name&Birthday2015!" → Several years to crack
- "Coffee#Lover@Morning*Time" → Decades to crack
- Random 16-character string → Centuries to crack

Key Learning Points:
- Length matters more than complexity
- Avoid personal information
- Use unique passwords for each system
- Consider passphrases for memorability

DEMONSTRATION 2: MFA Setup Process (12 minutes)

[Step-by-step MFA setup on company systems]

Step 1: Download Authenticator App
- Microsoft Authenticator (recommended)
- Google Authenticator
- Authy (backup option)

Step 2: Enable MFA on Email Account
- Access security settings
- Select "Add authentication method"
- Scan QR code with app
- Enter verification code
- Save backup codes

Step 3: Test MFA Login
- Log out of email system
- Log back in with username/password
- Complete MFA prompt on phone
- Verify successful access

Step 4: Set Up Backup Methods
- Register backup phone number
- Generate backup codes
- Store codes securely
- Test backup authentication

Key Learning Points:
- MFA adds critical security layer
- Setup is quick and easy

- Backup methods prevent lockout
- Required for all company systems

DEMONSTRATION 3: Password Manager Usage (10 minutes)

[Live demonstration of password manager]

Feature Overview:
- Automatic password generation
- Secure storage and encryption
- Auto-fill capabilities
- Cross-device synchronization
- Security audit features

Setup Process:
- Install recommended password manager
- Create master password
- Import existing passwords
- Generate strong passwords for weak accounts
- Set up MFA for password manager

Best Practices:
- Use unique master password
- Enable MFA on password manager
- Regular security audits
- Share credentials securely when needed
- Keep software updated

Key Learning Points:
- Password managers improve security
- Unique passwords for every account
- Master password must be memorable
- Company-approved solutions only

Hands-On Exercise: "Secure Your Accounts"

Exercise Instructions:

STEP 1: Password Assessment (5 minutes)
- Review your current passwords (don't share them)
- Rate their strength using provided checklist
- Identify accounts needing stronger passwords
- Note any duplicate passwords

STEP 2: MFA Activation (10 minutes)
- Set up MFA on your email account
- Configure MFA for company applications
- Test authentication process
- Save backup codes securely

STEP 3: Password Manager Setup (10 minutes)
- Install company-approved password manager
- Create strong master password
- Generate new strong passwords for weak accounts
- Update at least 3 account passwords

STEP 4: Verification (5 minutes)
- Test login to updated accounts
- Verify MFA is working properly
- Confirm password manager auto-fill
- Report completion to trainer

Completion Criteria:
✓ MFA enabled on all required systems
✓ Password manager installed and configured
✓ At least 3 passwords updated to strong versions
✓ Backup codes saved securely
✓ All systems tested successfully

MODULE 3: PHISHING & SOCIAL ENGINEERING DEFENSE

Duration: 40 minutes | **Format:** Video Scenarios + Interactive Exercises

Video Scenarios: "Spot the Threats"

Scenario 1: The Urgent Email (8 minutes)

SETUP: Employee receives urgent email claiming to be from CEO

Email Content:
From: CEO <ceo@commpany.com> [Note: misspelled domain]
Subject: URGENT: Wire Transfer Needed Immediately
"I'm in a meeting and need you to wire $50,000 to this vendor immediately.
Account details attached. This is confidential - don't discuss with anyone.
Thanks, [CEO Name]"

Red Flags to Identify:
- Misspelled domain name
- Urgent request for money transfer
- Request for secrecy
- Unusual request from executive
- Poor grammar/formatting
- Attachment from unknown source

Correct Response:
- Do not click any links or attachments
- Verify request through known contact method
- Report suspicious email to IT team
- Document the incident
- Never transfer money based on email alone

Discussion Points:
- CEO fraud is common in business
- Always verify unusual requests
- Trust your instincts about suspicious communications
- Cybercriminals research companies for realistic impersonation

Scenario 2: The Helpful IT Support Call (10 minutes)

SETUP: Employee receives call from "IT Support" requesting access

Phone Conversation:
Caller: "Hi, this is Mike from IT support. We're having network issues and need to remote into your computer to fix a security problem. Can you go to this website and download the remote access tool?"

Red Flags to Identify:
- Unsolicited call from IT
- Request for remote access
- Pressure to act quickly
- Request to download software
- Unfamiliar voice claiming to be IT
- Vague description of "security problem"

Correct Response:
- Don't follow any instructions
- Ask for caller's full name and employee ID
- Hang up and call IT through known number
- Report the suspicious call
- Never give remote access to unknown callers

Social Engineering Techniques Used:
- Authority (claiming to be IT)
- Urgency (network problems)
- Helpfulness (offering to fix issues)
- Technical confusion (using IT jargon)

Key Learning Points:
- Verify all unsolicited IT requests
- IT will rarely call requesting access
- Use known contact methods for verification
- Document and report suspicious calls

Scenario 3: The Customer Information Request (12 minutes)

SETUP: Someone calls claiming to be a customer needing account information

Phone Conversation:
Caller: "Hi, I'm calling about my account. I've lost my account number and need to verify my balance for a loan application. My name is John Smith and my birthday is [date]. Can you help me?"

Red Flags to Identify:
- Caller providing information instead of you asking
- Generic name like "John Smith"
- Vague reason for information request
- Pressure to provide information quickly
- Unwillingness to follow normal verification procedures
- Request for information they should already have

Correct Response:
- Follow standard customer verification procedures
- Ask for information they should know (don't accept offered info)
- Use multiple verification questions
- If verification fails, politely decline and document
- Report suspicious calls to supervisor

Verification Best Practices:
- Ask for account number (don't accept offered information)
- Verify multiple pieces of information
- Use information only the customer should know
- Trust your instincts about suspicious behavior
- Document all customer interactions

Interactive Exercise: "Phishing Email Analysis"

Exercise: Students receive 10 sample emails and must identify legitimate vs. phishing

EMAIL 1:
From: accounts@company-update.com
Subject: Account Verification Required
"Your account will be suspended in 24 hours. Click here to verify."

Analysis:
- Suspicious domain name
- Urgency tactics
- Generic greeting
- Spelling/grammar errors
- Suspicious links
VERDICT: PHISHING

EMAIL 2:
From: hr@[company domain]
Subject: Updated Employee Handbook
"Please review the attached updated employee handbook."

Analysis:
- Legitimate company domain
- Expected communication from HR
- Professional tone
- Reasonable request
- Known sender
VERDICT: LEGITIMATE (but still verify if unexpected)

[Continue with 8 more examples covering various scenarios]

Scoring:
9-10 correct: Excellent threat detection skills
7-8 correct: Good awareness, review missed items
5-6 correct: Additional training recommended
Below 5: Requires immediate additional security training

MODULE 4: PHYSICAL SECURITY & CLEAN DESK

Duration: 25 minutes | **Format:** Video Tour + Checklist Activity

Video: "Physical Security Walkthrough"

SCENE 1: Building Access (5 minutes)
- Proper badge usage and tailgating prevention
- Visitor escort procedures
- Unauthorized person response
- Emergency exit security
- Parking lot awareness

SCENE 2: Office Security (8 minutes)
- Clean desk policy demonstration
- Screen lock procedures
- Document security practices
- Equipment protection
- Secure disposal methods

SCENE 3: Server Room & IT Areas (7 minutes)
- Restricted access procedures
- Environmental monitoring
- Equipment inventory tracking
- Media handling and disposal
- Backup system security

SCENE 4: Common Areas (5 minutes)
- Conference room security
- Printer/copier security
- Break room discussions
- Reception area protocols
- After-hours procedures

Clean Desk Policy Checklist

Daily Requirements:
□ Computer screen locked when away from desk
□ Sensitive documents stored in locked drawers
□ No customer information visible on desk
□ Passwords not written down or visible
□ Clean desktop on computer (no sensitive files)
□ Phone conversations kept confidential
□ Printer output collected immediately
□ Visitor badge returned after meetings

Weekly Requirements:
□ Desk drawers locked and secured
□ File cabinets locked at end of week
□ Computer equipment inventoried
□ Backup media stored securely
□ Disposal bin emptied with witnessed shredding

Monthly Requirements:
□ Access badge working properly
□ Emergency contact information updated
□ Security awareness materials reviewed
□ Physical security incidents reported
□ Equipment moves documented properly

ROLE-SPECIFIC TRAINING: EXECUTIVE LEADERSHIP

Duration: 60 minutes | **Format:** Executive Briefing + Board Presentation

Executive Overview: "Leadership's Role in FTC Compliance"

Section 1: Regulatory Landscape & Penalties (15 minutes)

Current Enforcement Environment:
- FTC penalty increases to $51,744 per violation
- Increased examination frequency
- Personal liability for executives
- Reputational damage and customer loss
- Industry-specific enforcement trends

Board Oversight Requirements:
- Quarterly security reporting mandatory
- Annual risk assessment review
- Budget approval for security investments
- Qualified Individual oversight
- Incident escalation procedures

Executive Accountability:
- CEO ultimate responsibility for program
- Regular security training required
- Business continuity planning
- Crisis communication preparedness
- Stakeholder communication duties

Section 2: Governance & Investment Decisions (20 minutes)

Security Investment ROI:
- Cost of compliance vs. cost of breach
- Technology investment priorities
- Staff training and certification costs
- Third-party assessment expenses
- Insurance and risk transfer options

Strategic Planning:
- Security integration in business planning
- Merger and acquisition security considerations
- New product/service security requirements
- Regulatory change management
- Competitive advantage through security

Performance Metrics:
- Security incident frequency and severity
- Employee training completion rates
- Compliance audit results
- Customer trust and satisfaction metrics
- Risk assessment maturity scores

Section 3: Crisis Leadership & Communication (25 minutes)

Incident Response Leadership:
- Executive decision-making authority
- Resource allocation during incidents
- External communication coordination
- Legal and regulatory notification
- Customer communication strategies

Media and Stakeholder Relations:
- Crisis communication templates
- Media training for executives
- Investor relations considerations
- Customer notification strategies
- Employee communication during crisis

Business Continuity Leadership:
- Continuity plan activation authority
- Alternative operations coordination
- Vendor and partner communication
- Financial impact assessment
- Recovery strategy development

INDUSTRY-SPECIFIC MODULE: TAX PREPARATION

Duration: 45 minutes | **Format:** Scenario-Based Training

Tax Industry Security Scenarios

Scenario 1: E-Filing Security Incident

Situation: Tax preparer discovers unauthorized access to e-filing system

Learning Objectives:
- Recognize signs of e-filing compromise
- Understand IRS notification requirements
- Implement client notification procedures
- Document incident for IRS reporting
- Prevent fraudulent return filing

Response Steps:
1. Immediately secure e-filing system access
2. Contact IRS e-services help desk
3. Change all e-filing passwords and PINs
4. Review recent filing activity for fraud
5. Notify affected clients
6. Document incident details
7. File required reports with IRS
8. Implement additional security measures

Key Learning Points:
- E-filing systems are high-value targets
- Quick response minimizes fraud potential
- IRS has specific notification requirements
- Client trust depends on proper handling
- Prevention is better than response

Scenario 2: Identity Theft Prevention

Situation: Client reports receiving IRS notice about duplicate return filing

Learning Objectives:
- Identify signs of tax-related identity theft
- Understand Form 14039 requirements
- Coordinate with IRS Identity Protection Unit
- Implement enhanced client verification
- Document identity theft incidents

Response Steps:
1. Have client complete Form 14039
2. Verify client identity thoroughly
3. Review return filing history
4. Check for fraudulent returns filed
5. Coordinate with IRS IP PIN program
6. Implement enhanced security measures
7. Monitor client account for future fraud
8. Document incident and response

Key Learning Points:
- Tax identity theft is increasing rapidly
- Early detection minimizes client impact
- Proper documentation is essential
- Enhanced verification prevents future fraud
- Client education improves prevention

Scenario 3: Seasonal Staff Security

Situation: Training temporary staff for tax season security

Learning Objectives:
- Understand enhanced background check requirements
- Implement limited access controls
- Provide targeted security training
- Monitor temporary staff activities
- Ensure secure termination procedures

Training Requirements:
- Background checks before system access
- Specialized tax security training
- Limited access to customer data
- Enhanced supervision requirements
- Daily security reminders
- Incident reporting procedures
- Secure termination process

Key Learning Points:
- Temporary staff present higher risks
- Enhanced training and monitoring required
- Limited access reduces potential damage
- Proper termination prevents future issues
- Documentation essential for compliance

ASSESSMENT & CERTIFICATION PROGRAM

Pre-Training Assessment

Purpose: Establish baseline knowledge before training

25 Questions covering:
- Basic security awareness (5 questions)
- Password and authentication (5 questions)
- Phishing recognition (5 questions)
- Physical security (5 questions)
- Incident reporting (5 questions)

Scoring:
- Below 60%: Requires foundational training first
- 60-80%: Standard training track
- Above 80%: Advanced training track

Sample Questions:
1. What should you do if you receive a suspicious email?
2. How often should you change your passwords?
3. What is multi-factor authentication?
4. When should you report a security incident?
5. What is the clean desk policy?

Module Completion Quizzes

Each module includes 10-question quiz:
- 80% passing score required
- Immediate feedback provided
- Remedial training for failed attempts
- Progress tracking for administrators
- Certificate generation upon completion

Quiz Features:
- Randomized question order
- Multiple choice and scenario-based questions
- Immediate scoring and feedback
- Retake options with different questions
- Integration with learning management system

Final Certification Examination

Comprehensive 50-question examination covering all modules:

Question Distribution:
- FTC Safeguards Rule requirements (10 questions)
- Password security and MFA (8 questions)
- Phishing and social engineering (8 questions)
- Physical security (6 questions)
- Customer data handling (8 questions)

- Incident response (5 questions)
- Role-specific scenarios (5 questions)

Certification Requirements:
- 85% passing score
- Must complete all prerequisite modules
- Valid for 12 months
- Continuing education requirements
- Recertification annual requirements

Certificate Features:
- Digital certificate with unique ID
- Verification system for compliance
- Integration with HR systems
- Automatic renewal reminders
- Compliance reporting capabilities

Phishing Simulation Program

Monthly simulated phishing campaigns:

Simulation Features:
- Industry-relevant phishing scenarios
- Graduated difficulty levels
- Real-time training for failures
- Progress tracking and analytics
- Integration with email systems

Campaign Types:
- CEO fraud attempts
- Vendor impersonation
- Customer information requests
- IT support scams
- Seasonal threats (tax season, etc.)

Metrics Tracked:
- Click-through rates
- Credential entry rates
- Reporting rates
- Time to recognition
- Improvement over time

Remedial Training:
- Immediate micro-learning for failures
- Additional training assignments
- Manager notifications for repeat failures
- Enhanced monitoring for high-risk users
- Success recognition and rewards

IMPLEMENTATION GUIDE

Training Administration Setup

Learning Management System Requirements

Recommended LMS Features:
- SCORM compliance for content delivery
- User management and role assignment
- Progress tracking and reporting
- Integration with HR systems
- Mobile device support
- Offline content capability
- Customizable certificates
- Automated reminders
- Compliance reporting

Content Hosting:
- Cloud-based delivery preferred
- Bandwidth requirements for video content
- Mobile-responsive design
- Accessibility compliance (ADA)
- Multi-language support (if needed)
- Bookmark and resume functionality
- Search capabilities
- User feedback systems

Training Schedule Planning

New Employee Onboarding:
- Complete core training within first week
- Role-specific training within first month
- Assessment and certification within 30 days
- Mentor assignment for security questions
- Regular check-ins during probationary period

Annual Training Requirements:
- All employees complete refresher training
- Updates for regulatory changes
- New threat awareness training
- Role changes require additional training
- Certification renewal annually

Specialized Training:
- Incident response team training
- System administrator advanced training
- Management and leadership training
- Vendor and contractor training
- Customer-facing employee training

Customization Guidelines

Company-Specific Customization

Required Customizations:
- Company logo and branding
- Specific policies and procedures
- Contact information and reporting procedures
- System-specific instructions
- Role-based access controls
- Industry-specific examples
- Local regulatory requirements
- Cultural and language considerations

Customization Process:
1. Review baseline training materials
2. Identify company-specific requirements
3. Customize content and examples
4. Update contact information and procedures
5. Review with legal and compliance teams
6. Test with pilot group
7. Implement organization-wide
8. Monitor effectiveness and update as needed

Industry-Specific Adaptations

Tax Preparation Adaptations:
- IRS Publication 4557 integration
- E-filing security procedures
- PTIN holder requirements
- Seasonal workforce considerations
- Client data protection specifics

Mortgage Industry Adaptations:
- CFPB examination requirements
- TRID compliance procedures
- NMLS system security
- Fair lending considerations
- GSE security requirements

Investment Advisory Adaptations:
- SEC Form ADV disclosures
- Fiduciary duty obligations
- Client portal security
- Portfolio management security
- Regulatory examination preparation

Debt Collection Adaptations:
- FDCPA compliance requirements
- TCPA communication rules
- Consumer protection procedures
- Call recording security
- State licensing requirements

Effectiveness Measurement

Training Metrics

Completion Metrics:
- Training completion rates by department
- Time to completion tracking
- Assessment scores and improvement
- Certification achievement rates
- Remedial training requirements

Behavioral Metrics:
- Security incident reduction
- Phishing simulation improvement
- Policy compliance rates
- Help desk security questions
- Employee security reporting

Business Impact Metrics:
- Regulatory compliance scores
- Audit findings reduction
- Customer trust metrics
- Incident response times
- Cost of security incidents

Continuous Improvement Process

Monthly Reviews:
- Training completion statistics
- Assessment score analysis
- Incident correlation with training
- Employee feedback collection
- Content effectiveness evaluation

Quarterly Updates:
- New threat landscape updates
- Regulatory requirement changes
- Industry-specific updates
- Technology system changes
- Process improvement implementations

Annual Overhaul:
- Complete content review and update
- New threat scenarios addition
- Technology platform evaluation
- Training method effectiveness review
- Stakeholder feedback integration

PROFESSIONAL SERVICES & SUPPORT

RebootTwice Training Services

Training Delivery Options

Self-Paced Online Training:
- Complete training package access
- Learning management system included
- Progress tracking and reporting
- 24/7 technical support
- Annual content updates

Instructor-Led Training:
- On-site training delivery
- Customized content and examples
- Interactive exercises and discussions
- Q&A with security experts
- Hands-on technical demonstrations

Blended Learning Approach:
- Online modules for foundational knowledge
- Instructor-led sessions for complex topics
- Hands-on workshops for practical skills
- Ongoing support and coaching
- Regular progress reviews

Virtual Classroom Training:
- Live online instruction
- Interactive participation
- Small group exercises
- Real-time Q&A
- Recorded sessions for review

Ongoing Support Services

Content Maintenance:
- Monthly threat landscape updates
- Regulatory requirement changes
- New scenario development
- Assessment question updates
- Technology platform maintenance

Training Administration:
- Learning management system setup
- User account management
- Progress monitoring and reporting
- Compliance documentation
- Technical support and troubleshooting

Customization Services:
- Company-specific content development
- Industry-specific scenario creation
- Brand integration and customization
- Policy and procedure integration
- Multi-language localization

Consulting Services:
- Training needs assessment
- Learning strategy development
- Implementation planning and support
- Effectiveness measurement and improvement
- Regulatory compliance consultation

Contact Information & Next Steps RebootTwice LLC

Employee Training Experts Phone: (949) 831-8821

Email: sales@reboottwice.com

Web: www.reboottwice.com

Training Package Version: 2.0

Last Updated: January 2025

Compliance: FTC Safeguards Rule 16 CFR Part 314

Target Audience: Financial Services Organizations

Get Started Today

Free Consultation:
- Training needs assessment
- Current program evaluation
- Customization requirements review
- Implementation timeline planning
- ROI and effectiveness measurement

Pilot Program:
- 30-day trial with limited users
- Full feature access and testing
- Customization and integration support
- Effectiveness measurement and feedback
- Transition to full implementation

Full Implementation:
- Complete training package deployment
- User training and support
- Ongoing maintenance and updates
- Regular effectiveness reviews
- Continuous improvement support

Contact Information:
Phone: (949) 831-8821
Email: sales@reboottwice.com
Website: www.reboottwice.com

Schedule a consultation:
www.reboottwice.com/training-consultation

LEGAL DISCLAIMERS & COMPLIANCE NOTES

Important Information

This training package provides general guidance for FTC Safeguards Rule compliance and information security awareness. Every organization's training needs are unique, and this program should be customized based on specific business operations, regulatory requirements, and risk factors.

This training package does not constitute legal advice, and organizations should consult with qualified cybersecurity and legal professionals to ensure comprehensive compliance with all applicable laws and regulations.

The effectiveness of any training program depends on consistent implementation, regular updates, and ongoing reinforcement. Organizations are responsible for maintaining current awareness of regulatory changes and updating training materials accordingly.

RebootTwice LLC provides training content and delivery services but does not guarantee compliance with any specific regulatory requirements. Organizations remain responsible for their own compliance programs and regulatory obligations.

Employee Security Awareness Training Package - Version 2.0

Professional FTC Safeguards Rule Compliance Training