Financial Institution Security Training provided by WRK Consulting

Introducing our newest resource at WRK!

Arturo Romero - A seasoned cybersecurity leader who plays a critical role in safeguarding organizations' digital assets and infrastructure. With deep expertise in risk management, threat intelligence, and security operations, he supports organizations in developing and executing comprehensive security strategies. Known for bridging technical insight with business priorities, they lead cross-functional teams, drives incident response readiness, and ensures compliance with evolving regulatory standards. Their leadership helps foster a culture of security awareness while enabling innovation and resilience across the organization. He has spent a number of years in both the private sector as well as the government side, providing great insight into what the cybersecurity landscape is and isn't.

Introducing our newest service at WRK!

Security Classes: Arturo will conduct remote class training with unlimited attendees via Teams. Base pricing includes 6 classes for $6,000.00. Each class will be 60 to 90 minutes depending on the topic. Classes over six can be scheduled at a reduced price.

1. Phishing Awareness
2. Social Engineering Awareness
3. Password Management and Authentication
4. Ransomware and Malware Prevention
5. Remote Work and Mobile Device Security
6. Data Protection and Confidentiality
7. Incident Reporting and Response
8. AI and Modern Social Engineering threats
9. Safe Social Media Usage and Behaviors
10. Physical Security Awareness
11. Insider threats and Data Handling

Arturo Remero Dave Ward Ed James



Below is our **practical, regulator-aligned overview of Security Awareness Training**. This training is useful for banks, credit unions, mortgage lenders, FinTechs, and investment firms.

1. Why Security Awareness Is Critical for Financial Institutions

Financial institutions are **high-value targets** because they handle:

- Customer PII and NPI (SSNs, account numbers, credit data)
- Payment systems (ACH, wire transfers, card networks)
- Market-sensitive and nonpublic financial information

Most breaches in financial services still start with **human error**:

- Phishing
- Business Email Compromise (BEC)
- Credential theft
- Mishandling customer data

Security awareness training is therefore both a **risk-reduction control** and a **regulatory expectation**, not just a best practice.

---

2. Regulatory & Compliance Drivers

Federal & Industry Requirements

- **GLBA Safeguards Rule** – Requires employee training to protect customer information
- **FFIEC IT Examination Handbook** – Emphasizes ongoing, role-based security training
- **NYDFS 23 NYCRR 500** – Mandates cybersecurity awareness training (for covered entities)
- **PCI DSS** – Requires security awareness for personnel handling card data
- **SEC / FINRA** – Cyber policies and supervisory controls for broker-dealers and advisors

---

3. Core Training Objectives

1. **Reduce successful phishing and social engineering**
2. **Protect customer financial data**
3. **Prevent fraud and wire/payment compromise**
4. **Ensure employees know how and when to report incidents**
5. **Demonstrate regulatory compliance**

---

4. Required Core Training Topics

4.1 Phishing & Social Engineering

- Email, SMS (smishing), and voice (vishing) attacks
- Realistic bank- and vendor-themed examples

- Red flags for spoofed executive and vendor emails
- Safe link and attachment handling

And **must-have** simulated phishing exercises.

4.2 Business Email Compromise (BEC) & Fraud

- Wire transfer and ACH fraud scenarios
- Vendor payment change scams
- Executive impersonation
- Dual-control and verification procedures

This is one of the **highest-loss attack types** for Fis.

4.3 Data Protection & Privacy

- Handling NPI and PII
- Secure document storage and disposal
- Emailing and sharing customer data securely
- Clean desk and screen-lock practices

Mapped to **GLBA Safeguards** expectations.

4.4 Passwords & Authentication

- Strong password practices
- Password managers (if approved)
- Multi-factor authentication (MFA)
- Credential reuse risks

4.5 Malware & Ransomware Awareness

- Malicious attachments and links
- Drive-by downloads
- Safe internet use on work devices
- Immediate steps if ransomware is suspected

4.6 Remote Work & Mobile Security

- Secure Wi-Fi usage
- VPN expectations
- Lost or stolen devices
- Mobile phishing

4.7 Incident Reporting

- What qualifies as a security incident
- How and where to report
- Why early reporting protects customers and the institution
- "No blame" reporting culture

---

5. Role-Based Training

- **Tellers & Branch Staff**
  - Social engineering
  - Customer impersonation attempts
  - In-branch fraud cues
- **Accounting / AP**
  - Wire fraud
  - Vendor change verification
  - Payment authorization controls
- **Executives**
  - CEO fraud
  - Targeted spear phishing
  - Decision-making during incidents
- **IT & Security**
  - Advanced threat recognition
  - Incident escalation
  - Secure configuration practices

---

6. Training Frequency & Structure

Minimum Recommended Baseline

- **Annual mandatory training** (all staff)
- **Quarterly phishing simulations**
- **Ongoing micro-training or reminders**
- **New-hire training within first 30 days**

Best-in-Class Programs

- Monthly microlearning (5–10 minutes)
- Adaptive phishing difficulty
- Just-in-time training after failed simulations

---

7. Measurement & Metrics

- Training completion rates
- Phishing clicks rates over time
- Reported Phishing Emails
- Repeat offenders vs. improvement
- Incident trends tied to training topics

Improvement over time is often more important than perfect results.

---

8. Documentation for Audits & FFIEC Exams

Maintain:

- Training policies and curriculum
- Attendance and completion logs
- Phishing simulation reports
- Evidence of management oversight
- Updates reflecting new threats

This documentation is frequently requested during:

- FFIEC exams
- Internal audits
- Vendor risk assessments
- Cyber insurance underwriting

---

9. Buy vs. Build Considerations

Use a Vendor When:

- You want FFIEC-aligned content
- You need automated phishing simulations
- You need reporting for exams

Build In-House When:

- You have a mature security team
- You want highly customized scenarios
- You can maintain content regularly

Most FIs use a **hybrid approach**.

---

10. What a "Good" Program Looks Like to Examiners

Examiners usually look for:

- Clear executive support
- Training that matches institutional risk
- Evidence employees understand threats
- Continuous improvement, not check-the-box training

If you'd like, we can:

- Create a **12-month training roadmap**
- Map training topics directly to **GLBA / FFIEC controls**
- Compare **security awareness vendors for banks/credit unions**
- Tailor this to **community banks vs. large FIs**
- Provide a **sample policy or exam-ready documentation checklist**

Just tell us how you plan to use it.

WRK will utilize Microsoft Teams to provide training input and delivery of results.

Monthly Security Awareness Training Program

Below is our **practical, exam-ready Monthly Security Awareness Training program** designed specifically for **financial institutions** (banks, credit unions, lenders, and fintechs). It aligns with **GLBA, FFIEC, PCI DSS, and NYDFS expectations** and is easy to run with minimal staff time.

For Financial Institutions:

Program Structure (What Works Best)

Each month includes:

- **5–10-minute training module** (video or interactive)
- **Targeted phishing simulation**
- **1–2 key takeaways** staff must remember
- **Metric to track** (for management and examiners)

This format prevents training fatigue while improving real behavior.

12-Month Security Training Calendar

January – Phishing Fundamentals

Focus:

- Identifying phishing, smishing, vishing
- Red flags: urgency, spoofed senders, fake links

Simulation

- Basic credential-harvesting email

Key Message

"If it pressures you or surprises you—verify first."

February – Business Email Compromise (BEC)

Focus:

- Wire fraud & ACH scams
- Executive impersonation
- Vendor payment change requests

Simulation:

- Fake CFO or vendor email requesting payment change

Key Message

“Money requests always require verification.”

March – Passwords & MFA

Focus:

- Strong passwords
- Password reuse risks
- MFA fatigue attacks

Simulation:

- Fake “password reset” phishing

Key Message

“Your password protects every system behind it.”

April – Customer Data Protection (GLBA)

Focus:

- Handling NPI and PII
- Secure email and file sharing
- Clean desk policy

Simulation:

- Email asking for customer info

Key Message: Customer data is our most valuable asset.”

May – Malware & Ransomware Awareness

Focus:

- Malicious attachments
- Drive-by downloads
- Early signs of ransomware

Simulation:

- ZIP or invoice attachment lure

Key Message

"One click can stop the bank—or protect it."

June – Secure Remote & Mobile Work

Focus:

- Home Wi-Fi security
- VPN usage
- Lost or stolen devices

Simulation:

- Fake Wi-Fi or travel-related phishing

Key Message

"Remote work = same security expectations."

July – Social Engineering Beyond Email

Focus:

Phone scams (vishing)

- In-person tailgating
- Impersonation attempts

Simulation:

- Voicemail-themed phishing email

Key Message

“Attackers exploit helpfulness.”

August – Payment & ACH Fraud

Focus:

- Red flags in payment requests
- Changes to standing instructions
- Dual-control procedures

Simulation:

- Vendor banking change request

Key Message

“Pause, verify, and document.”

September – Incident Recognition & Reporting

Focus:

- What is a security incident?
- How and when to report
- No-blame culture

Simulation:

- Obvious phishing to measure reporting

Key Message

“Early reporting limits damage.”

October – Cybersecurity Month (Expanded)

Focus:

- Threat trends in financial services
- Real breach case studies
- Review of year-to-date lessons

Simulation:

- Spear-phishing email tailored to the institution

Key Message

"Cybersecurity is everyone's job."

November – Executive & Privileged User Awareness

Focus:

- Spear phishing
- Targeted attacks on leadership
- Approval abuse

Simulation:

- Executive-only phishing campaign

Key Message

"Authority increases attacker interest."

December – Year-End & Holiday Threats

Focus:

- Holiday phishing scams
- Donation fraud
- Out-of-office risks

Simulation:

- Shipping or bonus-related phishing

Key Message

"Attackers know when we're distracted."

Metrics to Track Monthly (Audit & FFIEC Exam-Friendly)

Track and retain:

- Training completion %
- Phishing click rate
- Reporting rate
- Repeat offenders
- Improvement trends

FFIEC examiners prefer **demonstrated improvement**, not zero failures.

How FFIEC Examiners View This Program

This structure demonstrates:

✅ Ongoing training (not annual-only)
✅ Risk-based content
✅ Fraud and payments focus
✅ Management oversight
✅ Measurable effectiveness

Optional Training Enhancements

- Role-based modules (tellers, AP, executives)
- Just-in-time training after phishing failures
- Monthly security awareness email from leadership
- Annual tabletop exercise