Skill to Mastery Tracking in 1View:

Summary

Phishing Awareness Training & Mastery Framework

This framework delivers a comprehensive, neuroscience informed, and data driven approach to training learners on cybersecurity. It integrates Bloom's Taxonomy, Webb's Depth of Knowledge (DOK), Node Science, and neuroscience principles to build a scalable, measurable, and mastery-focused learning experience.

Core Objectives

Equip learners with the knowledge and skills to identify and respond to phishing threats.

Track learner engagement, progression, and mastery using a structured point-based system.

Reduce organizational risk by correlating mastery with an increase of resiliency to phishing attacks.

Instructional Design Highlights

Bloom's Taxonomy (learning progression)

- Bloom's Taxonomy guid_es the learning arc: from remembering to creating.

Webb's Depth of Knowledge (DOK) (assessment rigor)

- Webb's DOK weights assessments by cognitive rigor, ensuring meaningful progression.

Node Science (networked learning)

- Node Science fosters networked learning through diverse content sources and peer collaboration.
- Rule of 27 (touchpoint-based mastery tracking)

Neuroscience (memory and mastery)

- Neuroscience principles (spaced repetition, active recall, encoding) ensure long-term retention and skill transfer.

Mastery Tracking System

Learners earn 1–4 points per activity based on DOK level.

27 points signify mastery, triggering a final simulation-based assessment.

Progress is tracked by individual, department, and organization, enabling benchmarking and risk analysis.

Mastery data is used to correlate training effectiveness with real-world phishing resilience.

Reinforcement & Retention

Content is revisited at strategic intervals (Days 1, 3, 7, 14, 21, 28).

Learners engage in multi-modal activities tailored to visual, auditory, and kinesthetic styles.

Simulations, microlearning nudges, and gamified reviews reinforce learning.

Outcome

This framework not only builds phishing awareness but also creates a measurable path from knowledge to skill to mastery, empowering organizations to proactively reduce cybersecurity risks through targeted education.

Unified Learning & Mastery Tracking Framework

Learning Architecture

Instructional Flow (Bloom's Taxonomy)

Step 1: Instruction (video, reading, discussion)

Step 2: Homework (scenario analysis, peer discussion)

Step 3: Assessment (quiz, simulation)

Step 4: Reassessment (if mastery not achieved)

Step 5: Progression (if mastery achieved)

Assessment Weighting (Webb's DOK)

Assign point values based on cognitive depth:

DOK 1 (e.g., video, infographic, awareness newsletter): 1 point

DOK 2 (e.g., CBT or video that includes a quiz): 2 points

DOK 3 (e.g., Simulation, Choose Your Own Adventure with multiple path outcome): 3 points

DOK 4 (e.g., Game or Level 4 Training, Build your own): 4 points

Commented [1]: Not a model we offer now, but might be an idea for the future - Build your own infographic - the Company can pick on a quarter and use it in the break room - giving staff by in and a culture around CSA.

Neuroscience-Based Timing

Short to Long-Term Memory: Use dual coding (visual + verbal), retrieval practice, and elaboration to strengthen encoding.

Overcoming Forgetting Curve: Apply spaced repetition (e.g., Day 1, 3, 7, 14, 21, 28) and interleaved practice (mixing phishing with other cyber threats).

Active recall: Use quizzes and peer teaching

Encoding: Use multi-modal content (visual, auditory, kinesthetic)

Consolidation: Reinforce with sleep cycles and reflection

Node Science Integration

Learners connect to multiple nodes: experts, peers, tools, simulations

Encourage networked learning: forums, Slack channels, leaderboards

Use peer feedback and collaborative creation to deepen understanding, creating a culture of reporting and socializing the material amongst staff.

Mastery Tracking System: Rule of 27

Touchpoint-Based Mastery

Each content piece or activity earns 1–4 points based on DOK level for each topic and tactic.

Learners must accumulate 27 points across varied activities to unlock a mastery level training path.

Simulation acts as a mastery check.

Tracking Dimensions

By Learner: Individual progress toward 27-point mastery on a topic or tactic (e.g. Credential Phishing)

By Department: Average mastery score and simulation pass rate

By Organization: Benchmarking across teams and time

Over Time: Correlate mastery with increase in reporting rates and resiliency score across the organization to phishing attacks.

Workflow Example

Phase	Activity	Bloom's Level	DOK	Points	Tool	Revisit
1	Watch a video	Remembering	DOK 1	1	LMS	Day 3
2	Quick Tip CBT	Understanding	DOK 2	2	LMS	Day 7
3	Analyze phishing case study	Analyzing	DOK 3	3	LMS	Day 14
4	Complete phishing simulation	Creating	DOK 3	3	PhishMe	Day 21
5	Level 4 Game	Creating	DOK 4	4	LMS	Day 28

Commented [2]: Not a model we offer now - but an interesting concept. We offer pieces of this but I think we can expand further.

Reporting & Insights

Dashboard: Visualize learner progress toward 27 points

Alerts: Flag learners who stall or regress

Comparative Analytics: Benchmark mastery across roles, teams, and time

Risk Reduction: Track phishing susceptibility pre- and post-training

Topics and Tactics

- Topics
- Brand Impersonation
- Compliance
- Emotions
- Financial Transactions
- General Phishing
- Generic Cloud
- Mobile
- News and Events
- Office Communications
- Passwords
- Reporting
- Safe Web Browsing
- Shipment & Deliveries
- Small/Medium Businesses
- Social Media
- Spear Phishing
- Advanced Topics
- Data Breach
- Malware
- MFA
- Personal Security
- Physical Security
- Ransomware
- SEG
- Shared File
- Tactics
- Attachment Phish
- BEC/CEO Fraud
- Credential Phish
- QR Codes
- URL Phish

Formatted: Indent: Left: 0.25", No bullets or numbering

Learning Types and Points

Type	DOK Level	Points
Awareness Newsletter	0	1
Benchmark	3	3
CBT	1 or 2	2
Email Template	3	3
Game	4	4
Infographic	0	1
Job Aid	0	1
SEG Miss	3	3
Video	0	1
Choose Your Phish	3	3

Sample of Knowledge/Skill/Mastery Tracking

Topic	Activity	Type	Time	Interval	Points
Credential Phishing	The War of the Worlds - A Tale of Stolen Credentials	Awareness Newsletter	5 min read	Day 1	1
Credential Phishing	Quick Tip Card via Slack	Job Aid	< 1 min read	Day 2	1
Credential Phishing	Cybersecurity Awareness – Credential Phishing	CBT	5 min read	Day 4	2
Credential Phishing	Credit Distribution	SEG Miss	< 1 min read	Day 5	3
Credential Phishing	Formula Phish	HTML Education	3 min read	Day 7	1
Credential Phishing	CYP Credential Phishing	Choose Your Phish	5 min read	Day 14	3
Credential Phishing	Credential Phishing	Video	1 min	Day 16	1
Credential Phishing	Urgent Payment	SEG Miss	< 1 min read	Day 17	3
Credential Phishing	Quick Tip Card via Slack	Job Aid	< 1 min read	Day 20	1
Credential Phishing	Sherlock	Game	10 min	Day 21	4
Credential Phishing	Dropbox Credential Phishing	Video	1 min	Day 25	1
Credential Phishing	Hooked on Phish – Credential Phishing	Infographic	2 min read	Day 27	1
Credential Phishing	MS Login	SEG Miss	< 1 min read	Day 30	3
Credential Phishing	Credential Phishing	Podcast Reel	1 min	Day 34	1

Commented [3]: Eventually build playbooks that have the same look and feel - much like we do for CAM

Commented [4]: Can we add 2 points for clicking the reporter button

Credential Phishing	Cyber Safe Lesson – Credential Phishing	Video	1 minute	Day 37	1
		Total Time	39 minutes	Total Points	27

BACKGROUND

Gamified review: Kahoot or leaderboard challenges

Learning Theory Framework: 3 Styles × 3 Ways × 3 Times

◇ 3 Learning Styles (Based on VARK Model)

1. **Visual** – Learners prefer images, diagrams, and spatial understanding.
2. **Auditory** – Learners absorb information through listening and speaking.
3. **Kinesthetic** – Learners learn best through hands-on activities and movement.

◇ 3 Ways to Teach Each Style

Each learning style is addressed using three different instructional methods:

Style	Way 1	Way 2	Way 3
Visual	Infographics	Slide decks with icons	Concept maps
Auditory	Podcasts or lectures	Group discussions	Mnemonic songs

Style	Way 1	Way 2	Way 3
Kinesthetic	Simulations	Role-playing	Interactive labs

◇ 3 Times for Reinforcement

To move learning from **short-term to long-term memory** and overcome the **forgetting curve**, content is revisited:

1. **Initial Exposure** – Introduction of concept.
2. **Reinforcement** – Within 24–48 hours (retrieval practice).
3. **Mastery Check** – After 7–10 days (spaced repetition).

Neuroscience Integration

- **Encoding**: Multi-modal input strengthens neural pathways.
- **Consolidation**: Repetition and sleep help stabilize memory.
- **Retrieval Practice**: Strengthens recall and builds mastery.
- **Spacing Effect**: Revisiting material over time improves retention.

Node Science-Based Training Plan: Phishing Awareness

◇ Core Principle

Learning occurs through connecting to diverse **nodes** (sources of knowledge), including people, digital tools, communities, and experiences. Learners are **active participants** in a networked environment.

Training Structure

Phase	Objective	Node Types	Activities	Tools	Duration
1. **Connect**	Introduce phishing concepts	Expert videos, articles, LMS	Watch explainer videos, read blog posts	PhishMe, LMS	30–45 min
2. **Explore**	Discover real-world examples	News sites, forums, peers	Analyze phishing case studies, discuss in forums	Cybersecurity blogs	60 min
3. **Interact**	Apply knowledge in context	Simulations, mentors, peers	Identify phishing emails in sandbox inbox	PhishMe, LMS	45 min
4. **Reflect**	Evaluate and share learning	Peer feedback, journaling	Write a reflection or critique of a phishing attempt	LMS	30 min

Phase	Objective	Node Types	Activities	Tools	Duration
5. **Create**	Build awareness	Team collaboration, design tools	Design a phishing awareness poster or video	LMS	60–90 min

---