

CAM 2026 Delivery Flow

When to release each of the 12 assets across the 4-week program: the day, the order, and the channel.

WHY THIS FLOW WORKS

Every week follows the same **Learn → See → Practice** rhythm across three assets: a core lesson, a supporting infographic, and a hands-on activity. Space delivery across the week so employees have time to engage with each asset before the next one lands.

BEFORE YOU LAUNCH

Getting started

Download your 12 assets

Everything for the campaign lives in one place.

Download them here →

- ✓ Map the channels you're using to communicate: **email/LMS**/chat/intranet channel (Teams, Slack, or intranet).

✓ Start every **Monday**, so users will get used to the cadence.

✓ Send a **launch announcement** (template below) the Friday before Week 1.
- ✓ Upload the **four core modules (SCORM)** to your LMS and test playback before launch.

✓ Brief managers so they can **reinforce each week** in team meetings.

✓ Decide who **tracks completion** each week and where results are recorded.

Launch announcement template

Send the Friday before Week 1

SUBJECT

This October, we're getting ahead of AI-powered scams

Hi team. This month we're running a four-week Cybersecurity Awareness campaign built for the most current threats that surround companies like ours: AI impersonation, evolved phishing, identity attacks, and the risks of everyday AI tools. Each week you'll get one short lesson plus a follow-up. Watch your inbox every **Monday**. Let's invest time in achieving a stronger, safer work environment.

WEEK 01LEARN → SEE → PRACTICE3 assets

AI-Powered Deception

Why it matters. Deepfake video, cloned voices, and AI-written phishing are now cheap, fast, and convincing enough to fool trained employees. This week resets what "proof" means. Seeing and hearing are no longer enough.

Mon
LEARN

VIDEO
When AI Pretends to Be Human
Deliver via **Email + LMS**

Wed
SEE

INFOGRAPHIC
How AI Scams Manipulate You
Deliver via **Intranet / Teams / Slack**

Fri
PRACTICE

INTERACTIVE MODULE
Spot the Manipulation
Deliver via **LMS / team huddle**

ANNOUNCE IT

"This week we're looking at how AI is being used to impersonate people we trust. Start with the short module in your inbox. Five minutes that will change how you read your next 'urgent' message."

RECOMMENDED ACTION

Run "Spot the Manipulation" live in a Friday team huddle and compare answers as a group.

WEEK 02LEARN → SEE → PRACTICE3 assets

Evolution of Phishing

Why it matters. Phishing no longer lives only in suspicious emails. Attacks now arrive through QR codes, chat platforms, fake MFA prompts, and lookalike browser pages, the channels most training never covered.

Mon
LEARN

VIDEO
Modern Phishing: Beyond Suspicious Emails
Deliver via **Email + LMS**

Wed
SEE

INFOGRAPHIC
Modern Phishing at a Glance
Deliver via **Intranet / Teams / Slack**

Fri
PRACTICE

INTERACTIVE MODULE
Spot the Phish: How Attackers Really Get In
Deliver via **LMS / team huddle**

ANNOUNCE IT

"Phishing has moved beyond the inbox. This week's module shows the newer traps (QR codes, chat links, and fake login pages) and how to slow down before you click, scan, or approve."

RECOMMENDED ACTION

Run "Spot the Phish" as a Friday team activity, and ask managers to share one real suspicious message their team received.

WEEK 03LEARN → SEE → PRACTICE3 assets

Identity and Login Risk

Why it matters. Attackers don't break in anymore. They log in. Every MFA prompt and access approval an employee taps is now a security decision.

Mon
LEARN

VIDEO
MFA Manipulation: Pause Before You Approve
Deliver via **Email + LMS**

Wed
SEE

INFOGRAPHIC
Your Login Is the Target
Deliver via **Intranet / Teams / Slack**

Fri
PRACTICE

INTERACTIVE MODULE
Would You Approve This?
Deliver via **LMS / team huddle**

ANNOUNCE IT

"Your login is the new front door. This week covers why attackers target identities, and why that unexpected MFA prompt deserves a second look before you tap approve."

RECOMMENDED ACTION

Remind employees exactly how to report an unexpected MFA prompt through your normal security channel.

WEEK 04LEARN → SEE → PRACTICE3 assets

Shadow AI & Data Leakage

Why it matters. Employees paste sensitive data into AI tools with good intentions and no sense of risk. This week makes the invisible visible, and gives people a simple rule for what's safe to share.

Mon
LEARN

VIDEO
What Happens When Sensitive Data Enters AI Tools?
Deliver via **Email + LMS**

Wed
SEE

INFOGRAPHIC
Safe AI Usage at Work
Deliver via **Intranet / Teams / Slack**

Fri
PRACTICE

INTERACTIVE MODULE
Should You Upload This?
Deliver via **LMS / team activity**

ANNOUNCE IT

"AI tools are everywhere now, and so is the risk of oversharing. This week closes the campaign with one question to ask before you paste anything into an AI tool: should this data leave the building?"

RECOMMENDED ACTION

Post the "Safe AI Usage at Work" infographic where people actually work: your AI-tools channel or pinned in Teams/Slack.

AFTER THE CAMPAIGN

Measure what changed

Two simple reads tell you whether the month worked: how people **feel**, and what they **do**.

Team feedback

Run a short pulse (1–2 questions) after Week 2 and at wrap-up. For example, "Do you feel more confident spotting AI-powered scams?" Add a quick manager read from team meetings.

Behavior, before & after

Compare a baseline from before October to the weeks after: phishing-report rate, simulation click-through, unexpected-MFA reports, and weekly module completion. Rising reports and falling clicks are the signal that behavior is shifting.

Track completion **weekly, not just at the end**, so you can nudge quieter teams mid-campaign.

THE WHOLE PLAN IN ONE LOOK

At-a-glance delivery calendar

Week	Monday	Mid-week · Wed / Thu	Friday
1	Video	Infographic	Interactive Module
2	Video	Infographic	Interactive Module
3	Video	Infographic	Interactive Module
4	Video	Infographic	Interactive Module

Questions about your rollout?

We're here to help you run October well.

marketing@right-hand.ai →