

TECH & AI CASE STUDY - REGIONAL BANK - 2026

Security Awareness That Cut Phishing Clicks From 11% to 2.4% at a Regional Bank

Based on a delivery engagement with CedarRun Bank

11% to 2.4%
PHISHING CLICK RATE

6x
SUSPICIOUS-EMAIL REPORTING

45 min to 9 min
MEDIAN TIME TO REPORT

zero
EXAMINATION FINDINGS

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the CedarRun Bank case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME		ROLE	
COMPANY		TEAM / DEPARTMENT	
DATE		EMAIL (OPTIONAL)	

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at CedarRun Bank - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

CedarRun Bank is a community lender with 1,100 employees across 42 branches, serving consumers and small businesses with deposit, lending and treasury services. Its workforce is a mixture of branch staff, loan officers, back-office operations and a treasury team that moves large sums on instructions that arrive, more often than not, by email. The bank's technology footprint is typical of regional banking: a core processing platform, online and mobile banking, merchant services, and a heavy dependence on email as the connective tissue between employees, customers and counterparties.

Banking is also a business where the human factor is the attack surface. Attackers do not need to defeat CedarRun's firewalls when they can convince a treasury analyst that a legitimate vendor changed its banking details, or persuade a branch employee that a fraud investigator urgently needs account credentials. The bank's fraud team tracked attempted business email compromise against the treasury function as it grew more convincing each quarter, and the state banking regulator's examination framework had begun scrutinizing human-factor controls with increasing specificity. CedarRun's security leadership knew the awareness program they had was not the one the environment required.

02 Where Things Stood

The measurable symptom was a simulated phishing click rate hovering at 11% across the bank — one in nine employees clicking malicious links in every test campaign. Behind that number sat a training model that could not produce better results: security awareness consisted of an annual compliance video that employees clicked through at their desks, usually while doing something else, followed by an attestation recorded for the examination file. Training was an attendance exercise measured once a year; behavior was never measured at all.

The consequences concentrated where the money was. Business email compromise attempts against the treasury team grew more sophisticated with every passing quarter — spoofed vendor domains, hijacked email threads, and wire-change requests that mimicked the bank's own procedures. The fraud team estimated that a single successful invoice-fraud or wire-redirect attack could cost \$500,000 or more before recovery, and the FBI's Internet Crime Complaint Center reportedly logged roughly \$2.9 billion in business email compromise losses from US victims in 2023, so the threat was hardly hypothetical. The Verizon Data Breach Investigations Report found that users click malicious links a median of just 21 seconds after opening a phishing email, which meant any defense that relied on employees pausing to scrutinize messages needed to be trained into reflexes, not delivered through an annual video.

The bank also lacked the machinery to see its own exposure. There was no reliable way for an employee to report a suspicious email — the process involved forwarding to an address nobody remembered — and no data on how long suspicious messages circulated before someone acted. When the regulator's examiners asked for evidence about human-factor controls, the bank could produce attendance records for a video, which is precisely the kind of evidence that invites deeper questions rather than closing them.

03 The Challenge

The challenge was to change the daily behavior of 1,100 employees across 42 branches — a population that includes tellers handling a lobby queue, lenders working from client sites and treasury staff processing wires under time pressure — and to prove the change with data a banking regulator would accept. Behavior change at that scale cannot be mandated into existence; it has to be engineered, with the same discipline applied to any product: short feedback loops, visible metrics and an experience employees do not resent.

The program also had to succeed without villainizing its audience. The fastest way to kill a phishing awareness program is to punish the people who click, because punished employees hide their clicks and stop reporting genuine mistakes — exactly the opposite of the goal. Security wanted a program that measured behavior monthly rather than attendance once a year, which meant the bank needed instrumentation it did not have: simulation infrastructure, one-click reporting inside the mail client, a data pipeline into the BI tool leadership already read, and a coaching model that turned every click into a three-minute lesson rather than a disciplinary event. KnowBe4's industry benchmarking reportedly finds average phish-prone rates falling from over 30% at baseline to under 5% after twelve months of continuous training — evidence that the target was achievable, but only through continuity, not campaigns.

04 Discovery and Diagnosis

Emerson Technology began with a four-week diagnostic that combined a baseline simulation across all staff with interviews across branches, treasury and the fraud team. The baseline was measured before any program announcement, so the 11% click rate was an honest number rather than a post-policy artifact, and it gave leadership a concrete metric to fund the program against. The diagnostic also examined what happened after a click: currently, nothing — no coaching, no data, no feedback loop of any kind.

Interviews surfaced the friction points that any design had to remove. Reporting a suspicious email took a minute and required remembering an address, so nobody did it; there was therefore no early-warning signal, and the median time for a suspicious message to be flagged — when it was flagged at all — was 45 minutes, long after colleagues had opened it. The fraud team was a latent asset: they saw live scam attempts constantly, but nothing connected their knowledge to the training the rest of the bank received. The technical layer had gaps too — no DMARC enforcement and no monitoring for lookalike domains — which meant the easiest attacks required no human failure at all. The final design layered four components over twelve months, each one addressing a specific diagnosed failure: simulations, reporting with instant feedback, just-in-time coaching and an executive dashboard, with DMARC and domain monitoring closing the technical side.

05 The Solution

The program ran on a twelve-month rhythm with four reinforcing components, designed so that each month's data shaped the next month's campaign.

Simulations that scale with resilience

Realistic simulations scaled from obvious templates to targeted lures that imitated the bank's own payroll and wire processes, with difficulty rising as click rates fell. Difficulty tracked the trend, not the calendar: when a department's click rate dropped below threshold, its next campaign got harder, so the program kept pace with the bank's improving reflexes instead of plateauing. The fraud team fed live scam examples into next month's scenarios — real BEC attempts against treasury, real vendor-impersonation emails — so simulations rehearsed the attacks CedarRun actually faced rather than generic templates. Employees experienced a curriculum that recognized them, which was visible in how seriously the harder lures were taken.

Reporting and instant coaching

One-click reporting landed directly in the mail client, and every report triggered immediate automated feedback: a praise message for true positives and a quiet teaching moment for false ones. Reporting took under five seconds, which converted the bank's most vigilant employees from private skeptics into a distributed sensor network. Just-in-time micro-training of three to five minutes replaced hour-long modules, delivered within minutes of a risky click rather than months later at compliance time. Training delivered weeks later changes policy documents, not day-to-day behavior; training delivered while the moment is memorable changes reflexes. The no-blame framing was explicit and enforced — clicks triggered coaching, never discipline — which kept reporting flowing and stopped the hiding behavior that punishes programs create.

The executive dashboard and the technical net

A monthly executive dashboard in the bank's existing BI tool tracked click rate, report rate and time-to-report by department. Departments competed, laggards got targeted coaching rather than blanket scolding, and because the dashboard lived where leaders already read, the metric survived budget season. In parallel, the technical gaps the simulations kept exposing were closed the same quarter: DMARC enforcement cut direct spoofing of the bank's domains, and lookalike-domain monitoring flagged attacker infrastructure before campaigns landed. Training and technology advanced together instead of pointing at each other's failures.

06 The First 90 Days

Month one was the honest baseline and the infrastructure build: the unannounced baseline simulation produced the 11% number, the one-click reporting button deployed to every mailbox, and the automated feedback flows were tested against real reports from a pilot group of treasury and branch managers. Month two launched the first announced campaign — deliberately moderate in difficulty — alongside the first monthly dashboard, and the reporting rate tripled within weeks as employees discovered that reporting produced appreciation rather than bureaucracy. The coaching engine went live, delivering its first three-minute lessons within minutes of clicks. Month three brought the first difficulty escalation for departments that had cleared the threshold, the fraud team's first live-scam-derived scenario, and the start of DMARC enforcement in monitor mode ahead of full policy. The dashboard added time-to-report as a headline metric once the data supported it, and the security team's weekly review shifted from campaign logistics to coaching targeted at the two departments with the weakest trends. By day 90 the program had its first proof of behavioral change: a branch employee reported a genuine credential-harvesting email within four minutes of receiving it, the security team pulled the message before colleagues opened it, and the incident was written up in the monthly dashboard as the new normal rather than a lucky catch.

07 The Results

Click rates fell from 11% to 2.4% within a year, while voluntary reporting of suspicious email rose sixfold as reporting became routine. Median time-to-report dropped from 45 minutes to 9, giving the security team time to pull messages before colleagues opened them. The regulator's next examination closed the security-awareness line of inquiry with zero findings, and treasury flagged two live wire-fraud attempts that simulations had trained them to recognize. The program now costs less per employee than the annual video it replaced.

METRIC	BEFORE	AFTER
Phishing click rate	11%	2.4%
Suspicious-email reporting	-	6x
Median time to report	45 min	9 min

METRIC	BEFORE	AFTER
Examination findings	-	zero

The cultural result is the one the numbers only hint at. Reporting suspicious email became ordinary behavior at every level of the bank, from tellers to treasury, and the sixfold increase in reports continued even as lures became harder — the signature of genuine vigilance rather than click-shyness. The security team's relationship with the workforce shifted from enforcement to coaching, and department leaders began asking for their metrics instead of waiting to be told. Two live wire-fraud attempts stopped by trained treasury staff paid for the program many times over, and the examination evidence file now builds itself from monthly data instead of being assembled the week before an examiner arrives.

08 What Your Business Should Do

The CedarRun program is replicable at almost any scale, and its lessons begin before the first simulation is sent. Baseline your click rate first — run a measured simulation across all staff before announcing any program or policy change, because a baseline number makes improvement visible and gives leadership a concrete metric to fund. Scale difficulty with resilience: start with obvious templates, then advance to lures imitating your own payroll, invoice and wire processes, with difficulty tracking the click-rate trend rather than a calendar. Put one-click reporting in the mail client so every report takes under five seconds and triggers immediate automated feedback — reward true positives publicly and teach quietly on false ones to keep the habit flowing. Coach within minutes of a click, delivering three-to-five-minute micro-training immediately while the moment is still memorable, because training delivered weeks later changes policy documents, not behavior.

Report by department to executives monthly, tracking click rate, report rate and time-to-report in a dashboard leaders already read; departments compete, laggards get targeted coaching, and the metric survives budget season. Feed real scam attempts into your scenarios by forwarding live BEC and fraud attempts to the awareness team each month, since scenarios built from real attacks against your organization land harder than generic templates. Close technical gaps alongside training — enforce DMARC, monitor lookalike domains and add external-sender banners, fixing in the same quarter whatever the simulations expose rather than letting it sit on a someday backlog. Finally, measure reporting rate, not just clicks: a falling click rate with flat reporting may mean staff are just click-shy rather than vigilant, while healthy programs show rising report rates even as lures become more convincing. Put these eight steps to work with the action checklist in this practice book, and use the reflection questions as the agenda for your quarterly program review: what is your measured click rate today, how many seconds does reporting take in your mail client, and when your regulator or examiner last reviewed human-factor controls, what evidence could you actually produce?

REAL-WORLD PROOF & BENCHMARKS

The 2024 Verizon Data Breach Investigations Report finds users click malicious links a median of just 21 seconds after opening a phishing email. - Verizon DBIR, 2024

The FBI's Internet Crime Complaint Center reportedly logged roughly \$2.9 billion in business email compromise losses from US victims in 2023. - FBI IC3, 2023

KnowBe4's industry benchmarking reportedly finds average phish-prone rates fall from over 30% at baseline to under 5% after twelve months of continuous training. - KnowBe4 benchmark, 2024

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐
1. Baseline your click rate first

Run a measured simulation across all staff before announcing any program or policy change. A baseline number makes improvement visible and gives leadership a concrete metric to fund.

OWNER

TARGET DATE

STATUS

--	--	--

☐
2. Scale difficulty with resilience

Start with obvious templates, then advance to lures imitating your own payroll, invoice and wire processes. Difficulty should track the click-rate trend, not a calendar.

OWNER

TARGET DATE

STATUS

--	--	--

☐
3. Put one-click reporting in the mail client

Every report should take under five seconds and trigger immediate automated feedback. Reward true positives publicly and teach quietly on false ones to keep the reporting habit flowing.

OWNER

TARGET DATE

STATUS

--	--	--

☐
4. Coach within minutes of a click

Deliver short, three-to-five-minute micro-training immediately after a risky click while the moment is still memorable. Training delivered weeks later changes policy documents, not day-to-day behavior.

OWNER

TARGET DATE

STATUS

--	--	--

☐
5. Report by department to executives monthly

Track click rate, report rate and time-to-report in a dashboard that leaders already read. Departments compete, laggards get targeted coaching, and the metric survives budget season every year.

OWNER

TARGET DATE

STATUS

--	--	--

**6. Feed real scam attempts into scenarios**

Forward live BEC and fraud attempts to the awareness team each month. Scenarios built from real attacks against your organization land harder than generic templates.

OWNER

TARGET DATE

STATUS

--	--	--

**7. Close technical gaps alongside training**

Enforce DMARC, monitor lookalike domains and add external-sender banners. Simulations expose which technical controls are missing, so fix them the same quarter rather than on a someday backlog.

OWNER

TARGET DATE

STATUS

--	--	--

**8. Measure reporting rate, not just clicks**

A falling click rate with flat reporting may mean staff are just click-shy, not vigilant. Healthy programs show rising report rates even as the lures become increasingly convincing.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1	PRIORITY 2	PRIORITY 3
NUMBER IT SHOULD MOVE	NUMBER IT SHOULD MOVE	NUMBER IT SHOULD MOVE

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. What is your organization's measured phishing click rate today — and when did anyone actually measure it?

Q2. If a treasury employee received a convincing wire-fraud email tomorrow, would they report it or act on it?

Q3. How many seconds does reporting a suspicious email take in your mail client right now?

Q4. Does your awareness program teach within minutes of a mistake, or months later at annual compliance time?

Q5. Which departments see phishing metrics in a dashboard they already read, and which never see them at all?

Q6. When your regulator or examiner last reviewed human-factor controls, what evidence could you actually produce?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Days 31-60 Focus: build and prove

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like CedarRun Bank's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact