



AI & Security Training

Self-serve portal and in-person workshops that make AI and security skills stick.

SERVICE PACKAGE

September 2026

fletchlabs.ca • info@fletchlabs.ca • Cambridge, Ontario, Canada

Executive summary

AI has changed both the attacks your team faces and the skills it needs to face them. Fletch Labs delivers AI and security training that leads with the AI era (safe use of AI assistants, prompt injection and AI data-leakage awareness, and AI-era social engineering), then backs it with the fundamentals that still carry the load: phishing, credential hygiene, MFA, and incident reporting. Content reaches your team through a self-serve training portal and in-person workshops, and it is measured: the goal is demonstrable reduction in human-factor risk, not a compliance checkbox.

The human element is the biggest weakness

Three data points make the case for ongoing, measured training:

Human first

The 2026 Verizon Data Breach Investigations Report finds the most common causes of breaches continue to heavily involve the human element: social engineering, phishing, and stolen credentials.¹

Mobile shift

The same report documents higher click rates on mobile phishing than email: as people got better at spotting phishing emails, attackers moved to texts and calls, channels most awareness programs never cover.¹

Training works

Industry benchmarking across 13.2 million users and 31,000 organizations shows a measurable, sustained drop in phish-prone rates from baseline through 90 days and one year of ongoing security awareness training.²

The lesson is twofold: education is crucial, and one-off education is not enough. Threats shift channels and tactics; the training has to keep pace and prove that behavior is actually changing.

The curriculum

Content leads with the AI topics your teams now face, then reinforces the fundamentals that never stopped mattering. We scope everything to your industry, tooling, and risk profile so people leave with habits they can use the next day:

- **AI literacy & safe use of AI assistants:** what data may reach which tools, and the habits that keep sensitive material out of the wrong ones.
- **Prompt injection & AI data-leakage awareness:** how injected instructions and careless data sharing can turn AI tools into attack paths, explained in language your teams can act on.
- **AI-era social engineering:** what AI-crafted phishing, deepfakes, and voice cloning look like today, and the verification habits that hold up against them.
- **Role-based tracks:** tailored tracks for developers, IT staff, and executives, including secure AI adoption for teams integrating AI into their workflows.

- **Core security fundamentals:** phishing and social engineering, credential hygiene and MFA, device and data handling, and what to report and when.
- **Incident response & reporting readiness:** making sure staff know what to do when something looks off (who to contact, what to capture, and how to escalate), not just what to avoid.

Two ways to learn

Pick the delivery mode that fits your team, or blend both. The **self-serve training portal** at training.fletchlabs.ca serves the curriculum on demand in video and textual formats, so staff learn at their own pace and new hires can start on day one. **In-person workshops** put a Fletch Labs practitioner in the room for live sessions and hands-on exercises, the format where questions actually get asked and habits form.

Testing & campaigns

Awareness only counts if it changes behavior. We run controlled campaigns that simulate phishing and security-awareness scenarios so you can see how teams respond in practice: who reports, who clicks, and where coaching will help most. Results feed back into the next round of content and into executive-level reporting that shows measurable human-factor risk reduction over time, turning awareness into action, not a one-off compliance exercise.

How we work with you

You are matched with a **named Fletch Labs representative** who designs the program with you, curates your portal tracks, delivers the workshops, and stays your point of contact as the program matures. Continuity means each campaign builds on what the last one revealed about your organization, not a generic curriculum restarted from zero.

Engagement & pricing

The two delivery modes are priced separately: portal access is generally priced per user, while in-person workshops are scoped per engagement, from a single session to an ongoing cadence. Contact us for a quote tailored to your team and risk profile.

Start a conversation

Tell us about your team, your tooling, and any incidents or near-misses that worry you, and we will scope a program that fits.

Reach us at info@fletchlabs.ca or through fletchlabs.ca/contact.

Sources

1. Verizon, 2026 Data Breach Investigations Report · <https://www.verizon.com/business/resources/reports/dbir/>
2. KnowBe4, Phishing Benchmarking Analysis Center (vendor benchmark) · <https://www.knowbe4.com/phishing-benchmarking-analysis-center>