



Security Awareness & Training

Building the human firewall, for today's threats and tomorrow's.

SERVICE PACKAGE

August 2026

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

Executive summary

You can patch a server; you cannot patch a person, but you can train one. People remain the most targeted and most exploited part of every organization, and no stack of technical controls closes that gap on its own. Fletch Labs delivers security awareness and skills training tailored to your risk profile, covering both traditional fundamentals and the emerging AI-specific risks your teams now face. Programs run as one-time workshops or as an ongoing cadence, and they are 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.

Training services

We scope content to your industry, tooling, and risk profile so people leave with habits they can use the next day:

- **Core security awareness:** phishing and social engineering, credential hygiene and MFA, device and data handling, and what to report and when.
- **Role-based training:** tailored tracks for developers, IT staff, and executives that reflect the decisions and tooling each role actually faces.
- **Phishing education & simulation:** spotting modern lures, verification habits, and handling suspected compromise, paired with controlled simulations that track behavior change over time, not just click rates.
- **AI-specific awareness:** safe use of AI assistants and internal tools, prompt injection risks, data leakage through AI systems, and secure adoption practices for teams integrating AI into their workflows.
- **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.

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, delivers the sessions, 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

Available as one-time workshops or an ongoing training cadence. Pricing is generally based on the number of users in scope; 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>