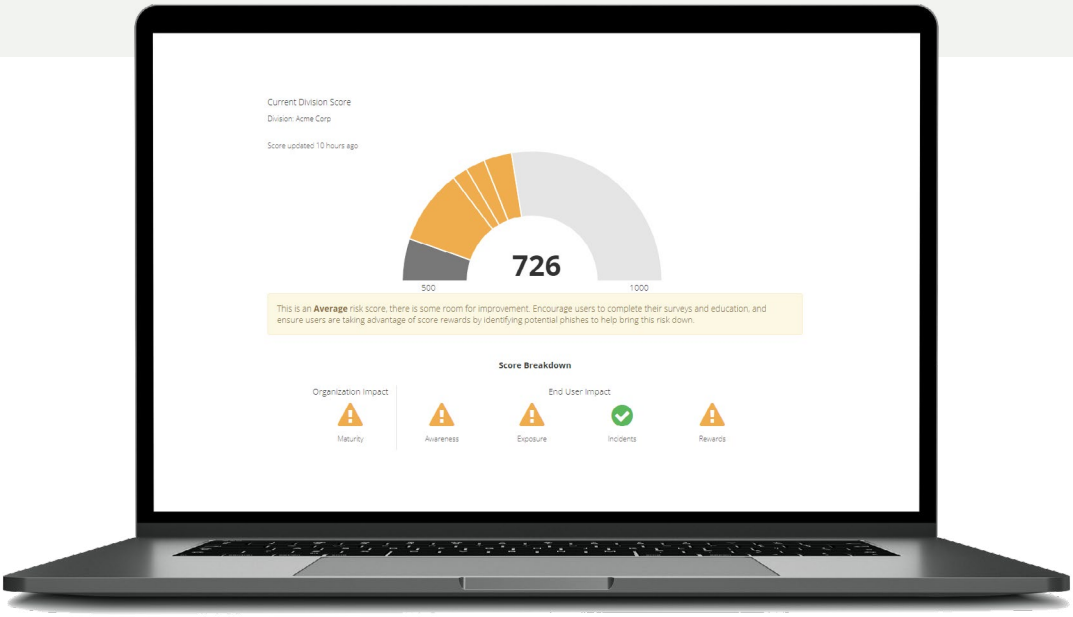
CIRA Cybersecurity Awareness Training

Transform your users into a **human firewall**.

Engaged users are proven to reduce cybersecurity risk

People play a critical role in helping to reduce organizational risks associated with cyber attacks. CIRA Cybersecurity Awareness Training gives IT professionals and security teams a cloud-based platform to train users, simulate phishing tactics, and measure the results. Empower users to be part of the solution, instead of a risk to be managed.



44%

of Canadian organizations faced a cyber attack in the past year (2022 CIRA Cybersecurity Survey). IT teams are adding more layers of security to reduce the risk of cyber incidents affecting their network, devices and data.

82%

of breaches involved the human element (2022 Data Breach Investigations Report). Even if your organization deploys multiple technical layers of security, human emotion can still be exploited through social engineering.

3x

Reduction in users clicking on phishing emails after implementing CIRA Cybersecurity Awareness Training.

> "The personalized risk score really caught everyone's attention by providing context. It helps us zero in on high-risk individuals and groups for more focused interventions."
>
> **CITY OF FREDERICTON**

Time-saving automation

- Assigns training and phishing simulations automatically based on user needs and behaviour, including remedial courseware.
- Dynamically executes phishing tests with content based on an individual's results from past tests.
- Avoids the "gopher effect," where employees warn each other of phishing tests, by sending simulations on a variable schedule.
- Empowers employees to report suspected phishes through a button (integrates with Outlook - 2013 or newer, O365, and GSuite) or by email.

Engage and educate users

- Select from a library of courseware and phishing assets based on real-life situations or customize for your organizational profile.
- Create and customize content with an easy-to-use editor or using third-party tools to author SCORM 1.2 compliant content.
- Personal risk scores change based on course completion and successful reporting of real and simulated phishing tests.
- Gamification and personal dashboards provide user and departmental risk scores which encourages employee involvement.

Useful analytics

- Individual risk scores are assigned based on training and simulation results and accessed via a personal dashboard.
- Customize department scoring to include exposure to cyber attacks that are based on the type of work performed.
- Measure user, department, and organizational risk against the NIST cybersecurity framework and against other organizations.

Simple for IT and business unit administration

- Truly unified training, simulation and results tracking makes administration and reporting simple.
- Fully integrated with Office 365, ADFS and SAML-based identity providers for group and user management.
- Role-based administration to allow departmental level administrators to access key functions.
- Interactive tool highlights top risk factors by category to help you prioritize IT investment.