

New Cybersecurity Awareness Training resources for lawyers and law firms



The prevalence of cyber risks is underscored by multiple successful cyberattacks on Ontario law firms over the last several months that resulted in unauthorized withdrawals of several million dollars.

Many of these frauds could have been easily prevented. Active frauds can be stopped if lawyers and law firm staff recognize the red flags of a fraud in progress. Firms can also take steps to make their systems more secure.

LAWPRO is collaborating with the Law Society to make cybersecurity awareness training resources available to all Ontario lawyers and paralegals in private practice. This training, which is designed to foster a culture of cybersecurity awareness and resilience at law firms, will be provided by the Canadian Internet Registration Authority (CIRA), a globally recognized leader in cybersecurity and risk management.

Participation is optional, but strongly encouraged, and the training is being provided at no extra cost to LAWPRO insureds.

Program content

The content is presented in short 5–7 minute microlearning modules focused on topics like phishing and spear phishing, social engineering, password hygiene, ransomware situations, safe remote working practices, data protection, and fraud prevention. The modules include interactive feedback and can be completed in approximately one hour over 12 months.

For law firms with their own domains, the CIRA platform also includes phishing simulations. These simulations provide practical experience for recognizing real threats, reinforce secure behaviours, and help participants develop the skills needed to respond appropriately to real phishing attacks. Phishing is the most common way that firm systems are compromised.

Registration process

CIRA will administer access to the platform and provide introductory sessions and ongoing support. Lawyers must register with CIRA to access these training resources. CIRA will send an email with a registration link directly to lawyers.

Program offerings vary by size of firm

Recognizing that law firms have different IT configurations and security needs depending on their size, there are three levels of training resources available. Participants will be organized into these groups based on their email environments and their firm's desired level of participation.

Group A:

Sole practitioners and small firms without a domain

If you use an email ending in gmail.com, outlook.com, or another free email service, you are in Group A and will receive the core cybersecurity awareness training. Phishing simulations are not included due to limitations in these email environments.

Group B:

Smaller firms with their own domain

Lawyers and firms using their own email domain (e.g., yourname@your-lawfirm.ca) are in Group B. This group receives the core training content, plus phishing simulations administered by CIRA throughout the year.

Group C:

Enhanced Firm Access for medium and larger firms

Lawyers at firms in this group will receive the training and phishing simulations included in Group B, with the option for additional platform access. Designated firm administrators can receive additional training and platform control, allowing them to enroll users in additional cybersecurity education as needed.

LAWPRO will communicate with managing partners at medium and larger firms to coordinate the desired level of access. Several larger firms are already using the CIRA training resources. All firms are encouraged to use this training resource, but may opt out if they want to. Lawyers at firms that opt out will not be contacted by CIRA.

LAWPRO believes participation in this program will help develop a culture of cyber awareness at firms, reduce cyber and funds transfer frauds, and increase protection for licensees and the clients they serve. ■