



NAVACORD®

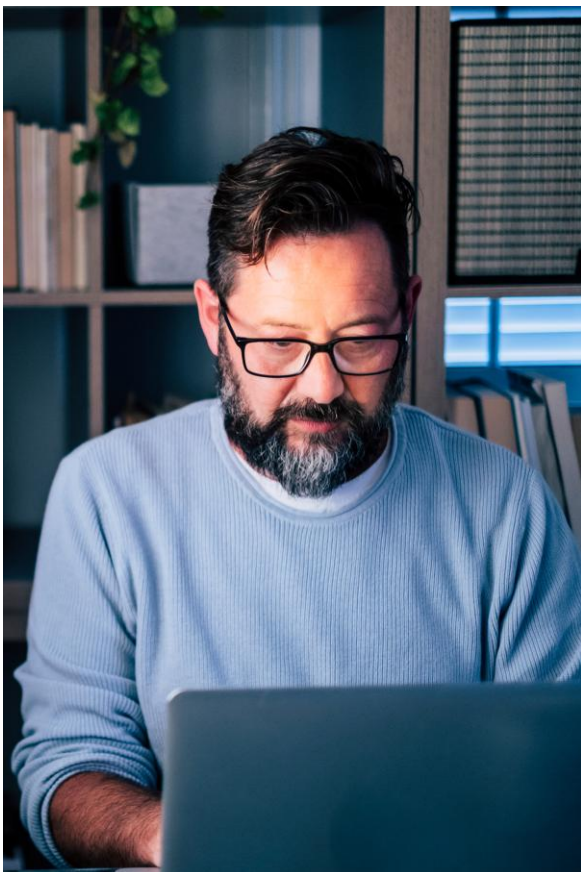
Cybersecurity Best Practices For BCACC Members

Local Touch. National Strength.™

Cybersecurity Best Practices

Understanding and being able to identify potential online fraud techniques is the key to keeping your company safe.

Use these tips to protect your intangible assets and ensure protection against cyber threats.



- 1 Never give sensitive information like social insurance numbers or credit card numbers out over the phone unless you know the person on the other line.
- 2 Shred all credit reports and other sensitive data before disposal.
- 3 Provide regular cybersecurity awareness training to employees.
- 4 Always monitor credit reports and other financial data for the company. If you see things that don't belong, investigate.
- 5 Do not allow employees to write down passwords in the office.
- 6 Always encrypt sensitive data.
- 7 Use Multi-Factor Authentication for cloud-based services, email and remote access.
- 8 Regular backups of critical data to a separate location (i.e. offline/disconnected hard drive).
- 9 Implement loss-control measures such as antivirus software, firewalls and regular software updates.
- 10 Implement an endpoint detection and response (EDR) solution.
- 11 If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- 12 Purchase Cyber Liability Insurance

Protect Your Business from Cyber Threats

Cyber Liability Insurance may provide coverage for eligible losses arising from cyber incidents and data breaches, subject to the policy's terms, conditions, limits and exclusions. Available coverage includes liability protection, breach response costs, cyber extortion, digital asset replacement and eligible social engineering losses.

Navacord has tailored solutions that address the specific needs of your business, keeping you protected in an increasingly digital landscape.

- **Social Engineering Fraud Coverage:** Protects individuals and organizations from financial losses caused by deceptive practices where victims are tricked into transferring money, sensitive data, or other valuable assets to fraudulent parties. These attacks typically involve criminals posing as trusted individuals—such as executives, vendors, or clients—to manipulate victims into taking harmful actions.
- **Breach Cost Coverage:** Protects against costs of lost or stolen data, including customer notifications, credit monitoring, and legal fees.
- **Cyber Extortion Coverage:** May cover eligible extortion payments and related expenses arising from a covered cyber extortion event.
- **Regulatory Proceedings Coverage:** May respond to eligible defence costs and other covered amounts arising from a regulatory proceeding, subject to the policy terms and where legally insurable.
- **Third-Party Liability:** Protects against claims from customers or partners affected by your breach.



BCACC Members: Cyber Liability Coverage Offer

Coverage	Deductible	Limit of Liability
Security, Privacy and Regulatory Proceedings	\$2,500.00 CAD	\$1,000,000 each claim and \$1,000,000 aggregate each Named Insured

AND

Breach Cost, Cyber Extortion and Digital Asset Replacement	\$2,500.00 CAD	\$500,000 each claim and \$500,000 aggregate each Named Insured
--	----------------	---

AND

Social Engineering Coverages	\$2,500.00 CAD	\$50,000 each claim and \$50,000 aggregate each Named Insured
------------------------------	----------------	---

- Program aggregate \$10,000,000 each Policy Period for all payments under all coverages combined for all subscribers under each certificate.
- Higher coverage limits are available upon request as well as options for members with over three professionals.

Coverage is contingent on the submission of a Warranty Statement which confirms that the following cyber controls are in place:

- **Multi Factor Authentication (MFA)** for cloud-based services (such as cloud-based email account access) and for all remote access to your network; or, the business will use Jane, Clinicmaster, Owl Practice or Practice Perfect, with MFA (or 2FA) enabled.
- **Regular back-ups (quarterly at a minimum) of critical data** to a separate location (such as an offline/disconnected hard drive) or a suitable cloud service (Microsoft OneDrive, Google Drive, Dropbox, etc.) that would be unaffected by an issue within your environment. If you use a clinic software such as Jane, your data within the software complies with the warranty.
- **Implement loss control measures** such as regular software updates to your operating system. It's also good practice and recommended to regularly update your antivirus software, firewall, and any other software used.

Complying with the Insurance Warranties

Qualifying for Cyber Liability Insurance through the BCACC Insurance Program is contingent on submitting a Warranty Statement confirming that the required cybersecurity controls are in place.

A warranty is a statement or commitment made by the insured as part of the application for coverage. It is important that all responses are accurate and that the required controls remain in place.

This resource explains the three required cybersecurity controls and provides practical information to help you understand and maintain them.



Multi-Factor Authentication



**Quarterly Backups of Data
Stored on Laptops or
Workstations**



**Regular Operating System
Updates**



Multi Factor Authentication

Multi Factor Authentication (MFA) is a way of verifying your identity when you sign into online accounts with more than one factor such as a password and a code from an app. If you use systems like Jane, Clinicmaster, Owl Practice or Practice Perfect you can enable MFA for all these systems. Make sure to enforce MFA across your organization for every user account.

MFA Resources

Enable MFA for all cloud-based software

Enable MFA for cloud-based services, including cloud-based email accounts, and for all remote access to your network. If your practice uses Jane, Clinicmaster, Owl Practice or Practice Perfect, ensure that MFA or two-factor authentication is enabled.

MFA should be enabled for every user account, not only the administrator's account. Follow the software provider's instructions to activate and manage MFA.

Enable MFA for Email

Enabling MFA for email is an additional measure you can take to protect your business. Your email provider will have support documentation to advise how to enable this specific to your provider.



[View practiceperfect MFA Info](#)



[View OwlPractice MFA Info](#)



[View clinicmaster MFA Info](#)



[View Jane MFA Info](#)

Regular Backup of Critical Data

Backup data stored on laptops or workstations at least quarterly to a physically disconnected hard drive or a suitable cloud service. The backup should remain accessible if the original device, network or data is compromised.

Data Protection

If you store any sensitive data on your computer, it is important to backup your data regularly to a separate location such as an offline/disconnected hard drive.

If you use a clinic software such as Jane, your data within the software complies with the data backup requirement. However, if you store data anywhere outside of the software, you should regularly backup this data to a separate location.

Data backup ensures that your critical data will not be affected by an incident affecting your device or network.



[View practiceperfect Backup Info](#)



[View OwlPractice Backup Info](#)



[View clinicmaster Backup Info](#)



[View Jane Backup Info](#)

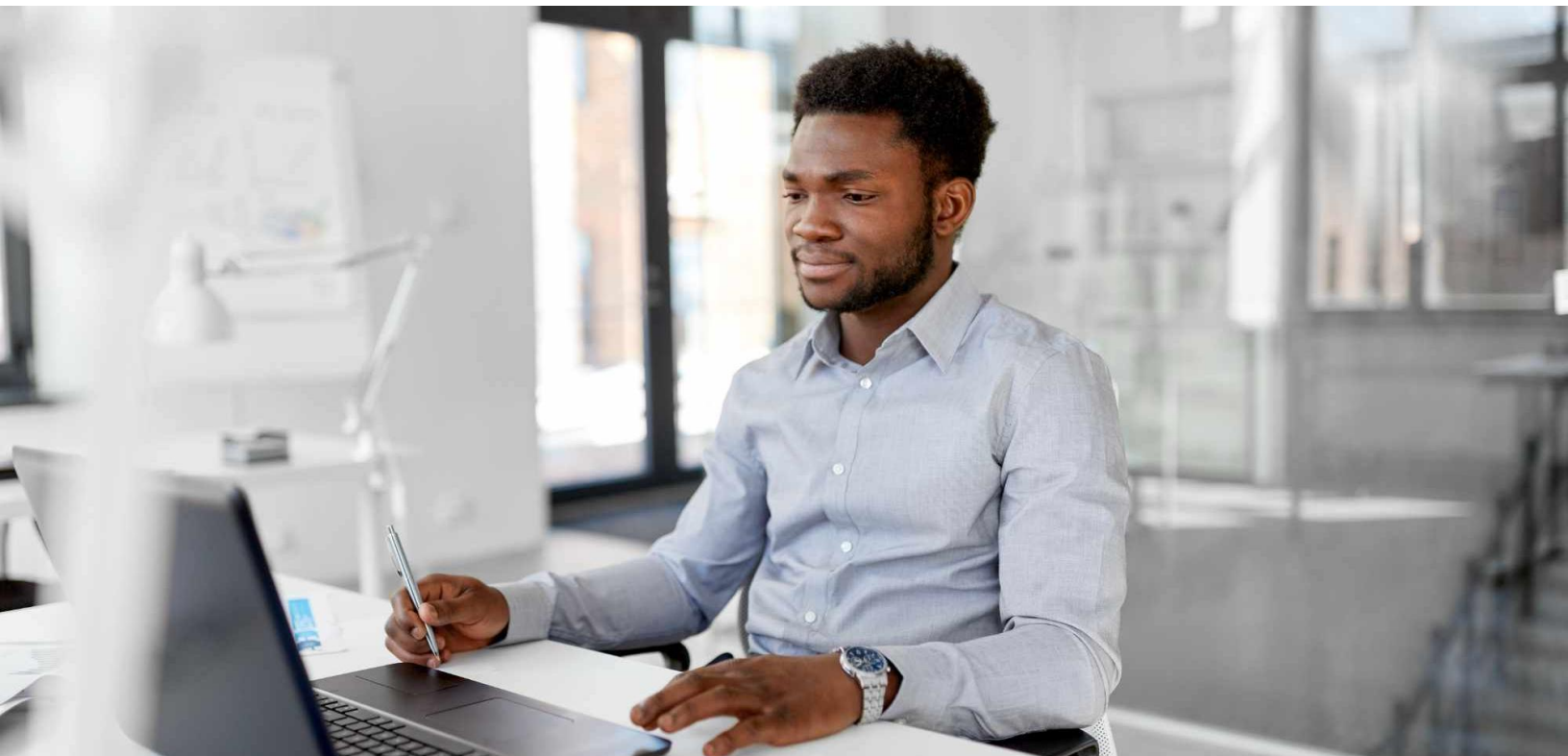
Loss Control Measures

Implementing loss control measures like Firewall, Antivirus and Software updates are important steps to take to prevent a cyber liability loss.

Updates Matter

Regularly update the operating systems on laptops and workstations used by your practice. Updates often include security patches that address known vulnerabilities.

Firewalls act as a digital barrier, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. Regularly updating your firewall ensures that it can recognize and block new and emerging threats. This proactive approach is essential for maintaining a secure digital environment.



Coverage Options for Larger Practices and Higher Limits

Standard BCACC Cyber Liability coverage is available for practices with one to three professionals. Practices with more than three professionals, or those requesting higher coverage limits, must complete a separate short application so that a quotation can be obtained.

If your business has more than three professionals, or if you require a limit that exceeds the limits available through the standard program option, [use this link](#) or scan the QR code to complete the application.



Free Cyber Assessment

Victor is offering a free cyber assessment & consultation (valued at CAD \$397).

Eligible BCACC members with Professional Liability Insurance have access to a complimentary cyber assessment and consultation. During the assessment, a cybersecurity specialist will review your current practice, provide a customized scorecard, discuss potential next steps and provide a written report.

What Can You Expect During a Cyber Assessment Call?

In 90 minutes or less, a cybersecurity expert will:

1. Questionnaire

Guide you through a series of questions about your company's cybersecurity operations and practices, including the policies that you currently have in place.

2. Scorecard

Provide you with a customized cyber assessment scorecard based on your responses to a series of questions. A cybersecurity specialist will review your customized cyber assessment scorecard and answer any questions or concerns that you may have.

3. Recommendations

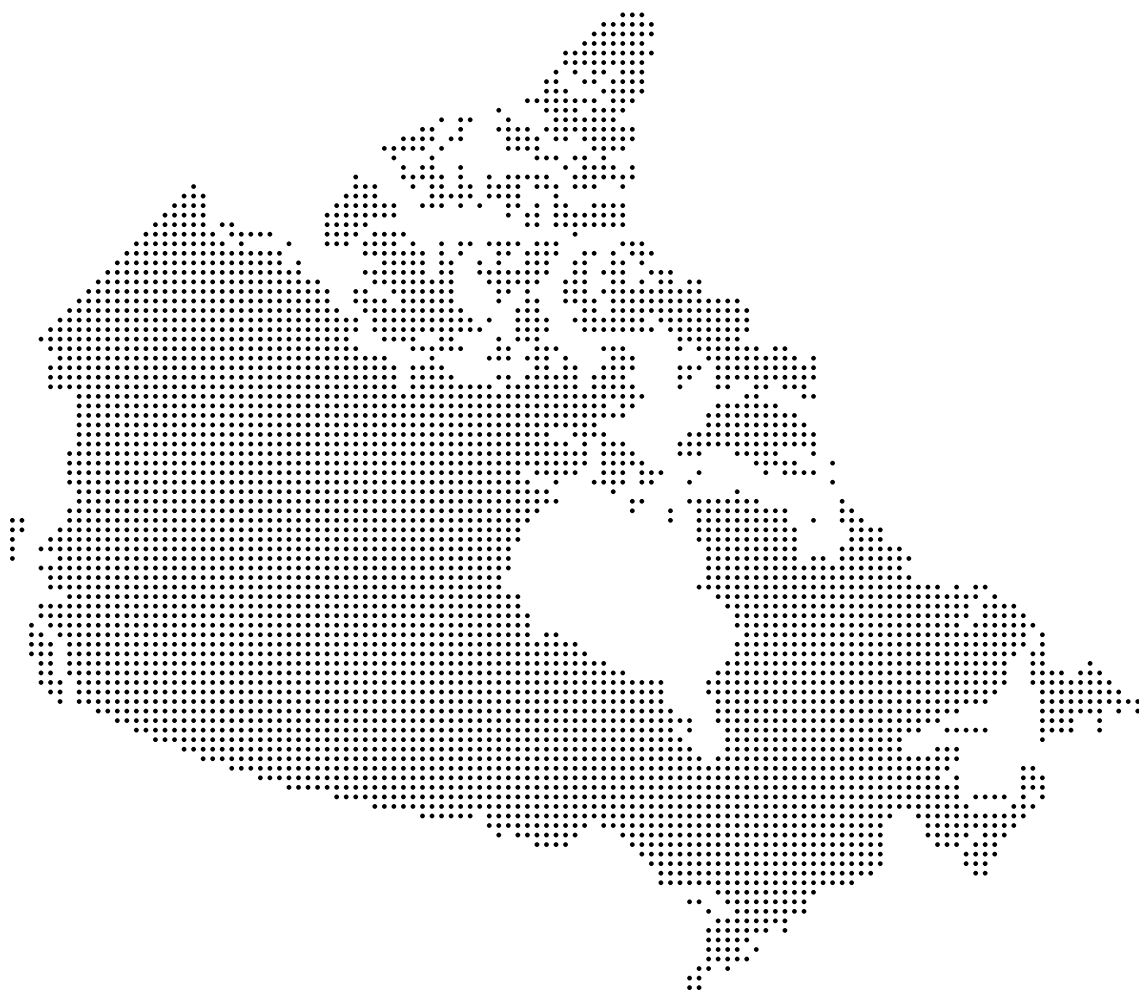
Give you recommendations on next steps and the additional cybersecurity service packages available to you. Victor policyholders receive up to 30% off these packages.

4. Report

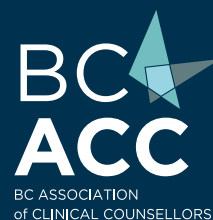
Provide you with a comprehensive cybersecurity report. This detailed formal report will help create the basis for a cybersecurity action plan for your company.

Visit this [link](#) or scan the QR code to book your cyber assessment appointment online.





NAVACORD®



We can help protect you and your business from cyber threats.
Contact us: 1-800-463-5208 x3006 | BCACC@navacord.com



Use this [link](#) to visit our online BCACC Coverage information resource page.