

Protecting Your Information

At the BCMEA, the security of your personal and private information is of utmost concern. We are committed to keeping your confidential information as safe as possible. While the BCMEA utilizes strong internal measures to protect the security and privacy of your information, there are important steps you should take to help protect your information when using the BCMEA website(s).

THIS SECURITY INFORMATION MAKES RECOMMENDATIONS AND SUGGESTS BEST PRACTICES WHICH USERS MAY FOLLOW AT THEIR OWN DISCRETION. ALL TERMS OF THE WEBSITE USAGE POLICY GOVERNING THIS SITE ARE STILL APPLICABLE.

You play a critical role in keeping your personal information protected. Please review each security section below and become familiar with the measures taken to protect your on-line information as well as the steps you can take to help secure your on-line experience.

Strong Encryption Requirements

The BCMEA web systems require that you have 128-bit encryption, the highest level of encryption generally available today, installed on your browser. When using this encryption, all data sent to the BCMEA website(s) is scrambled and then de-coded. We do not transmit personal and/or private data over any non-encrypted connections.

Your BCMEA website(s) session is protected in a “secured” network environment through Secured Socket Layer (SSL) encryption. SSL technology is used within your session to encrypt your personal information before it leaves your computer to help ensure no one else can read it. Depending on your browser setting, a pop-up window will appear to notify you that you will be entering a secured page. You will know when you are on a secured BCMEA page when you see the “https://” before the web address. A padlock symbol in the lower right hand corner of your browser window will also be present. This padlock indicates that your BCMEA on-line session is in a “secured” environment.

Protecting Our Internal Systems

The BCMEA protects the security of your personal information at all times. We have taken reasonable measures to protect our internal computer systems from unauthorized access. To protect our systems from public Internet traffic, firewalls are used. Firewalls are a combination of computer hardware and software that separate the Internet from the BCMEA’s internal web servers and computer systems. Firewalls prevent unauthorized Internet traffic from accessing our web servers and internal systems, thereby protecting your information and transactions.

Limiting Unauthorized Access To Your On-Line Session

The BCMEA web systems use “timed log-outs” on all of our websites. This means that on-line sessions are terminated after 20 minutes of inactivity. Once the BCMEA website has ended your session, you will be required to re-enter your username and password. “Timed Log-Outs” protect you against unauthorized access.

Intrusion Detection Systems

The BCMEA websites employ state-of-the-art network based IDS (Intrusion Detection Systems) to secure the integrity of our network by ensuring that unauthorized traffic cannot pass through our systems undetected.

What Can You Do To Protect Your Information?

As an Internet website user, you play an important role in protecting your personal and private information. In addition to a myriad of website technologies we use for secure exchange of personal data, you play a significant role in configuring your own computer to maximize its security environment. The following is a checklist to ensure that your system conforms to known "security best practices".



Two pieces of key information must remain confidential to you - your username and password. Passwords must be kept confidential at all times and not be disclosed to anyone. BCMEA staff and related personnel will NEVER ask for your passwords.



The auto-complete function on your browser should be disabled to avoid the automatic completion of your username and password when you type in the relevant fields.



Passwords should be changed on a regular basis (at least once every 30-60 days).



Passwords should be memorized and NOT be written down or stored in the computer hard disk, diskettes or other insecure devices.



Ensure that the browser and application software used is upgraded to support 128-bit encryption or a higher encryption standard.



Whenever you are logged-on to a secured BCMEA website(s), check that the bottom right corner of the screen shows a secure symbol of the lock.



If you suspect any unusual account activity or that your password confidentiality has been compromised, please change your password immediately and contact our Support line.



Before you logon to BCMEA websites, for security purposes, ensure all other Internet sessions, i.e. browser windows, are closed.



Always remember to log out properly (by clicking on "Log out" instead of simply closing the window with the x on the top right corner of the screen) from your BCMEA session before visiting other websites.



Remember to close the browser window after you have logged-out of your session.



Whenever security updates and patches are made available by your computer or browser vendor, always ensure that you download and apply them as they are designed to provide you with protection from known possible security problems.

Use "Supported" Products To Access BCMEA Systems

The BCMEA Development team performs security audits of our applications, operating systems and services on an on-going basis to ensure that all components comply with the highest standards of security and best practices. We do not recommend accessing our systems with "unsupported" products.

"Supported" Products are:



Microsoft Internet Explorer® 5.x or higher



Microsoft Windows® NT, 98, 2000, ME, XP

Examples of "Unsupported" Products are:



Mozilla Firefox® Internet Browser



Netscape® Internet Browser



Apple Macintosh® Operating Systems



Linux Operating Systems

Keep Your Computer Secure

Installing virus detection software on your computer is a good computing practice that protects your information from being corrupted or accessed by unauthorized users. This software needs to be updated often to ensure you have the most current protection available. To further protect yourself from viruses or other unwanted problems, do not open e-mail attachments from unknown or untrustworthy sources. Do not install unlicensed software, or software from an unknown source. Make sure you know anyone who uses your computer and limit unauthorized access.

Logon and Password Feature

To help make accessing your BCMEA website account more secure, we require you to obtain your personal and confidential password to logon to the BCMEA secured website(s). This information is then authenticated by the BCMEA website(s) to verify who you are before providing access to the system.

Should too many failed login attempts be detected, the account will be locked automatically and you may have to contact the password reset telephone line to have the lock cleared. This step is required to protect your account from random password attempts.

Your Password

Your password is the key to your on-line account information. Protect and change your password on a regular basis — every 30-60 days is recommended. Create a password that is unique to you and that cannot be easily guessed by someone else. Create a password that contains a combination of both letters and numbers. Do not associate your password with anything personal such as names, birthdates, telephone numbers, or other familiar words. Memorize your password and never write it down, electronically store, or reveal it to anyone.

Note: No one at BCMEA will ever ask you for your password. Never give out personal information to anyone on the telephone or from a website unless you have verified the credibility of the source and/or have initiated the call to a trusted source.

Disable The Autocomplete Feature On Your Browser

Disable the 'AutoComplete' function to prevent others from seeing your logon information each time you use the web site(s). On Internet Explorer for example, the 'AutoComplete' function remembers data you have input including your passwords on frequently used sites. Check the User Guide for your computer setup to get instructions, or go on-line to the manufacturer's website.

[Instructions on disabling the "AutoComplete" on Internet Explorer.](#)

Protecting Your Identity On-line

Install commercial-grade firewall software on your computer to help prevent unauthorized individuals or information from entering your computer system. This is especially important on computers that use a broadband connection to access the Internet (Cable modems or DSL). Since your Internet connection is alive when your computer is on, the risk for malicious activity to your computer increases.

Run a current updated anti-virus program on your computer frequently. Anti-virus software can scan your incoming and outgoing e-mail and attachments for computer infections like worms, viruses, Trojan Horses and other malicious code that can affect your computer files and operation.

Keep your software current and apply all security patches for your computer operating system (e.g. Microsoft Windows) to keep security information current.

Be aware that there are phony websites designed to trick consumers and collect personal information. Verify the source of your e-mails and only open e-mail that you expect. Always run anti-virus software before opening e-mail.

"Password protect" your computer to prevent unauthorized individuals from accessing your information.

How Do I Know If I Am Connecting To The BCMEA And Not To Other Parties?

You may check the validity and owner of the encryption certificate. Using the "supported" Internet Explorer browser, double-click the security lock icon at the bottom right of your session window (you may need to enable the status bar if it cannot be seen). In the General tab, the Certificate Information should state who it is issued to (e.g. mybcmea.bcmea.com) and when it is valid for. The certificate should still be within the valid period.

Using The BCMEA Website(s) Via A Public And/Or Shared Computer

Avoid using the BCMEA website(s) at Internet cafés, libraries, and other public sites to avoid your information from being copied, traced, or re-entered after you leave.

If you must use a public computer, please take the following precautions:

[Disable the "AutoComplete" on Internet Explorer.](#)

Please remember to log-out of your session and close all browser windows.

Why Do I Need To Accept "Cookies" To Access The BCMEA Website(S)?

A cookie is a text file that resides on your computer. In order to provide a more stable and personalized experience, BCMEA website(s) use two types of cookies as part of the interaction between your browser and the websites:

Persistent Cookies:

A "Persistent Cookie" is used frequently throughout the website(s) to track usage of our latest information, news bulletins and to ensure that users are receiving personalized and up-to-date information. This cookie does not contain any private information.

Per-Session Cookies:

A "Per-Session Cookie" assigns a session id when you log-on and stores it in your PC's temporary memory (RAM). This session ID is used to establish and validate your PC during your session. When you log-off from the website(s), the "Per-session Cookie" is removed. These cookies also do not contain any private information.

If your browser prompts you when a cookie is "served", you must accept it in order to access BCMEA website(s). Since cookies are site-specific, only BCMEA website(s) can access, decode and make use of the information.

Logoff And Close Browser

Always remember to log-off from the website(s) and to close your browser when you have finished visiting secure websites. Please ensure that you use the "Logout" functionality of the websites and not the [x] button on the top right corner of the browser window. This may help prevent others from being able to view your on-line information at a later time. Please contact us immediately if you suspect any unusual account activity.

Test Your Computer For Security Vulnerabilities Regularly

There are several commercial tools currently available on the Web that you can use to test your computer system for security vulnerabilities. For example, if your system is not configured properly, it may be easier for hackers and intruders to break in.

Stay up-to-date with the latest security events and incidents and make sure that you stay current with all security updates/patches and fixes that become available from the vendors.

For further details of how to protect your computer systems please visit the [Microsoft security web site](#).

Terms and Definitions

Anti-virus Software

Commercial-grade anti-virus software should be installed on your home computer and laptop to scan e-mail and files on your computer for potential viruses that may be attached. If a virus is detected, you are notified immediately and the anti-virus software will prevent the e-mail or file from being sent to you before it's opened. You should run your anti-virus software frequently to prevent computer infections like viruses, worms, or Trojan Horses from entering your computer system. Purchase a program that automatically upgrades your virus protection on a regular basis.

Browsers

A browser is a software application that works with the Internet to provide a way to view, find and interact with websites and web pages. As new versions of browsers are developed, users will be able to experience a full multimedia spectrum, including text, graphics, sound, and video.

Cable Modem

Cable modems provide high-speed Internet access using cable television networks. They use either the traditional coaxial cables or newer fiber optic cables for the transmission of data. Cable modems offer continuous connection to the Internet without having to dial into an Internet Service Provider (ISP) each time you wish to connect to the Internet.

Cookies

Cookies are pieces of information stored directly on the computer and provide a more efficient and more personalized experience at a website. The BCMEA website(s) do not store any personal information in the cookies.

Digital Certificates

Like a driver's license or passport, Digital Certificates allow individuals or organizations on the Internet to verify each other's identity to prevent unauthorized access. A Digital Certificate is a randomly generated set of characters that a computer sends to your browser. The browser on your computer stores this information and uses it as a digital stamp to certify the authenticity of the information sent to you and as a means of establishing identity. You may see a Digital Certificate issuer logo at the bottom of a browser page for your reference.

Encryption

When you establish a connection to the BCMEA secured website(s) the information you enter on-line is "encrypted" or transformed into a string of unrecognizable characters before being sent over the Internet, likewise information coming from the BCMEA websites are encoded and decoded by your browser. This helps to keep the information between the BCMEA computer system and your Internet browser private. Your session is in a secured "encrypted" environment when you see "https://" in the web address and/or when you see the locked "padlock" symbol at the bottom right corner of your browser window.

Firewall

Firewall software can be installed on company and home computers as a barrier against hackers and viruses. Firewalls are used to filter potentially destructive information or prevent unauthorized access. This is especially important on computers that use a broadband connection to access the Internet (Cable modems or DSL). Since your Internet connection is on when your computer is on, the risk for malicious activity to your computer increases.

Keystroke Capturing

Keystroke Capturing or "keystroke logging" is a surveillance tool that is used to record the keystrokes of unsuspecting victims in order to determine password and logon information which can be used for fraudulent purposes.

Plug-in

A plug-in is a software module that adds a specific functionality to the web browser. Plug-ins for Internet Explorer allow the browser to display various types of audio and video messages. For example, the popular Adobe® Acrobat® (PDF) Plug-in is used for viewing files and reports.

Secure Sessions

Your on-line sessions are protected in a "secured" environment which use Secure Socket Layer (SSL) technology to encrypt your personal information before it leaves your computer to help ensure that no one else can read it. You will know that you are on a "secured" page when you see the "https://" before the web address. You will also see a padlock symbol in the lower right hand corner of your browser window. Commonly, a closed padlock indicates that your on-line session is "secured" by encryption to protect your personal information.

Server Authentication

When you logon to the BCMEA website(s) that requires authentication, you usually input a specific username and password to gain access to your personal information. The encrypted information then passes through a rigorous test on BCMEA computer systems to ensure proper authorization before your personal information is displayed.

Security Holes/Bugs

Security holes/bugs are often faults, defects or programming errors exploited by unauthorized users to access computer networks or web servers from the Internet. As these holes or bugs become known, software publishers develop "patches," "fixes" or "updates" users can download that usually fix the problems.

Session Time-outs

For your added on-line security, BCMEA uses a session time-out feature. If your BCMEA Internet session is idle for a given amount of time, it is ended automatically. This helps ensure that your on-line session is in a "secured" environment and that the personal information you enter is protected.

Social Engineering

Social engineering is an identity theft process that relies on human interaction and often involves tricking an unsuspecting individual into providing personal information like bank account details or passwords. Social engineers search dumpsters for valuable information, memorize access codes by looking over someone's shoulder, or take advantage of people's natural inclination to choose passwords that are meaningful to them and can be easily guessed (children's names, addresses, or birthdates). The personal information discovered is then used illegally to apply for credit, purchase goods and services, or gain access to funds.

Spam

Sometimes companies or individuals purchase e-mail address lists to send unsolicited ads for products and services. The unsolicited e-mail is defined as "spam," and it fills up e-mail files and could add additional pop-up windows on your computer screen. You can purchase anti-spam software to filter unwanted e-mail or spam from your e-mail list until you delete it.

SSL

Secure Socket Layer (SSL) protocol provides a high-level of security for Internet communications. SSL provides an encrypted communications session between your web browser and a web server. SSL helps verify that sensitive information (e.g. credit card numbers, account balances and other financial and personal data) sent over the Internet between your browser and a web server remains confidential during on-line transactions.

Trojan Horse

A Trojan Horse is the name of another type of virus, which is simply a computer program that masks itself as another program. Trojan Horses are usually sent as an e-mail file attachment. For example, it may claim to be a game, but once opened, can cause damage to your computer, from erasing files to changing your desktop. It then sends itself to other people in your address book to propagate itself.

Virus

Often through e-mail, file sharing and downloaded programs, computer viruses are sent as attachments. A virus is a small program that piggybacks onto e-mail and program files. For example, a virus might attach itself to a program or a game. Each time the program is opened, the virus runs and can infect other programs or damage your computer. Some viruses move around through e-mail then replicate by automatically mailing to the victim's entire e-mail address book. Never open an e-mail attachment unless first scanned through anti-virus software.

Worm

A worm is a specialized virus that searches through networks to find security holes to replicate itself from machine to machine. Worms use up computer time, space, and speed when replicating, with a malicious intent to slow or bring down entire web servers and halt Internet use.

Adobe® and Acrobat® are registered trademarks, and Acrobat Reader™ is a trademark, of Adobe Systems Incorporated. Macintosh® is a registered trademark of Apple Computer, Inc. Microsoft® and Windows® are registered trademarks of Microsoft Corporation. Firefox™ is a trademark of the Mozilla Foundation. Netscape® and Mozilla® are registered trademarks of Netscape Communications Corporation. Norton AntiVirus® is a registered trademark of Symantec Corporation. All other trademarks and service marks are the property of their respective owners.

Copyright © 2005 British Columbia Maritime Employers Association. All rights reserved.

Q: How do I change the password security default in my browser?

A: An Internet Explorer feature called "Autocomplete" allows user typed entries to be stored in the users local computer. This is not a recommended setting if the computer is shared by more than one user. The optimal setting for "Autocomplete" saving is to have it set off. The default behavior of Internet Explorer is to prompt the user prior to storing sensitive information such as passwords. To view and/or modify this setting to ensure that your login id and password is not saved follow these steps:

1. Open Internet Explorer browser.
2. Click on Tools.
3. Click on "Internet Options".
4. Click on "Content" tab.
5. Click on "Autocomplete" button.
6. Ensure that "Autocomplete" for "Forms" and "User names and passwords on forms" is checked off. Also click on "Clear Passwords" button to remove any existing entries. (See below)
7. Click OK.



[Back to top](#)

