

Internet Security

The Internet has changed the way financial institutions do business. Internet banking provides convenient access to information and the ability to perform transactions from home, work or other locations. It is important to be aware that when you communicate via the Internet, other people and software can also communicate with your computer. An inadequately protected computer can be accessed by an unknown party or a virus in a very short period of time.

What we are doing to protect your security

We take many precautions to protect the online banking environment and ensure your information is safe. Our online services offer you the best security currently available in a commercial environment so that your personal and financial information is protected while in transit between your computer and our server. This is done through the use of industry standard security techniques such as encryption. Encryption ensures that information cannot be read in transit or changed by scrambling the data using a complex mathematical formula. Some browsers can create a more secure channel than others, owing to the 'strength' of their encryption. We use only the strongest channel available - referred to as 128-bit SSL (Secure Socket Layer). If you have a browser that only supports 'weaker' encryption such as 40-bit or 56-bit SSL, you will need to upgrade your browser before using our site. The longer and more complex the 'key' is, the stronger the encryption. The 40 and 128 refer to the length of the key. Since 128 is longer, than 40, it is more secure. According to Netscape, 128-bit encryption is trillions of times stronger than 40-bit encryption.

We also ensure that only individuals who provide an authentic Personal Access Code can access your account information. To help you protect your information your online banking session will end automatically if there has been no activity for 15 minutes.

Access to our databases is strictly managed and systems are in place to ensure security is not breached, including the physical security of our computer hardware and communications.

For more information on the specific policies and practices that we use to safeguard your personal and financial information, [please click here to view our Privacy Statement](#).

What you need to do to protect your computer and PAC

Protecting your Personal Access Code (PAC)

Just as you play a vital role in ensuring the security of your home and your possessions, you too share in the responsibility for ensuring that your personal information is adequately protected.

In order for us to ensure that *only* you are accessing your accounts, we need a unique way of knowing that it's you. Just as the key to your home protects unwanted entry, the online banking 'key'—your Personal Access Code (PAC)—ensures that only you can access your accounts.

It is your responsibility to ensure that your 'key' to the online banking section of this website is protected. Please observe the following security practices:

- Select a PAC that is easy for you to remember but difficult for others to guess.
- Do not select a part of your PIN (your ATM 'key') or another password.
- Keep your PAC confidential and do not share it with anyone.
- Do not write your PAC down or store it in a file on your computer.
- Never disclose your PAC in a voice or email, and do not disclose it over the phone.
- Ensure no one observes you typing in your PAC.
- Change your PAC on a regular basis. We suggest every 90–120 days.

Protecting your computer

We have provided a secure channel for our members to communicate with us. Once the information has reached your computer, it's up to you to protect it. To protect your information, you should:

- **Never leave your computer unattended** while using our online banking services.
- **Always exit the site using the Logout button** and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.
- **Prevent the browser from caching** (storing) the pages that you view by using the Enhanced Security feature located on the login screen. We strongly recommend that you use this feature if you are accessing the online banking section of the website from a shared computer, such as at a friend's house or through a publicly-accessible computer, such as at a library or airport.
- **Secure or erase files** stored on your computer by your browser so others cannot read them. Most browsers store information in non-protected (unencrypted) files in the browser's cache to improve performance. These files remain there until erased. They can be erased using standard computer utilities or by using your browser feature to 'empty' the cache.
- **Disable automatic password-save features** in the browsers and software you use to access the Internet.
- **Install and use a quality anti-virus program.** As new viruses are created each and every day, be sure to update your anti-virus program often. It is recommended you update anti-virus definitions weekly. Scan all download files, programs, disks and attachments and only accept files and programs from a trusted source.
- **Install and use a personal firewall** on your computer to ensure others cannot access your computer through the Internet.
- **Install new security patches** as soon as your operating system and Internet browser manufacturers make them available.
- **Install an anti-spyware program** and check your computer regularly.

Protecting your information when using a public computer

You should be extra vigilant when using publicly available computers. Even if you adopt the tips above to protect your information, you need to bear in mind that even benign programs, like popular desktop search programs, can pose a security risk. Certain programs, such as Google Desktop, cache items that you have viewed so you - or potentially, an unwelcome third party - can easily search and find those pages later again.

If you come across a program like this when you are using a public computer, using the Enhanced Security feature located on the login screen will not stop these types of programs from caching the pages you view. You can adjust the search program preferences so it does not store secure pages you wish to view. If you forgot to adjust the preferences before banking online, you can remove the stored items via the Google Desktop results page by clicking on the Remove items link.

To learn more about browser security, please visit the [Netscape](#) and [Microsoft](#) web sites. To ensure a safe and secure Internet session, only visit reputable sites. If you visit any questionable web site beforehand, we recommend you close your browser and restart it before proceeding to use our online banking services.

Fraud: Recognize it. Report it. Stop it.

Electronic identity theft can occur when you respond to a fraudulent email that asks for your personal banking information. Armed with this information, a person may be able to access your accounts or establish credit, pay for items or borrow money using your name. You can help protect yourself from electronic identity theft by following some simple precautions.

Safety precautions for online banking

- The easiest way to tell if an email is fraudulent is to bear in mind that we will never ask you for your personal passwords, personal information numbers or login information in an email. Legitimate financial institutions do not include links to their web sites in email communications to customers.
- When banking online, check the address of any pages that ask you to enter personal account information. In the toolbar at the top of the page any legitimate Internet banking web site will begin with 'https' to indicate that the page is secure.
- Look for the padlock found in the lower right corner of your screen. If the page is legitimate, by clicking on the padlock, you can view the security certificate details for the site. A fraudulent site will not have these details.
- Type in our web address yourself to ensure you are transacting with our server.
- Check your bank and credit card statements regularly to ensure that all transactions are legitimate.

Contact *Easy Savings* immediately if you suspect someone has gained knowledge of your PAC/PIN, or if you suspect any loss, theft or unauthorized use of your account.

Browser Requirements

Browsers Supported

The website you are using has been developed to provide a convenient experience for a broad range of users, including users that access the site with assistive technologies (such as Screen Readers). To accomplish this task, the site has been developed to support a number of current Internet specifications. Below is a table that summarizes the varying levels of support for a number of browsers:

Definitions of levels of support:

Level 1: We carry out Quality Assurance using this browser across at least one platform and support this browser.

Level 2: We support this browser, but do not carry out Quality Assurance to verify the impact of any changes made to the site. We use the test for this browser on a different platform, or with a newer, related release.

Level 3: We do not test any of these browsers on any platform. We do not support the visual display of what these browsers render, although the functionality of the site should remain fully accessible. If this is not the case, please tell us.

N/a: The browser is not known to work on this platform.

Browser	MS Windows				Mac	
	98	2000	XP	Vista	10.3.x	10.4
IE 7.0	n/a	n/a	1	1	n/a	n/a
IE 6.0	n/a	2	1	n/a	n/a	n/a
IE 5.5	n/a	3	3	n/a	n/a	n/a
IE 5.0	n/a	3	3	n/a	n/a	n/a
Netscape 8.1	n/a	2	2	2	n/a	n/a
Netscape 4.7+	3	3	3	n/a	3	3
Firefox 1.5+	3	2	1	1	2	1
Firefox 1.0	3	2	2	3	2	2
Mozilla Derivatives	3	3	3	3	3	3
Opera 9	3	2	2	2	2	2
Opera pre 9	3	3	3	3	3	3
Safari 2.0	n/a	n/a	n/a	n/a	n/a	1

Browser	MS Windows				Mac	
	98	2000	XP	Vista	10.3.x	10.4
Safari 1.3+	n/a	n/a	n/a	n/a	2	n/a

For our technically inclined users, the particular specifications that we support are HTML 4.01, CSS 1.0 and 2.0, DOM Level 1 and 2, and ECMA Script (JavaScript). The site will work using all browsers in so far as they correctly implement these recommendations. Those browsers that do not support these specifications are expected to gracefully degrade to some lower level of support.

To maximize your Internet banking experience, we recommend that you use a newer browser version to take advantage of new technologies and to ensure that the most current security updates are being utilized. More information on some of the common browsers listed above follows:

Internet Explorer 7.x

While Internet Explorer versions 5.x and older can be used for accessing our services, users of IE 6.0 onwards will have a superior experience while using the site

Our product no longer formally supports browsers used in combination with Windows 98/98SE/Me. However, the site is expected to continue to work as it does today on older platforms. In addition, IE for Mac is no longer formally supported.

Get the latest version of Internet Explorer:

[Download PC Version](#)

Firefox 1.0 onwards (formerly Mozilla)

This site supports Firefox versions 1.0 onwards (including Mozilla versions from 1.3 onwards). We recommend you upgrade to a recent version of Firefox, as older versions had known issues that may affect your enjoyment of the site.

Get the latest version of Firefox:

[Download Firefox](#)

Netscape 7.x

Our services can also be used effectively with Netscape 7.1 onwards.

Get the latest version of Netscape:

[Download PC & MAC Versions](#)

Netscape 4.7, IE 5.X and older browsers

Netscape 4.7 and IE version 5.X browsers only meet some of the development standards we aim to comply with. As such, much of our site will display differently than it will using a newer browser version. If you currently use one of these older browser versions, we recommend that you consider upgrading to a newer version to take advantage of our more advanced features, as well as those used on other sites that you might visit regularly.

Safari

We provide support for Apple Safari browser version 1.3 onwards. Apple's requirements for using this browser are Mac OS X 10.3 or later or any Macintosh computer.

Get the latest version of Safari:

[Download Safari](#)

128-Bit Secure Socket Layer (SSL) Encryption

To access our services, your browser must also support 128-bit Secure Socket Layer (SSL) encryption. If you don't have it, you will need to download the appropriate encryption support from the supplier of your browser. Most browser upgrades now support 128-bit as the default level of encryption when you download the installation package.

If you use Netscape, you can download the appropriate support from Netscape - www.netscape.com.

If you use Internet Explorer, you can [download a High Encryption pack from Microsoft](#).

Cookies

In order to use our online banking services, you must ensure that you have not disabled your browser's ability to accept cookies (particularly first-party session cookies). For more information on enabling, and disabling cookies within your browser, please review your browser's Help section.

For more information on our use of cookies, please review the cookies section in [our Privacy Statement](#).

Javascript

JavaScript is also used to enhance our services. If JavaScript is disabled on your browser, the main features of the site will be functional but you may disable some or all of the enhanced capabilities or features such as the Print button, or the Memorized Accounts feature. To use these enhanced capabilities, please re-enable JavaScript on your browser.

Hardware Configurations

We have no minimum hardware requirements, however certain minimum requirements may be specified by the browser you use.

Accessibility Statement

We are committed to ensuring our online services are as accessible as possible to all users. To achieve this we have built our site to comply with the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG). These guidelines assist website developers by describing best practices to implement websites that will be accessible to all users.

- This site complies with WCAG Level Double-A of the Guidelines, available at <http://www.w3.org/TR/1999/WAI-WEBCONTENT-19990505>, with the small number of known exceptions itemized below.
- This site also complies with the guidelines found in Section 508 of the US Federal Government Rehabilitation Act.

Pages on this site were authored using technologies selected to produce a user-friendly and visually pleasing website. Some older browsers may not support these technologies and while we make every effort to accommodate these browsers, it may be necessary to disable some features, such as Cascading Style Sheets (which controls the colours and fonts used) or JavaScript (which builds interactive dynamic content) on your browser to view the site.

If your browser does not support these technologies (or if they are disabled), the content of each page is still readable although the look and layout will be significantly altered. Best efforts have been made to make the site functional without these advanced features.

We recommend that users keep their browsers up-to-date to take advantage of new technologies. For more information on which browsers we support see the Browser Requirements section of this site.

Pages were also created to allow visually impaired users to use the site effectively using a screen reading aid. For example, all images have text describing the image, Title attributes tell users where a link will take them if they click on it, and structured headings are used so users can get an overview of the site and jump quickly to desired sections.

Exceptions

- Calendar pop-ups for our product application forms and our calculators do not function if the Cascading Style Sheets are switched off when you view the site. If you are using a screen reading aid to help you, it will not be able to read the contents of the calendar. Simply enter the date manually by typing it in the following format: MM-DD-YYYY.
- In our Products and Services section of the site, on both request forms and application forms, a screen reading aid will read the first heading of the form twice.

Adjusting your Browser Settings

Our Internet Banking service can be adapted for use by partially sighted members. You can change some of the options in your Internet browser and, using the latest version of Netscape or Internet Explorer, you will be able to:

- alter the size and colour of most text (but not images)
- alter the background colour (black text on a yellow background gives the most contrast)
- alter the line length, by changing the size and shape of your browser window
- override the colour schemes of this website and others with your preferred settings

Refer to the accessibility topic in the help section of your browser for details on how to change your browser settings.

Technologies Used

If you are technically inclined or wish to know more about how we achieve accessibility on this site, you may be interested in reading below.

- All pages on this site were authored using Extensible Hypertext Markup Language (XHTML) 1.0 Transitional for markup.
- Cascading Style Sheets (CSS) have been used for visual layout, which follow the principle of separating content from presentation. If you are having difficulty reading the web pages because of the colours, fonts, etc, you can disable the CSS on your browser to view the site. Best efforts have been made to make the site functional without the use of CSS or JavaScript, although the look and layout will be significantly altered.
- Some pages on this site have been created using JavaScript (DOM 1/2) for browser effects.
- All pages in this site use structured semantic markup. H1 tags are used for main titles, H2 tags for subtitles, etc. This helps users get an overview of the site when using an access aid and jump quickly to desired sections of the site.
- Many links have TITLE attributes, except those where the text of the link already fully describes the target. These attributes describe where a link will take you if you click it to help you navigate effectively through the site.
- This site has been checked using W3C Validators for both XHTML and CSS. However, some features, such as banking and calculator pages, use legacy code and may not validate.

Testing and Validation

To test for compliance, we have used the following accessibility aids and resources:

- W3C WCAG Guidelines
- IBM aDesigner version1.02 - a disability simulator that helps Web designers ensure that their pages are accessible and usable by the visually impaired.

- JAWS 4.51 Screen reader software for the visually impaired.
- This site has been checked using W3C Validators for both XHTML and CSS. However, some complex interactive features of this site, such as banking and calculator pages, may not validate.
- This site has been cross-checked using Internet Explorer (5.5 +, PC only), Netscape (7.2+, PC only), FireFox (1.0, PC and Mac) and Safari (1.2 +, Mac only).

Your Privacy

Your Privacy is Important to Us

We are committed to protecting your privacy and safeguarding your personal and financial information. While the Internet is revolutionizing the way that we do business — providing convenient access to financial services from your home or office — we also recognize that it may bring legitimate concerns about privacy and security.

Please refer to our [Privacy Code](#) to learn about our commitment to your privacy. To learn more about your privacy and this website, please refer to the [Privacy Online page](#).

Privacy Online

This information page describes in general terms how your personal information is collected and used within the online banking section of our site. The online banking area of the site is the area of our website that requires you to use your Member ID and Personal Access Code (PAC) to enter.

Controlled Access to your Information

To ensure that you are the only person accessing your personal financial information, we restrict access to the online banking section of the site by requiring that you enter your Member ID and PAC to login. Only you know your PAC. Our employees do not have access to your PAC, and they will not ask you to reveal it. If someone does ask you to provide your PAC to them, we ask that you refuse to do so and contact us immediately.

Transactional Services

By nature, our Internet banking site has many transactional functions such as transfers between accounts and bill payment functions. These transactions are all logged to ensure that your accounts are debited or credited appropriately, and a history of each transaction is available to

verify your account information. We store and use your transactional information in the same fashion as if you performed the transaction at a branch or through any other service channel.

We may also use transactional information for servicing your account — for example, billing you for the particular transactions that you perform, or for the services that you use.

Creating a Secure Channel

We create a secure channel between your browser and our server to protect your information when you use the site. To learn more about how we do this, [please review our information on Internet Security](#).

Application Forms

To provide you with a convenient method for applying for loans and mortgages, or for purchasing other financial services products such as Registered Savings Plans, we may provide secure online application forms. These forms capture personal information that we use to provide you with the products and services you request. This information is processed in a similar way to application forms received through our other channels .

Website Usage Statistics

To continually improve our site, we often collect statistics about how our members are using it. These usage statistics are only viewed in the aggregate and are not associated with you as an individual. We use this information for purposes such as improving the pages where our members are having difficulties.

The information collected may include your IP address, your browser type and your operating system, as well as data such as the number and types of pages visited, and the length of time spent per page and on the site overall.

Our use of Cookies

We also use a key web technology called cookies. A cookie is a small information token that sits on your computer. As you use this site, cookies are passed back and forth between our server and your browser.

Specifically, we use two kinds of cookies — session cookies and persistent cookies. A session cookie exists only for the length of your browsing session and is deleted when you close your browser. A persistent cookie is a cookie that stays on your computer after you close your browser. A persistent cookie may or may not expire on a given date.

We use a session cookie to maintain the integrity of your online banking session. With each page that you visit, the cookie is passed back and forth between our server and your browser. We use

the cookie to distinguish your session from the many others that may be happening at the same time. Our session cookies never store any personal information, such as your name, or date of birth, or financial information, such as your accounts and balances.

Most recent browser versions allow you to set some level of control over which cookies are accepted and how your browser uses them. For example, it may be set to notify you when it is receiving a cookie so that you accept cookies from only known, reliable sites such as this one. If you are concerned about cookies, we encourage you to upgrade your browser to a recent version and review the Help section of your browser to learn more about its specific control features.

Memorized Accounts Feature

We use a persistent cookie to store information to help you personalize the site and to make it easier to use. For example, we allow you to make the login easier by remembering your login information within our Memorized Accounts feature. Since the Memorized Accounts feature is optional, this cookie only contains information that you have entered into it. We never store your Personal Access Code (PAC) in a cookie.

Logout Button

To ensure that no-one else can access your personal information, always use the logout button to end an online banking session. It is located at the top of every page. When you exit using the logout button, we delete your session cookie so that your session cannot be resumed unless your Member ID and PAC are re-entered.

Automatic Session Time-outs

In the event that you leave your computer without logging out, the online banking feature of this site has been designed to end your session automatically if our system detects that you haven't provided any instructions or used the browser buttons to navigate for several minutes. To restart the session, you will need to provide your PAC again.

Email

To communicate with us electronically, we strongly recommend that you use our Contact Us feature. This feature provides a secure channel for sending us comments, questions or instructions.

General email is not secure since it passes through many points on its route from you to us. If you are using general email to communicate with us, we strongly recommend that you do not include personal financial information (such as account numbers) within the email as we cannot guarantee its confidentiality en route to us.

When you email us your comments, questions or instructions, you provide us your email address and we use it to correspond with you. We then store your email and our replies to you in case we correspond further.

Links to Other Sites

Our site may also contain links to other websites or Internet resources. As an example, from time-to-time we may provide links to Microsoft or Netscape to assist you in upgrading your Internet browser. However, we have no control over these other websites or Internet resources and do not control their collection, use and disclosure of your personal information. Always review the Privacy Statements of the sites that you are viewing.

Contact Us

We welcome any questions or concerns about your privacy relating to use of our website. Please use the [Contact Us](#) form to submit your questions or comments.

As we continue to expand our online banking service to serve you better, and as new Internet technologies become available, we may update the information on this page at any time, to reflect changes.