Manulife Retirement | John Hancock

Safeguarding your information is our *top* priority

Manulife John Hancock Retirement backs you up with a Cybersecurity Guarantee when you follow these online safeguards.

As part of our continued commitment to providing you with an easy, safe, and secure way to access your retirement account online, here are the security safeguards we require you to follow when creating or updating your account profile.

Is your account profile up to date?

Username

- Create a unique username for your account.
- Pick a username that's personal to you and difficult for others to guess. This should be something only you know.
- Don't use your Social Security number.

Password

- Create a unique and strong password that will be hard for others to figure out.
- A password may contain a random combination of upper and lowercase letters, numbers, and special characters (e.g., @, #, ^, %) and is at least eight characters long.
- Consider using a passphrase (and not dictionary words)—a short phrase that's easy for you to recall and strengthen using only the first letter of each word in the phrase and adding special characters. For example, "I like toast and eggs for breakfast on weekends" can be changed to "Ilt&e4bow."

Questions about security?

Call 800-395-1113

Contact us if you need assistance updating your profile or want to learn more about account security.

In an age where people share so much personal information on social media, blogs, and websites, it can be a challenge to pick unique IDs, passwords, and questions that are only known to you.

Remember, you can always update your personal and account security information by clicking on "My profile" when you sign in to your account at myplan.johnhancock.com.

Recommended browsers

Microsoft Edge

Mozilla Firefox

Google Chrome

Safari (Mac)

Also, keep in mind the following:

- Don't use common words (e.g., water, car) or any personal information.
- Don't use the same password for multiple websites—create a unique password for each of your critical accounts. Once a password is compromised at one site, it's easy for someone to try that same password for other sites.
- Don't use your username for your password—these should always differ.
- Don't share your password with anyone—including family members.
- Change your password immediately if you're a victim of identity theft.

Better security takes more than a username and password

Security question and answer

- Pick a question with an answer that's relevant to you—and that only you know.
- The answer to your security question is needed to reset your username or password online, so consider choosing a question with a concise answer that only you can easily recall.
- For security purposes, never share your security question with anyone.

Mobile phone number and email address

To enhance security further, you're required to add a mobile phone number and personal (nonwork) email address to your account profile. This allows us to send you messages when a transaction or update occurs on your account to confirm it was actually initiated by you. If you don't recognize the transaction, contact us immediately so we can act quickly to protect your account.

There's also an authentication protocol that occurs when you sign in to your online account. Any visit to the website that doesn't pass this authentication protocol results in us sending a security code to your phone number on file that you must input to complete the login process.

Transactions to update certain personal information or to request a distribution (withdrawal or loan) from your account online go through additional security protocols to help identify fraudulent activity.

Browser security

We protect our systems, data, and clients' information by using a minimum 256-bit (SSI/TLS) encryption to secure access to our websites. Only secure connections are allowed access to the authentication page.

Therefore, we recommend you use a browser that supports 256-bit encryption, is JavaScript enabled, and accepts cookies. These requirements help ensure the safety of your financial information and allow us to track usage of the site in order to improve our service to you.

If your browser doesn't support 256-bit encryption, consider updating your browser. The latest versions of Microsoft Edge, Mozilla Firefox, Google Chrome, and Safari (Mac) offer 256-bit encryption as a standard feature.

See complete details on our **Cybersecurity Guarantee**.

Steps to help keep you safe online

- Fraudsters are out there looking for user credentials to steal. They're looking to impersonate people or organizations in order to trick you into disclosing sensitive information. Methods can include shoulder surfing, social engineering, and simple guessing based on online profile information (e.g., Facebook or LinkedIn). So make it as difficult and time consuming as possible for others to guess your credentials.
- When logging in to a website with your personal credentials, type the web address in the browser yourself, rather than clicking on a link from an email or a search engine. Look for signals that a website is secure, such as a URL that begins with "https" ("s" stands for secure).
- Be wary of emails you don't recognize or that look suspicious, as they could be phishing attempts.
- Be cautious about opening attachments or downloading files, regardless of who sent them.
- Don't send personal or financial information by email or text.
- Review your statements or transaction details as soon as you receive them. If you notice anything unusual or your statement arrives late, contact us to confirm your profile information and account balances.
- Become "malware aware" and stay away from suspicious websites, so your computer or device doesn't become infected. Make sure you're on the right site!
- Always update your web browser and use the latest versions of Microsoft Edge, Mozilla Firefox, Google Chrome, or Safari (Mac).
- Install antivirus and malware protection software on your home computer, and enable automatic updates.
- Download operating system and software updates only from trusted sources.
- If you have broadband or an "always on" internet connection, enable firewall software on your computer.
- Don't select "Remember passwords" in your browser.
- Understand the risks of using free Wi-Fi hotspots.

Manulife Retirement | John Hancock

See the full guarantee for eligibility requirements. The guarantee is available at myplan.johnhancock.com.

GT-P636983 GE 07/25 301150 GA0616254577000 | RET-301150