Safeguarding your information is our top priority

John Hancock backs you up with a Cybersecurity Guarantee when you apply and follow these online safeguards!

John Hancock takes the protection of your account seriously. As part of our commitment in continuing to provide you with an easy, safe and secure way to access your retirement account online, here are the security safeguards that we require you to follow when creating or updating your account profile.

Is your account profile up-to-date?

User ID
- A User ID is a username that uniquely identifies you and your account.
- Pick a User ID that is personal to you and difficult for others to guess. This should be something only you know.
- Do not use your Social Security number (SSN).

Password
- Create a unique and strong password so that it will be hard for others to figure out.
- Pick a random combination of upper and lowercase letters, numbers and special characters (e.g. @, #, ^, %) that is at least 8 characters long.
- Consider using a passphrase; a short phrase that’s easy for you to recall, which you strengthen by adding special characters. For example, “eggs for breakfast” can be changed to “eggs4bre@kfast or “Egg$4breakfast”.

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 websites. 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 User ID for your password – these should always differ.
- Don’t share your password with anyone – including family members.
- Change your password immediately if you are a victim of identity theft.

John Hancock Life Insurance Company (U.S.A.) (John Hancock USA) and John Hancock Life Insurance Company of New York (John Hancock New York) are collectively referred to as “John Hancock”.

John Hancock backs you up with a Cybersecurity Guarantee when you apply and follow these online safeguards!
“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 log into the website.

Better security takes more than a user ID and password

Security question and answer

- Pick a question with an answer that is relevant to you but only known to you.
- The answer to your security question is needed to reset your User ID or password online, so choose 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

For even greater security to protect your information, you are required to add a mobile phone number and personal (non-work) email address to your account profile. This allows us to send you a text message or email when transactions to update certain personal information are made. 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 are logging into your online account that does a second level check to verify that you are indeed the account holder. Any visit to the website that doesn’t pass this test for any reason will result in the need for us to send you a passcode in order for you to complete the login process.

Additional protocols help protect your account

We have procedures in place to protect your account. For example, under certain conditions, when you request a distribution (loan or withdrawal) a 15-day cooling period (or hold) may apply for wire/ACH payment methods.

Browser security

John Hancock protects our systems, data, and our clients’ information by enforcing access to our websites with a minimum 256-bit(SSL/TLS) encryption; only secure connections will be allowed access through 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 does not support 256-bit encryption, click on one of the links to update your browser. The latest versions of Internet Explorer, Mozilla Firefox, Google Chrome, or Safari offer 256-bit encryption as a standard feature.

Recommended browsers:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari (Mac)
Do these to help keep you safe online...

- Fraudsters are out there looking for user credentials to steal. They are 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 (Facebook, LinkedIn, etc). So make it as difficult and time consuming as possible for others to guess your credentials.

- When logging into a website with your personal credentials, type in 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 do not 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 via email or text.

- Review your statements or transaction details as soon as you receive them. If you notice anything unusual or your statement is late in coming, contact us to confirm your profile information and account balances.

- Become ‘malware-aware’ and stay away from shady websites so your computer/device does not become infected. Make sure you are on the right site!

- Always update your web browser and use the latest versions of Internet Explorer, Firefox, Google Chrome, or Safari.

- Install anti-virus 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 Wifi hotspots.
Cybersecurity Guarantee

John Hancock backs up your retirement account with a Cybersecurity Guarantee. If someone takes cash from your covered accounts through no fault of your own, John Hancock will reimburse your account the amount of cash taken.²

TO BE ELIGIBLE FOR JOHN HANCOCK’S CYBERSECURITY GUARANTEE:

FOLLOW PRUDENT ONLINE SECURITY PRACTICES¹ and maintain up-to-date contact information with us so we can contact you if we suspect unauthorized activity.

- Never share your account access information, including username, password, and answers to security questions.
- Use unique and strong usernames and passwords for your John Hancock accounts, and change your password immediately if you are a victim of identity theft.
- Remain current with security protections on your email, accounts, and devices, including anti-spyware and antivirus software, changing passwords when accounts may be compromised, and enabling automatic updates.

NOTIFY US IMMEDIATELY AT 1-800-395-1113 if you are a victim of identity theft or if you suspect unauthorized activity in your retirement account.

- Regularly monitor your account for unusual activity, promptly reviewing written and electronic correspondence, account statements, and confirmations as they are made available to you.
- Notify us within 30 days that you intend to make a claim on this Cybersecurity Guarantee.

COOPERATE IN GOOD FAITH with any investigation.

- We may ask you to take follow-up actions like having a professional computer security company clean your computer hard-drive or asking you to file a police report, provide an affidavit, or sign a release.
- John Hancock will determine the applicability of the Cybersecurity Guarantee and any amounts due to you.

OUR SIGNATURE IS BEHIND IT.

¹ "Covered accounts" includes your retirement accounts with John Hancock, such as a 401(k) or profit sharing plan, for which John Hancock Retirement Plan Services is the record keeper.
² See Guarantee, available at jhpensions.com and jhnypensions.com, for full eligibility requirements.
³ Recommended online security practices are available at jhpensions.com and jhnypensions.com.
John Hancock Life Insurance Company (U.S.A.) (John Hancock USA) and John Hancock Life Insurance Company of New York (John Hancock New York) are collectively referred to as "John Hancock".

Group annuity contracts and recordkeeping agreements are issued by: John Hancock Life Insurance Company (U.S.A.) ("John Hancock USA"), Boston, MA (not licensed in New York) and John Hancock Life Insurance Company of New York ("John Hancock NY"), Valhalla, NY. Product features and availability may differ by state. John Hancock USA and John Hancock NY each make available a platform of investment alternatives to sponsors or administrators of retirement plans without regard to the individualized needs of any plan. Unless otherwise specifically stated in writing, John Hancock USA and John Hancock NY do not, and are not undertaking to, provide impartial investment advice or give advice in a fiduciary capacity.

NOT FDIC INSURED | MAY LOSE VALUE | NOT BANK GUARANTEED
© 2018 All rights reserved.