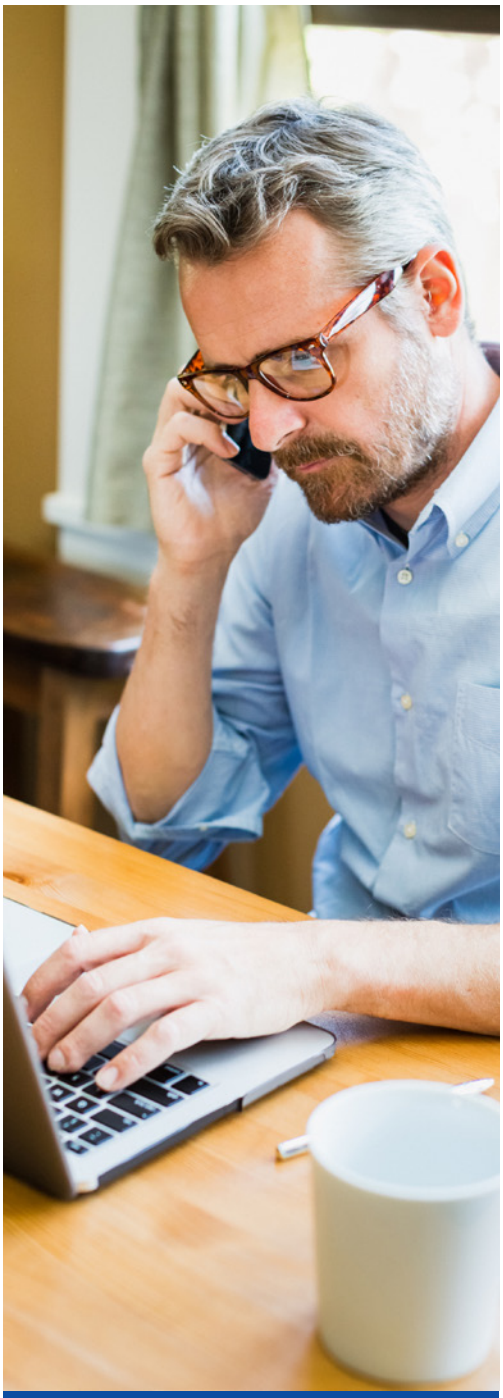

John Hancock

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?

Username

- A username uniquely identifies you and your account.
- Pick a username 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 that will be hard for others to figure out.
- Pick a random combination of upper and lowercase letters, numbers and special characters (e.g. @, #, ^, %) that's at least 8 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?

One-on-one support
800.294.3575
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 log into the website.

Recommended browsers:

- Internet Explorer
- 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 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 username 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.

Better security takes more than a username 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 username 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

To enhance security further, 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 security-related 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 are logging into your online account. Any visit to the website that doesn't pass this authentication protocol will result in us sending you a security code to your email or phone number on file that you must input to complete the login process.

As well, transactions to update certain personal information or to request a distribution (withdrawal or loan) from your account online will go through additional security protocols to help identify fraudulent activity. In these situations, we will send a security code to the personal email address or mobile number we have on file for you. You will then have a limited amount of time to enter that code into the site to authorize and confirm that transaction.

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 10-calendar day cooling period (or hold) may apply.

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.

John Hancock's Cybersecurity Guarantee – our promise to you!

At John Hancock, your trust and the security of your account is important to us. By doing your part in keeping your John Hancock accounts safe online, we will back you up with a Cybersecurity Guarantee.

For more information, read the attached **Cybersecurity Guarantee Certificate**.

One-on-one support
800.294.3575
Representatives are available between 8 a.m. and 10 p.m. Eastern time on New York Stock Exchange business days. For your protection, all calls to a representative are recorded.

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.

Visit us online at **johnhancock.com/myplan**

John Hancock

John Hancock's Cybersecurity Guarantee in full is available at JHRPS.com/CybersecurityGuarantee-OA

John Hancock Retirement Plan Services, LLC offers administrative or recordkeeping services to sponsors and administrators of retirement plans, as well as a platform of investment alternatives that is made available without regard to the individualized needs of any plan. Unless otherwise specifically stated in writing, John Hancock Retirement Plan Services, LLC does not, and is not undertaking to, provide impartial investment advice or give advice in a fiduciary capacity. John Hancock Trust Company LLC provides trust and custodial services to such plans.

MS-P30898-GE 09/19-39956 MS070319495401 | 16793

John Hancock

Cybersecurity Guarantee

John Hancock backs up your retirement account with a Cybersecurity Guarantee. If someone takes cash from your covered accounts[1] through no fault of your own, John Hancock will reimburse your account the amount of cash taken.[2]

TO BECOME ELIGIBLE FOR JOHN HANCOCK'S CYBERSECURITY GUARANTEE:

FOLLOW PRUDENT ONLINE SECURITY PRACTICES[3] 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're a victim of identity theft.
- Remain current with security protections on your email, accounts, and devices, including antispyware and antivirus software, changing passwords when accounts may be compromised, and enabling automatic updates.

NOTIFY US IMMEDIATELY AT 800-294-3575 if you're 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're made available to you.
- Notify us within 30 days that you intend to make a claim pursuant to this Cybersecurity Guarantee.

COOPERATE IN GOOD FAITH with any investigation.

- We may ask you to take follow-up actions, such as 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" include your retirement accounts with John Hancock, such as a 401(k) or profit-sharing plan, for which John Hancock Retirement Plan Services, LLC is the recordkeeper. **2** See Guarantee, available at johnhancock.com/myplan, for full eligibility requirements. **3** Recommended online security practices are available at johnhancock.com/myplan.

MS-P 37374-GE 02/20 41526

MS020320508599 | 19244