



Safeguarding Against Financial Scams and Identity Theft

Most of us have seen stories in the news media, known someone, or maybe even been a victim of a financial scam or identity theft. Large scale cyber data breaches where personal identifying data is compromised like the one at Equifax increase the risk of this happening. An area that is increasingly being targeted by identity thieves and financial scammers is retirement accounts such as 401(k) and pension plans. As a result, Siemens Healthineers is reaching out to let you know what we are doing to safeguard your information, as well as share some steps you may take to protect yourself against fraud and theft.

What we're doing to safeguard your information ...

If you have a Siemens Medical Solutions 401(k) plan balance, the Siemens Healthineers Benefits Center (SHBC) has a twenty-five day waiting period to process a withdrawal request from your account when your direct deposit banking information is changed. While this may require you to plan for additional lead time when making a withdrawal, it allows time for you to receive a letter via US mail notifying you of the bank account change. For those with a Siemens Medical Solutions pension benefit, built-in waiting periods when changing your direct deposit information are already in place and will continue.

The SHBC will send you a notice by postal mail and/or email when the following information is changed within your account: User ID, Password, Security Question Answers, Address (Permanent or Alternate), Communication Delivery Preference, Email, Phone Number, and Financial Information. Open and read these notices promptly and contact the SHBC immediately if you did not request the changes.

All notices sent to you by the SHBC will contain the "Siemens Healthineers" logo at the top. Whether calling or using the website, the SHBC requires you to provide your personal password to secure your account. The SHBC recently rolled out enhancements to password security, including separate phone and website passwords, stronger website password requirements, and requiring password changes every 90 days. In addition, when you use the myshsbenefits.com website, a two-step verification process is required if the computer or device you are using is not recognized. In this instance, you will be prompted to verify your identity to gain access to the site. Depending on the valid personal data you have on file with the SHBC, this may include receiving an access code via text message or phone call. If you have security questions set up for your account, you may also have the option to answer those security questions.

If the SHBC has a need to call you, the representative will identify themselves and ask if you know your password. If you do, then the representative will have you enter your password into the automated phone system (rather than telling the representative directly) before proceeding with the call. If you do not know your password, the representative will discuss alternative options to access your account or reset your password. Alternative options to access your account include a one-time code sent to an existing mobile phone number or email address on file. If you do not have a valid mobile phone or email address on file with the SHBC, the representative will discuss the password reset process. They will not ask for your full social security number, though they may ask for the last 4 digits. If you are not sure that the call is legitimate, end the call and dial the SHBC directly using the normal phone number, **833-935-3328**.

What you can do to safeguard your information ...

You are a key factor in protecting yourself against financial scams and identity theft. Though not comprehensive, below are some steps you may take to safeguard your data and your money:

- Make sure your contact information is up to date with the SHBC, especially if you have recently moved.
- Open mail sent via email or US Postal Service from the SHBC immediately upon receipt, and promptly review notices from the SHBC about any type of account changes.
- Use a strong User ID and password for online access to your SHBC account. It should differ from other user IDs/names and passwords you have. Keep your password secure and change it regularly.
- Add your current email address to your account and select it as your preferred method of correspondence so you will be notified immediately when important changes are made.
- Use strong passwords for your personal email account and other online accounts. You should protect your personal email account in the same manner in which you protect your SHBC account. Strong passwords consist of letters, numbers and characters.
- Set up security questions on the myshsbenefits.com website if you do not already have them set on your account. You may find this by Clicking on "Your Profile" in the top right corner of the home page, then select "Log On Information."
- Avoid choosing security questions where scammers could find the answers online or in social media. Be mindful of common answers to security questions; for example, how many people might list "Rover" or "Bandit" as the name of their first pet?
- Check your retirement account often. Check the balance and your listed addresses, phone numbers and emails. Immediately notify the SHBC if there is a problem.
- Avoid checking your accounts from public computers, or by using a public wireless network. Only use wireless networks that you trust. If you have a home wireless network, install passwords. When you are finished with a session, make sure you log out of your account and close the internet browser when you are done.
- Restrict access to your personal computer and mobile devices used to access the SHBC website.
- Be careful what you share on social media.
- Never provide personal information, such as your bank account number, credit card number, or social security number in response to an email. Do not click on an attachment or link from an unknown or suspicious source.
- Learn to recognize phishing emails and calls. Do not trust calls from individuals claiming to represent the IRS or financial institutions. Check for correctness of the Sender's email address. Scammers will attempt to trick you into believing the email is valid using an email address with a minor misspelling or use of common domains such as @gmail.com.
- Be aware that someone you know may use your identity to steal from you. Safeguard your personal information even from them.

While some of these precautions take time, they reduce your odds of becoming a victim of identity theft and fraud. Security measures are not foolproof, and anyone can suffer a moment of inattention or lapse in judgment. Nevertheless, awareness and basic prevention practices can protect you from the vast majority of attempts to steal your identity or money through fraudulent schemes.

For More Information

- **Online:** myshsbenefits.com.
- **Phone:** 833-935-3328 between 10 a.m. and 6 p.m., Eastern time, Monday through Friday. Generally, you'll have a shorter wait time if you call after Tuesday.