Added protection for your Security Benefit account

In 2022, consumers lost $3.8 billion to investment scams.[1]

Fighting fraud together with ID.me

Security Benefit and other retirement plan administrators are implementing ever-more stringent cybersecurity protocols to prevent criminals from accessing retirement accounts.

We are implementing the identity verification platform ID.me to add an additional layer of protection to all online accounts. With a few simple steps upfront, you can work with us to keep your savings away from cybercriminals. ID.me technology meets the highest federal standards and simplifies how you safely share and prove your identity across business and government sectors.

Customers who have not completed the ID.me process will be unable to access their accounts, and financial professionals need to complete verification to view client accounts and information.

What is ID.me?

ID.me verifies your identity and helps mitigate the risk of unauthorized access while making it easy for customers to complete a one-time identity verification process.

Learn More About ID.me

Why it Matters

Whether you're a financial professional or a client, safeguarding savings means being savvy about fraudulent schemes. Retirement plans are popular targets because they typically have more money than a checking or savings account.

Cybercriminals can gain access to your account information, deplete funds, and even change contact information without your knowledge. These attacked are called *Account Takeovers*. By the time you discover you've been hacked, your savings could be substantially diminished. In the U.S. in 2021, account takeovers resulted in:

- $11.4 billion in losses.
- A 307% increase in attacks year over year.
- 22% of all U.S. adults had been victims at some point.
- 1 in every 140 login attempts was estimated to be an attempted takeover.

How to Protect Yourself

1. **Check Pay Stubs Against Statements**
   Check that the appropriate contributions have been made. If information is incorrect or missing, contact your Human Resources department.

2. **Stop Paper Statements and Use Online Access**
   Your mailbox can be a source of personal investment information for cybercriminals. Online statements and access allows you to check your account at any time and offers proactive intervention.

3. **Opt-in for Account Notifications**
   Texts or emails let you know immediately about account activity.

4. **Scrutinize Emails**
   Phishing emails can give cybercriminals access to personal data, bank accounts, and more. Ask yourself: Did the email come from an odd address, such as Gmail instead of a company account? Does the content have poor grammar or convey a sense of urgency? Verify all emails before transferring funds and contact your financial professional and financial institution immediately if you believe you are a fraud victim.

5. **Research Investments**
   Be wary of too-good-to-be-true opportunities. Is someone using hard-sell tactics? Is there a guaranteed return on investment or claim of no risk? Is the request asking you to wire funds or send a check directly to a person? (**Never give your personal information to an unknown entity without verification.**)

   Talk to your financial planner, banker, attorney, or another trusted source about whether the investment is legitimate and aligned with your goals.

   These resources can help you determine whether an entity you're considering is in good standing:

   - Your state securities regulator
   - Your state insurance department
   - Your secretary of state
   - The Securities and Exchange Commission
   - One of the retirement industry's self-regulatory organizations
   - Financial Industry Regulatory Authority (FINRA)
   - Association of American Retired Persons (AARP)

6. **Password Updates**
   Periodically changing your passwords is good practice. Avoid using personal information that could provide clues for cybercriminals. Consider using a reputable password management service.

Bottom Line

The best way to prevent fraud is to be vigilant. Monitor your statements and contact your employer, financial professional, and/or financial institution right away if something seems amiss.

---

[1] https://www.investopedia.com/investment-scams-rise-7113136

Other Sources:

https://www.forbes.com/sites/forbesfinancecouncil/2021/07/01/is-your-retirement-plan-protected-from-fraud/?sh=5b275fe77f69

https://www.investopedia.com/401-k-scams-to-avoid-5425468

Related Resources

- What is ID.me?
- ID.me FAQs
- Security Benefit ID.me instructions

SB-10032-87 | 2023-06-01