GENESYS

5 Ways to Protect Yourself from Cyber Fraud

Here's what you can do to keep your Fidelity workplace savings account safe.

1. Set up online access for your Fidelity NetBenefits® account with a unique username and password.

Cybercriminals frequently attack unregistered online accounts.

- If you're new to NetBenefits, create a UNIQUE username and password by selecting Register as a new user from NetBenefits.com.
- If you're already registered, change your username and password by visiting NetBenefits.com > Profile > Security Center.

2. Sign up for 2-factor authentication at login to further protect your Fidelity NetBenefits account.

With 2-factor authentication, an extra layer of security is added to your NetBenefits account to prevent someone from accessing your account or performing certain transactions within your account, even if they have your password. This extra security measure requires you to verify your identity using a randomized 6-digit code. You can choose to have this security code sent to your mobile phone (or an alternate phone number) via text or voice call. Each security code is used only once. It is not a password that you need to create and remember.

- Visit NetBenefits.com > Profile > Security Center to sign up.
- You must have a phone number on file in NetBenefits to be eligible for this service.

3. Add or update your mobile phone number and email address.

Get real-time alerts and confirm sensitive transactions through 2-factor authentication.

- Visit NetBenefits.com > Profile > Personal & Contact Information.

4. Sign up for eDelivery and monitor your Fidelity NetBenefits account.

Check account statements and other documents for unauthorized activity.

- Visit NetBenefits.com regularly. To receive your documents via email instead of U.S. Mail, go to Profile > Communication.

5. Enable Fidelity MyVoice®.

Eliminate the need for passwords with your personal encrypted voiceprint. The next time you call, a Fidelity Representative will offer to enroll you – you'll need to provide a Fidelity consent to create your unique voice print. To learn more, visit **https://nb.fidelity.com/public/nb/default/resourceslibrary/articles/myvoice**

Read on to learn more about online security, and how Fidelity is protecting your accounts online. Visit **NetBenefits.Fidelity.com/onlinesecurity**

6 Steps to Take if Your Identity Has Been Stolen

If you find out (or suspect) your identity has been stolen, here's what you need to do.

1. Know the Warning Signs.
Did your credit score take a nosedive? Are you questioning charges in your bank account? Did you stop receiving certain bills in the email, or worse, start receiving bills for purchases you didn't make or services you didn't use? It's possible your identity has been stolen.

2. Pull Your Credit Report and Review It for Signs of Fraudulent Activity.
You're entitled to one free copy of your credit report from each of the three major credit bureaus – Experian, Equifax or Transunion – each year via **annualcreditreport.com**. Look for inquiries from companies you haven't contacted, accounts you didn't open and debts you can't explain. Dispute incorrect or erroneous information with the credit bureaus individually.

3. Place A Fraud Alert or Credit Freeze.
As soon as you realize you're a victim, call one of the three credit bureaus to place a fraud alert or credit freeze on your account. A fraud alert mandates that creditors have to verify your identity before they issue new credit.

4. Report It to The Authorities
First, file a police report. This is important when dealing with creditors who may want proof of the crime. Then report the theft to the Federal Trade Commission, which tracks ID theft cases nationally. Go to **ftc.gov/idtheft** or call **1-877-ID-THEFT**.

5. Contact Your Creditors.
Disputing fraudulent accounts with the credit bureau is not sufficient. You need to contact individual creditors and businesses. Tell them this is a case of ID theft, provide them with a copy of your police report or FTC affidavit and they must provide, on request, copies of all applications and transaction information on the account. Any accounts you didn't open yourself should be closed. Change your passwords and/or PINs with these businesses to make them stronger.

6. Stay Vigilant.
Even if you don't suspect you are a victim of identity theft, regularly pull one report every four months to review as a preventive measure. Consider signing up for credit monitoring. Often, if you've been the victim of a data breach, you will be offered this service for free. Also, be wary of emails requesting confidential information – and don't click on links within unsolicited emails.

Fidelity Live Workshops

Get timely financial tips and learn how to maximize your retirement savings with Fidelity's Live Web Workshops. To register for a Web Workshop, log onto **https://netbenefits.fidelity.com/livewebmeetings**.
All times are Pacific Standard Time.

SEPTEMBER 2021
WEB WORKSHOPS

ALL TIMES ARE PACIFIC

Monday	Tuesday	Wednesday	Thursday	Friday
20	21	22	23	24
9:00 AM Get Started and Save for the Future You 11:00 AM Prepare for the Reality of Health Care in Retirement	9:00 AM Identify and Prioritize Your Savings Goals 1:00 PM Organize, Plan, and Own Your Future	7:00 AM Learn the Basics of When and How to Claim Social Security 1:00 PM Create a Budget, Ditch Your Debt, and Start Building for the Future	11:00 AM Get a Handle on Your Current Student Loan Debt 1:00 PM Take the First Step to Investing	11:00 AM Your College Planning Choices 1:00 PM Maximize Social Security in Your Retirement Strategy
27	28	29	30	
9:00 AM Five Money Musts 11:00 AM Manage Unexpected Events and Expenses	7:00 AM Invest Confidently for Your Future 9:00 AM Maximize Social Security in Your Retirement Strategy	11:00 AM Navigating Market Volatility 1:00 PM Make the Most of Your Retirement Savings	7:00 AM Create a Budget, Ditch Your Debt, and Start Building for the Future 1:00 PM Learn the Basics of When and How to Claim Social Security	

Upcoming BrightPlan Webinars

Friday, September 24th, 2021: Understanding Flexible Spending Accounts
Time: 10:00-10:30 AM, PST
Registration Link: **https://web.brightplan.com/register/finance-fridays-understanding-flex-spending-accounts**
Description: Should you decide to contribute to an FSA during open enrollment? Join us to learn how contributing to a Health Care FSA, or Dependent Care FSA, or Limited Purpose FSA can help you save on predictable expenses you have each year by allowing you to pay for qualified expenses with pre-tax dollars. If eligible, FSA contributions can help your paycheck go even further and you could come out ahead financially. Join us to learn simple planning strategies to spend and save with an FSA.

Wellness Corner

How to Prepare for Flu Season

This year, it's more important than ever to keep your immunizations up-to-date. Immunizations such as influenza, hepatitis A/B, measles and the COVID-19 vaccine are designed to prevent serious illness, keep you healthy and away from the doctor's office during peak flu season.

The single best way to prevent flu is to get the flu shot. It's also important to stay home when you are sick, wash your hands often, avoid touching your eyes, nose and mouth, and keep frequently touched surfaces disinfected. Regular exercise, healthy eating and managing stress helps you fight infection and minimize recovery time if you become ill.

Plan for your immunizations today. For immunization schedules, click **here** or download the CDC Vaccine Schedules app **here**.

Please note – for UHC medical plans, CVS vaccines are no longer in-network. However, as required under Federal mandates, you can still receive COVID-19 vaccinations at no cost at a CVS clinic. MinuteClinic locations inside CVS pharmacies or Target stores are still in-network. For a list of UHC in-network locations, **click here for details**.

The Delta Variant: What You Should Know
As news on the Delta variant emerges, click **here** for the most up-to-date guidance on how to keep you and your family safe and minimize the spread. For more information on the differences between influenza and COVID-19, visit this **link**.

For VSP Participants: VSP Vision Care HIPAA Notice of Privacy Practices

VSP® Vision Care maintains a HIPAA Notice of Privacy Practices (Notice) describing how health information about individuals covered under our vision care services insurance plans may be used and disclosed. The HIPAA Privacy Rule requires that every three years we notify individuals currently covered by a VSP plan of the availability of the Notice and how to obtain the Notice.

The attached notice describes how medical information about you may be disclosed and how you can get access to this information. **Click here for more details**.

Medical (UMR with UHC Choice Plus)	Medical (Kaiser Network)	Medical (Hawaii)