Dear Participant,

As the pandemic has required us to socially distance, people have relied on alternate ways to stay connected. A recent report in the *New York Times* found that traffic to Facebook's website has increased 27% during the pandemic. While social media can offer an online community for us to share with our family, friends, coworkers and others, we must stay vigilant against scams and take precautions to protect sensitive information online. Today, we'll share some risks and best practices for staying safe on social sites.

There has also been an increase in the use of websites to conduct financial transactions, due to long phone wait times and restrictions around in-person access to banks and other institutions. While Wespath's call center is open and available to serve you with normal wait times and service levels, we still encourage you to use Benefits Access for most of your participant account management needs.

Benefits Access will be even easier to use in June, as enhancements to the site will make it:

- More intuitive, so that it's easier to find information quickly, and
- Easy to read on smartphones and tablets, with a screen that is configured to fit the device

In the coming weeks, we will provide sneak peeks of the design and share more information about the site refresh—so stay tuned!

Our website and social media pages should remain your first stop when looking for the most current information about Wespath's COVID-19 response and our plans and services. So visit us at wespath.org and follow us on Facebook and Twitter.

Stay Safe on Social Media

Social networking sites like Facebook, Twitter, LinkedIn and Instagram are great tools for connecting, but they can also be data mines for criminals. Many financial institutions secure your accounts with challenge questions as an extra layer of security to protect your accounts and verify your identity. However, if you have a social media account, you may be freely sharing those answers with anyone you "friend."

By their nature, social sites are personal, but you should consider anything you post online to be public. Messages that most consider to be innocuous could make you vulnerable even if you have a high security setting on your account. The websites you subscribe to, the apps you download, the games you play and the "challenges" you take part in on social networking sites all contain personal information about you—some may even be designed to collect your data.

For example, the FBI reported on a recent trend where people shared their high school photo to support the class of 2020. Those who took part exposed their school name, mascot and graduation year—all common password-retrieval security questions. Other

examples noted by the FBI include posting a picture of your first car; answering questions about your best friend; providing the name of your first pet; identifying your first concert, favorite restaurant, or favorite teacher; and tagging your mother, which may reveal her maiden name.

Some social media privacy threats are tied to COVID-19. An April article from *Forbes Magazine*'s website warned of quizzes claiming to test a person's knowledge of coronavirus and the impact of the pandemic. In reality, some of these quizzes are designed to obtain personal information and facilitate identity theft.

How to Protect Your Private Information

There are ways to make it more difficult for criminals to access your information. Follow these tips to stay safe while connecting via social media:

- Use a complex password for your social accounts and set up multi-factor authentication.
- Set your privacy settings to high or "Friends Only" and use available "Do Not Track" features.
- Check for a blue verified badge next to the account name, which indicates an official account.
- Periodically check your social accounts—unused social accounts can be targeted by hackers, who could post fraudulent messages under your name.
- Don't reveal your location in your profile or geotag your pictures with your location.
- Beware of shortened URLs, such as those created on bit.ly and TinyURL—hover over the link to view the full URL in the lower corner of your browser.
- Contact your friends in real life before accepting "friend" requests to ensure you're not being targeted by an imposter account.
- Be careful when signing up for giveaways—they may be scams designed to steal your information or may contain malicious links.
- Beware of the terms and conditions of quizzes and social apps (e.g., "What's your personality type?" Or "Which celebrity is your spirit animal?"). Some may give the developers access to your name, pictures, friends and account history, IP address and device, as well as permission to sell your data to third parties.
- Don't post status updates sharing information that can be used to answer security questions.
- Never publicly post any of the following on your social accounts:
    - Full name
    - Date of birth
    - Hometown
    - Relationship status
    - Nicknames
    - Children's names, schools or birth dates

If you think you've been a victim of a coronavirus scam, contact law enforcement or report it to the FCC here.

For Your Education

UMPIP Webinar—Today at 11:00 a.m.
Wespath will offer a 30-minute webinar on **Wednesday, May 20** at **11:00 a.m., Central time** to explain how saving in the United Methodist Personal Investment Plan (UMPIP) can help prepare you for your financial future. The webinar will provide tips on

maximizing tax benefits, deciding on contribution options, managing your investments and more.

Register today!

a general agency of The United Methodist Church

wespath.org

Our address is 1901 Chestnut Ave., Glenview, IL 60025, USA

To contact Wespath Benefits and Investments, click here.