MERCER

KEEPING YOUR INFORMATION SAFE

MULTI-FACTOR AUTHENTICATION AND ONLINE SECURITY TIPS

As online security threats increase, Mercer is taking steps to help keep your information safe. Learn about Mercer's new security access step known as multi-factor authentication and best practices you should follow for improved online safety.

Multi-factor authentication

In order to better protect your online information, we have improved Mercer system applications with multi-factor authentication (MFA). MFA combines your username and password with an additional security factor — a temporary numeric code sent to you — to confirm your identity and keep your information secure. You may already be using MFA if you access banking, social media websites, or apps.

When you use multi-factor authentication, a stolen password is not enough for an unauthorized person to gain access to your sensitive data or our critical technology systems.

What you need to do:

- When prompted on your benefits website, enter your credentials or set up your account.
- Confirm your email and add a mobile phone number as a contact method. Your contact methods must include email or SMS text message.
- Select your desired contact method to receive a temporary code.
- Enter the received temporary code to complete the authentication process and access your personal account.

Although MFA will provide an additional layer of security, please review the best practices for online safety on the next page to further protect your online accounts. If you have questions or need assistance, please call the number in the "Contact Us" section of your benefits website.

BEST PRACTICES FOR ONLINE SAFETY

It's important to know how to keep all your accounts safe from online security threats. Follow these best practices.

PROTECT: Avoid getting hacked

1. **Choose a strong password and keep it safe.** We recommend using unique, long passwords (at least eight characters, but longer is better) for each online account.
2. **Enable multi-factor authentication (MFA).** For added security, use MFA (where available) to ensure two-step verification when logging in to personal accounts. Most banking and social media websites have this feature available, but you usually need to enable it.
3. **Don't click suspicious links or attachments.** Whether you're browsing online, using social media, or simply reading your email, be wary of all links and attachments. Hover over links before clicking to see the full URL in the lower left corner of your internet browser. Only open attachments from trusted sources.
4. **Beware of phishing scams.** Sometimes even legitimate-looking emails can be fake, causing you to inadvertently divulge personal financial data to a hacker. Call the company directly using a number you know is genuine if you notice anything suspicious about the email, such as spelling or grammar errors, unusual company logos or email addresses, or a request to provide personal or financial information via a link or email.
5. **Review mobile app permissions.** Many mobile apps can track your location, browsing history, photos, calendar, contacts, etc., and share that information with third parties. Carefully review all terms and conditions before you accept, and don't give an app permission to data that is not relevant to its use.
6. **Don't download from unknown websites.** It can be tempting to download free apps, music, and games; however, you should never download from a website that you don't know and trust, since this is a common way of distributing malware.
7. **Carefully review all terms and conditions before agreeing to them.** They may contain language that allows the providers to access unnecessary personal information or resell your data to third parties.

DETECT: Recognize the signs of a possible hack

Keep an eye out for the following warning signs:

- Are you receiving fake antivirus messages?
- Are you getting strange, unexpected emails from your contacts that they say they didn't send?
- Did you try to log in to your account, but your password isn't working?
- Did you receive a notification from your account provider saying your account password was changed when you didn't change it or that a transaction was initiated that you didn't request?
- Has your language preference changed?
- Have you noticed any unauthorized account activity?
- Are posts showing up in your social media accounts that you didn't make yourself?

RECOVER: Minimize potential damage

If you think an account has been hacked, use these steps to reduce the impact to you and others.

- If you think one of your company accounts has been hacked, notify your company's IT department immediately.
- If you can still log in to your account, change your password immediately and enable two-step verification.
- Contact your account administration team immediately to notify them of the suspected security breach and follow their recommended actions.
- Warn your contacts if you think your email has been hacked.
- Change all other passwords for all your online accounts and enable two-step verification.