



Communicating With Our Members in a Digital Age

Christian Brothers Services (CBS) has a history of evolving to meet the changing needs of our members. This includes the methods we use to communicate with you. Just 20 years ago, communications were generally delivered via U.S. mail, telephone and fax. Today, our communications landscape is dramatically different. U.S. mail, telephone and fax volumes have all decreased while website content and email messages have increased.

In this new digital age, members receive a wide variety of email messages from CBS on a regular basis. These email messages from our employees along with bulk email blasts about everything from webinars to invoices to electronic issues of our *OutReach* magazine, aim to provide you with the information you want and need in a timely fashion.

Unfortunately, email communication is a target for hackers. Hackers have become very adept at creating fake email messages that appear to come from one place, complete with authentic looking logo, in order to trick you into providing them with your login credentials or other confidential data. With these threats in mind, CBS is committed to keeping the lines of communication between us as open and safe as we can. We do this in order to protect the integrity of our communications and the information and data that flows between us. To help you spot potential fake messages from CBS, we want you to know how we communicate with our members, and also various ways we will never use for communication.

Here are a few tips you can use to help spot red signals in any incoming email message.

Links:

Are you expecting the message? CNN is not randomly sending you breaking news if you did not subscribe.

Do you know the sender? Messages from Christian Brothers Services will be sent from cbservices.org.

Hover over every link in every email message before clicking. Is the link taking you to the site you are expecting?

Look for the domain. Where is this link actually taking you, www.forms.cbservices.org is legitimate; however, www.cbservices.form.org is **not**. The domain is the text immediately preceding the .org/.com/.net, etc.

If in doubt, open your browser (Chrome, Firefox, Safari, etc.) and go directly to the site you need to access. Don't click the link at all.

CBS does communicate with you:

- Regular e-blasts promoting CBS plans, programs, webinars and important company information. The emails will include promotions for the latest edition of our eNewsletters, *Maintaining Your Health* and *Risk Factor*, and our company magazine, *OutReach*. We will also send e-blasts via our customer care department regarding holiday hours, and from IT & Website Services about website maintenance. Many of our email messages also include important documents that are generated to let the administrator and member know they can login to our web-based participant and administrators section to view, print and/or download these documents.
- CBS also sends regular member satisfaction surveys via email.
- CBS utilizes a Secure Message Center (SMC), which allows us to send and receive messages in a secure environment to protect our member's personal information. To register for this service, please visit cbservices.org, scroll to the bottom of the page under the Communications header and click on the Secure Message Center link.

- Since 2011, CBS has been active on social media sites including Facebook, Twitter, LinkedIn and WordPress. If you would like to connect with us on social media, please click on any of the social media icons at the bottom of our website, cbservices.org. You will never be sent a connection request via email.
- CBS also utilizes the MyCBS.org section of our website to make communicating easy with our members. Members can login to view their risk, retirement and health plans in detail, and stay up-to-date on important news, plans and programs.

CBS does NOT communicate with you:

- We will never make outbound telemarketing calls from individual agents or robocalls for surveys and marketing purposes.
- We will never send text messages.
- Members will never be asked to send confidential or personal information such as Social Security numbers through unsecure email messages.

If you, as a member of Christian Brothers Services, receive any communication that looks suspicious, or any form of communication you have never received before, please contact our Information & Technology Services Security Team at 800.807.0100 x2326. ☀

Tom Drez is the Chief Information, Privacy and Security Officer for Christian Brothers Services.

Attachments:

Are you expecting the attachment? The only 'safe' attachment is a .txt file so any other unexpected attachment can be suspicious. Use caution.

Is the file name and message of the email specific to you, or generic/vague?

Contact the sender if you are in doubt and confirm it is legitimate before opening.

This article first appeared in *OutReach*, a Christian Brothers Services publication. Vol. 8, No. 1, 2017. Reprinted with permission from Christian Brothers Services. All rights reserved.