COMMUNICATING WITH OUR MEMBERS IN A DIGITAL AGE

December 5, 2019

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, email and iChat messages, and social media activity have all increased substantially.

As part of our mission to create a comprehensive and exclusive Member Experience, we use this evolved technology to keep our members informed in a timely and efficient manner. However, we also are aware of the inherent risk the digital age poses and want to assure and educate you of the best practices we have put into place to communicate with you and keep your information safe.

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.

Christian Brothers Services exemplifies the Lasallian tradition by understanding the needs of our members, protecting the human and financial resources of institutions and guiding member organizations in finding practical solutions to business needs.

Unfortunately, every piece of communication can be a target for hackers looking to cause harm to CBS or its members. Hackers have become very adept at creating fake email messages that appear to come from a legitimate source, complete with authentic-looking logos 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 open and safe. We do this to protect the integrity of our communications and the information and data that flows between us.

It is important to note that authentic email messages from CBS will come to you from one of our three domain names: cbservices.org, mycbs.org, or cbprograms.com.

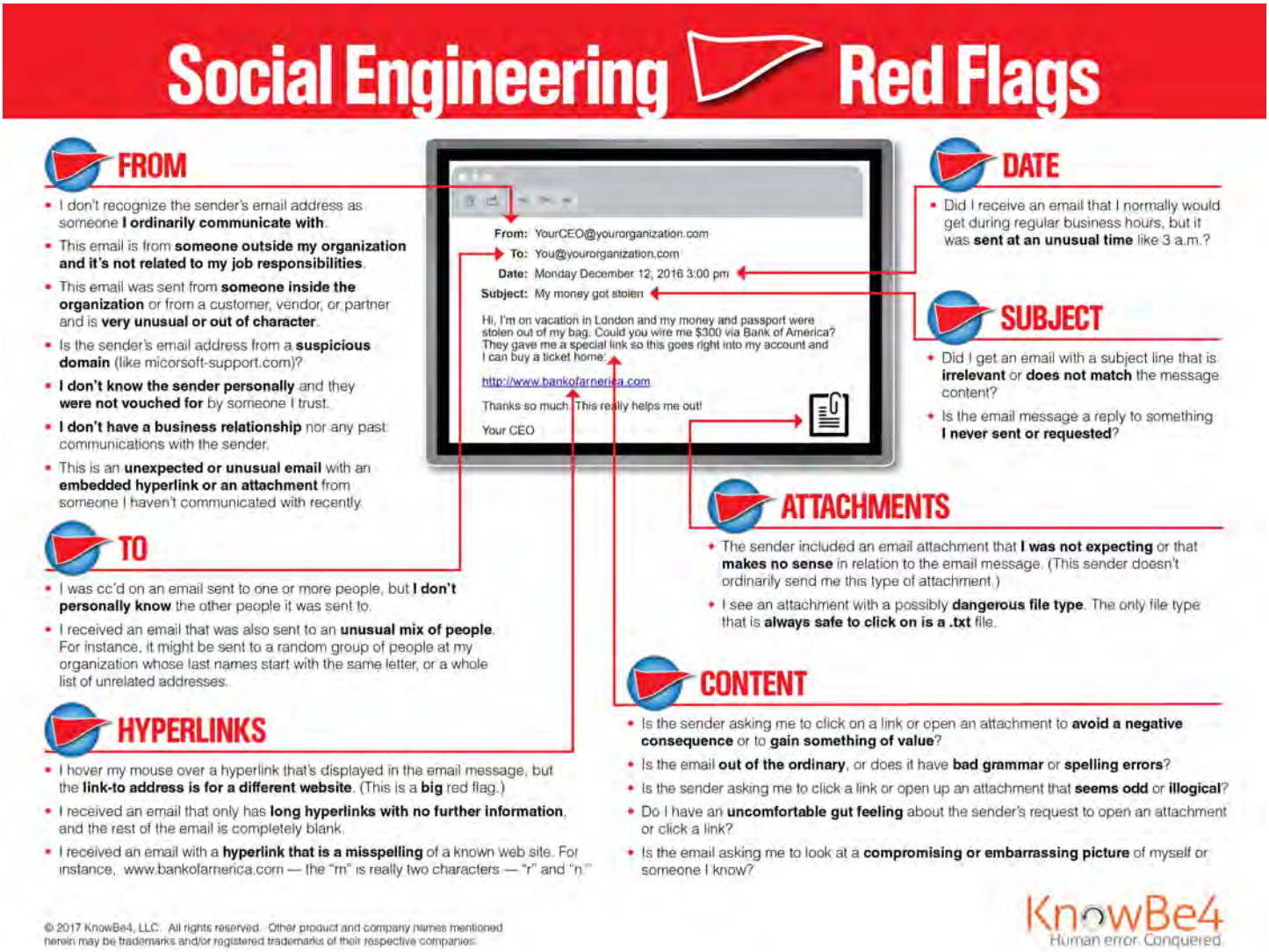
To help you spot potential fake messages from CBS, we want you to know how we regularly communicate with our members, as well as the ways in which we would never communicate.

Ways CBS communicates 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: Constellation, EBT and RMT Administrator e-newsletters, Health Benefits Services Participant e-newsletter, and our company magazine, OutReach. We will also send e-blasts from 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 log in to our web-based participant and administrator section to view, print and/or download these documents.
- CBS also sends annual member satisfaction surveys via email.
- CBS uses 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 our blog. 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.
- CBS also uses the MyCBS.org section of our website to make communicating easy with our members. Members can log in to view their risk, retirement and health plans in detail, and stay up-to-date on important news, plans and programs.
- Also, in the near future, CBS will expand our communication channels to include member text (SMS & MMS) messages.

Ways CBS does NOT communicate with you:

- We will never make outbound telemarketing calls from individual agents or robocalls for surveys and marketing purposes.
- CBS will never ask members to send confidential or personal information such as Social Security numbers through nonsecure email messages.



To help you spot potentially hazard phishing emails, please refer to this infographic from our partner KnowB4 to identify the ways hackers try to use a scam.

You can download a copy of the KB4-Phishing-Red-Flags https://www.cbservices.org/CBSBlog/wp-content/uploads/2019/12/KB4-Phishing-Red-Flags.pdf

One steadfast rule to practice safe computing is to never click on a web link in an email message that you are unsure of—often times; this can be a malicious link in which the text you actually see in an email may differ from the site the link will direct you to. If you click on it, you can be routed to a possible hacker's destination instead. To see the actual destination link, move your mouse over the web link, hover over it, and review the link that appears in the web browser's status bar. You can then review that link to determine if it matches the text in the email and is valid.

If you, as a member of Christian Brothers Services, are unsure of any communication that appears to come from CBS, please call Customer Care or your contact at CBS directly. Instead of clicking a link or phone number, you can always type the web address directly into your browser or type the phone number directly into your phone. By typing our legitimate web address or phone number yourself, you know that you are contacting CBS directly.

If you receive any communication that looks suspicious, or any form of communication you have never received before, please contact our Information & Technology Service Security Team at 800.807.0100 x2326.