Catholic Mutual…CARES

Electronic Fiduciary Transaction Requests

A request to conduct any online fiduciary transactions between your Arch/Diocese, parishes/schools, businesses and/or financial institutions can put your money and identity at risk. The key to safe online financial transactions is to always be informed of the everchanging cyber security environment and being cautious of new threats. When you receive a request to perform a fiduciary transaction, the following recommendations should have been instituted prior to and be performed during any wire transfer.

- If your Arch/Diocese and/or parishes utilize Microsoft Outlook for email, we recommend you implement the "2 Factor Authentication" (2FA), to add another layer of protection to password-protected remote access to your email. It is an authentication method that includes a password and time sensitive code, something only you will know.

  Even if a hacker has stolen your login credentials, 2FA should prevent them from accessing your email account as the hacker would also need to have the employee's mobile phone which is being utilized as the 2nd form of authentication. Please know, just having passwords is no longer enough to protect your email accounts. Remember, all online transactions should take place on a website whose address begins with: https://. The "s" means the site is secure. If you don't see the "s," do not trust the source.

- Wire Transfer Fraud is a top cyber threat to your financial accounts. Wire Transfer Fraud is when employees are deceived by criminals to wire money to a bank account controlled by them. A hacker can impersonate a bank, business (construction company), the Arch/Diocese or another parish. Every employee allowed to conduct wire transfers must be trained to be alert and always verify any changes made to the instructions of an existing wire transfer and a request to set up a new wire transfer. This verification must be conducted by calling a known and trusted phone number. Never use the contact information or phone number provided in the email request to wire transfer.
  Only allow certain employees to send wire transfers. Additionally, any transfers should be verified by two individuals to help reduce the potential of falling victim to wire fraud. All locations which use wire transfers should implement a wire fraud reduction policy which defines procedures to reduce or eliminate the risk of wire fraud.

- Training of all employees is critical in reducing your exposure to cyberattacks. Employees should be trained regularly on recognizing phishing emails to protect against email fraud. Human error is the number one cause of a cyberattack. NEVER, click any links in the contact email. Call the source of the email directly (but not by using the contact information in a potential fraudulent email), and then verify the validity of the request. A best practice to consider is to have your emails identified as coming from an external source, therefore, prompting the employee to question the true origin of the email.

  Recommended training should consist of the following:

  - Phishing
  - Employee Mistakes
  - Spear-Phishing
  - Ransomware
  - Threats of a Data Breach
  - Malware
  - Safeguarding Information

- Your email system can be configured in such a way that it filters phishing emails from getting to your employees/staff. This filtering system can quarantine suspicious emails and scan documents before they are opened. Furthermore, an alert policy can also be developed to detect suspicious behavior. It consists of having rules and conditions in place which will then notify you when those rules are triggered. This alert policy can alert you to very important security-related issues such as a malicious URL being clicked on, an email containing Malware or phishing URL's and/or infected email messages. When considering an alert policy, it is recommended to assign a higher severity level to the aforementioned activities. Checking emails and having an alert policy in place can help identify a compromised email and expose criminal activity. As such, the configuration of your email system can flag emails with similarities of your own address.

  Example: saintmarys@church.com vs. saint-marys@church.com

- Having an advanced endpoint protection system in place will also reduce your exposure to a cyberattack. Endpoint protection uses artificial intelligence, behavioral detection and machine learning algorithms to protect you and recipient of your transactions/emails. As always, once your transaction has been performed, never assume the transaction was completed safely. Always confirm with the recipient of the transaction to ensure it was submitted securely. If not, cancel the transaction immediately.

- The warning sign of wire fraud is typically an email with a request to change existing wire instructions like a bank account or mailing address. When you get an email request like this, **warning sirens should go off in your head! ALWAYS VERIFY!**

Should you need further assistance, please do not hesitate to contact your CMG Risk Management Representative at 800.228.6108.