Catholic Mutual Group
Risk Management Alert
Fake Email Payment Scams

Be careful who you pay! The use of fraudulent emails and invoices to advance schemes (email fraud) is on the rise.

Example: A construction company was scammed into paying over $200,000 to what it thought was a known vendor after receiving an email from the vendor. However, the "vendor" email was actually from criminals using an email that closely resembled or 'spoofed' a legitimate vendor of the construction company. The spoofed email stated the vendor's owner was having issues receiving payments and asked the construction company to use ACH or Wire Transfer. The construction company complied thinking the email was from the vendor. But was wrong and sent the money right to the criminal!

How to Protect Yourself
Train all employees to recognize potential phishing and spoofing emails (including always checking the email address).

- Contact requestors by phone (using known contact information) before complying with email requests to change payment methods like banking information or mailing addresses.
- Frequently monitor your email exchange server for changes in configuration and custom rules for specific accounts.
- Ensure company policies provide for verification of any changes to existing invoices, bank deposit information, and contact information.

Do you have questions or want assistance? Contact Jackie Sudia, Claims/Risk Management
jsudia@catholicmutual.org 916-639-3616 | 916-733-0281