

Email Phishing Warning



The Misericordia Family Association (MFA) communicates with Misericordia families predominantly via email. Maintaining good email etiquette and security is an important part of this process.

Phishing is the fraudulent practice of sending emails or other messages purporting to be from friends, family, or reputable companies or organizations to induce

individuals to reveal personal information.

Phishing attacks are on the rise and evolving every day. In fact, it's one of the top threats faced by organizations of all sizes around the globe. Knowing how to recognize phishing emails and what to do, and not to do, about them is everyone's responsibility.

This reminder provides general guidance on how to protect yourself against such malicious emails.

DO

- DO check links by using your mouse to hover over the hyperlink to determine if the URL makes sense with the sender—e.g., matching the sender's name to the URL; whether there's a foreign name or location in the URL.
- DO check for misspellings, grammatical errors, and abnormal spacing that may be indicative of a phishing email.
- DO use common sense—if it doesn't look right, trust your judgment.

DO NOT

- DO NOT open any suspicious email based on the Subject or Sender—delete it before you open it.
- DO NOT reply to, open attachments from, or click on URLs from unknown and untrusted sources.
- DO NOT use your company email address for personal communications.
- DO NOT ever send personal/sensitive information via email—e.g., passwords, credit card numbers, social security numbers, or account numbers.

RED FLAGS

- Does the email offer unsolicited photos for viewing?
- A suspicious sender address where the email address does not match the name in the 'From' field.
- Does the address in the 'To' field match the sender of the email?
- Does the hover-text link match what's in the text?
- Does the email ask for any sensitive/personal information (passwords, credit card numbers, SSNs, etc.)?
- Does the email ask for sensitive information about others?
- Does the email ask you to immediately act or open an attachment to avoid account closure?

When in doubt, toss it out!!