How to Spot Scam Emails: A Basic Guide

Scam emails, also known as phishing emails, are designed to trick you into providing personal information, clicking malicious links, or downloading harmful attachments. This document provides basic tips to help you identify common signs of email scams. You can expand or customize this content as needed.

1. Check the Sender's Email Address

- Scammers often impersonate trusted companies but use email addresses that look unusual, misspelled, or unrelated to the organization. If it does not say it is from "edomi.org" or "detroitcathedral.org" it is NOT the Cathedral or the Diocese. CCSP and EDOMI staff will not contact you from personal emails such as G-mail, Yahoo, AOL, etc…
- Always inspect the full email address, not just the display name as scammers will use people's names that are familiar to you.

2. Look for Urgent or Threatening Language

- Scam emails often try to panic you…claiming your account will be closed, your payment failed, or you must act immediately with their request. Please note that legitimate organizations rarely pressure you with immediate threats.
- Be cautious if the email asks for personal information, passwords, banking details, gift cards, or money. No member of staff of the Cathedral or Diocese will ever ask you for these things.

3. Inspect Links Before Clicking

- Hover your mouse/cursor over any link to preview the URL.
- If the link looks suspicious, misspelled, or unrelated to the sender, do not click it. If you clicked it by accident, quickly exit out of the page.

4. Watch for Poor Grammar, Spelling, and Odd Requests

- Many phishing emails contain obvious spelling errors, awkward phrasing, or formatting inconsistencies.
- Professional organizations usually proofread their communications.
- Never respond to emails that "need to chat for a minute" or "must have a response asap." These are scam emails trying to obtain information from you.

5. Avoid Opening Unexpected Attachments

- Scammers may attach files containing malware. Never open any attachments from an unfamiliar email.
- If you are expecting an attachment…even from someone you know…verify before opening it by contacting the person directly if you are not sure.

6. Verify Through Official Channels

- If something feels off, contact the Cathedral or the Diocese directly by phone or email provided on Cathedral Windows, the CCSP Website, and Facebook!

If you have any questions about scam emails or internet safety, please contact info@detroitcathedral.org or speak directly to your Parish Coordinator, Erin McClellan.