利用電子郵件和簡訊的釣魚和詐騙

越來越多的會眾和事工單位成為詐騙者和網絡釣魚攻擊的目標。這些電子郵件或手機短信通常會假裝他們是牧師或主教並要求進行私人對話，聲稱需要幫忙，或者購買禮物卡。

這些攻擊是網絡釣魚或詐騙。這意味著電子郵件帳戶或電話號碼可能沒有被黑客入侵。攻擊者使用備用電子郵件地址或電話號碼以及使用 AI 軟件找到聯繫人。

這種攻擊通常被稱為 CEO 網絡釣魚或商業電子郵件洩露。 2019 年，一個 FBI 報告顯示這是高達 260 億美元的詐騙手法。

這是怎麼運作的？



攻擊者確定目標（會眾、事工或教區）並搜索領導人的姓名和電子郵件地址。



攻擊者創建的電子郵件地址具有令人信服的名稱或域名，看起來與領導階層的人帳號相似。



然後，他們使用軟體查找與目標相關者的電子郵件地址或電話號碼。



他們冒充牧師或主教發送電子郵件或簡訊以徵求金錢或資訊。

如何避免或阻止詐騙

1. 檢查發送信息的電子郵件地址或電話號碼。現代電子郵件程序通常僅將名稱顯示為默認值，而不顯示電子郵件地址。攻擊者利用這一點並使用真實姓名創建地址，但使用虛假的電子郵件地址。通常會使用gmail或 yahoo 帳戶。手機簡訊詐騙者將使用您所在地區的區號，並聲稱它是新的電話號碼。

2. 在電子郵件或簡訊的語氣和語法中尋找危險信號。詐騙者會想要製造一種緊迫感，以利用您提供幫助的意願。他們經常會聲稱主教（監督）或牧師需要一些東西並且正在開會。或急需私聊。這些電子郵件可能會包含拼寫錯誤、奇怪的標點符號或稍微「偏離」的語法。仔細閱讀帶有請求的消息。

3. 詢問他人。讓其他人為您閱讀消息，看看他們是否注意到任何奇怪的事情。致電或發送電子郵件給教會或教區辦公室，以檢查此人實際的電子郵件地址或電話號碼為何。

4. 不要購買禮品卡或洩露信息。這些騙局通常要求您購買禮品卡或希望您提供更多信息（以獲得更多的詐騙對象）。切勿在未驗證信息的情況下通過文本或電子郵件請求分享信息或進行購買。

5. 報告。向此人或領導人物報告，如果您收到詐騙電子郵件或簡訊，其他人也很可能也收到了。同時向 FCC 報告。如果您是詐騙的受害者，請向當地執法部門報告。