Ratio Risk Services / Diocese of Springfield
RISK ALERT
ACCOUNT HACK RISK
No. 2022-20

Re: Phishing Scam **July 8, 2022**

Recently one of our parishes reported a spear phishing scam in the form of an email seemingly from one of their employees, requesting a change to their direct deposit information. Luckily, their email filter caught that the email address had never been used before, though it resembled a legitimate email.

Direct/automatic deposit scams like this are increasingly common and ever more sophisticated as cybersecurity risks escalate. Please do not think you or anyone on your staff are immune – anyone can fall victim to these scams. Carefully review and verify every request regarding financial matters and review our Cybersecurity checklist: https://springfieldrisk.org/knowledgebase/cyber-security-checklist-the-essentials/.

Be on your guard for unauthorized charges and always take several steps before you respond to any request for payment or for a change in the method of payment. Scammers know that once lost, there is usually no way to get your money back.

To prevent these types of cyber scams from happening to your parish or institution, please take the following steps:

- **Always look at the sender's email for clues of its legitimacy**. Examine the sender's email address closely, comparing it to previous emails or correspondence known to be legitimate. Scammers will use email addresses that look similar to a legitimate email, but you will usually find tell-tale signs that it's a fraud.
- **A transfer of funds should never be performed solely on the basis of an email exchange. Obtain verbal confirmation** by calling your known contact directly.
- **Do not call the number listed in the email or on the letter you received.** If it's a fraudulent email or letter, the number will be fraudulent as well. Always call the legitimate number of your known contact.
- **Do not share bank account numbers or other banking information over email.** Banks will never ask for your account number, social security number, name, address or password in an email or text message. They will only ask you to provide this information to verify your identity when you call them directly.
- **Frequently check your bank account for possible unauthorized payments**. Check over all charges at least once a week and flag any suspicious or unrecognized charges. Be on the alert for very small amounts that may "test" whether they can follow up with a larger amount, as this is a big red flag.
- **Check with your bank** about controls over unauthorized debits.
- **Watch for potentially misspelled Words.** It's less common these days to find typos in a fraudulent email or text, but you may still encounter it. If you find one in the message, it is most likely a scam.

- **If the tone of the email is urgent, this should be a signal for additional caution.** Never transfer money to anyone who pressures you to pay immediately, or who says this is the only way to pay.
- **When in doubt, call the IT department**

REMEMBER: STOP – CALL – CONFIRM

If you have any questions, please contact us at madeline@ratiorisk.com.