

Blast Scam Alert Table of Contents

(This document can change frequently)

Table of Contents

Bank Account, Payroll and Credit Card Scams	1
Church Vendor Scams	17
Copyright and Non-Compliant Scams	31
Email Hack Alerts	36
Gift Cards Scams	37
Invoice and Subscription Scams	40
Phishing Scams	68

Bank Account, Payroll and Credit Card Scams

8/31/22

Employee Retention Credit Scam

Over a year ago, it was determined that parishes are **not** eligible for Employee Retention Credit (ERC) and yet, it has been brought to our attention that parishes may or have received correspondence regarding Employee Retention Credit. Scammers are telling businesses that they qualify for Employee Retention Credit without really investigating if the business really qualifies, only to collect a fee. Below is a copy of a document that appears official and likely to have come from the IRS. These types of documents are only scam attempts. However, if you receive a legitimate notification from the IRS, please contact Parish Support or your Shared Accountant immediately. If you receive any documents regarding ERC please remember parishes are **not** eligible for ERC.

Thank you to Jacquie at St. Vincent De Paul for alerting us to this recent scam attempt.

Available Funds Alert
City: Marthasville

2022
E22674-59526
(202) 949-3237

Case Number:
Toll-Free:

22674-22_T#93 PH2 AADC B# 166-222024-40-26989

St. Vincent De Paul Parish
13495 S State Highway 94
Marthasville, MO 63357-2686



Please Keep a Copy of This Notice For Your Business Records

Our review dated August 5, 2022 indicates that you may have \$2,139,000 in available funds that are entitled to compensation for having Retained Employees during the pandemic. If you took a Paycheck Protection Program (PPP) loan from the Cares Act, you may also take advantage of the ERC credit. These funds are only available to the business owner/s and can be limited at your discretion.

UNDERSTANDING YOUR AVAILABLE TAX CREDIT FUNDS

Attention Owner(s) of Business Name	Evaluation Date	Case Number
St. Vincent De Paul Parish	August 5, 2022	E22674-59526
Business Property Address		
13495 S State Highway 94		
City	County	State
Marthasville	Warren	MO
AVAILABLE FUNDS		
\$2,139,000		

What you need to do:

Call (202) 949-3237 by September 2, 2022 to determine the total amount available to you. Please have your Case Number E22674-59526 available when calling our Tax Specialist.

- **YOU MAY QUALIFY FOR UP TO \$26,000 PER EMPLOYEE**
- **NUMEROUS WAYS TO QUALIFY-EVEN IF YOU TOOK PPP MONEY**
- **NO LIMIT/CAP ON FUNDING (ERC IS NOT A LOAN)**
- **ERC IS A REFUNDABLE TAX CREDIT-GET FUNDS DIRECTLY FROM THE US TREASURY**

Our ERC specialists have reached 6,030 businesses and help recover \$1,118,109,287 in tax credits and have qualified over 100,000 employees.

Call (202) 949-3237

Case Number: **E22674-59526**

www.YourERCMailer.com

22674-22

6/10/22

Curia Imposter Scam Alert

We have received a recent scam report of emails coming from scammers posing as Curia employees. An example is pasted below. This particular one claims to be from Sally Serbus asking about changing her bank account prior to the next payroll. Since this scam email appears to coming from Sally and contains her signature line, we can assume that someone she corresponds with by email has had their email hacked. Please be cautious when receiving external emails and always look at the "from" email address very carefully. If you receive a request from any staff or Curia member and you question its authenticity, please follow up with a phone call.

We strongly recommend that employees requesting changes in banking information for direct deposits do so in person and that emails are not accepted as legitimate authorization. All parishes have been informed of this concern regarding security issues with direct deposits and have been reminded to submit the direct deposit form with bank information through the secure email addresses. HR as well as Payroll continue to be on extra alert for scams and will verify banking account changes with a phone call.

These SCAM emails are sent, presumably from an employee, stating that there is a problem with their account used for direct deposit or wishing to change their direct deposit account. While not honoring email requests may seem to place a burden on the employee, you are ensuring that they securely receive their paychecks by not accepting email requests.

From: Sally Serbus [<mailto:wrship@virginmedia.com>]
Sent: Thursday, June 9, 2022 11:50 AM
To: Busciglio, Mary <MaryBusciglio@archstl.org>
Subject: D-D Update

This sender is an External Email.

Hi Mary,

Recently changed banks, can you update my payroll direct deposit information?
Previous account on record will be inactive a few days before the next pay day.

Let me know so I can send the new bank details.

Blessings,

Sally Serbus

3/4/22

PaycomOnline Scam Alert

We have received notification of a payroll phishing scam email received at a parish from PaycomOnline. This particular scam is more obvious since time card hours are entered into the Payroll Hours Application at the Archdiocese and the email is not coming from the archstl.org domain. A copy of the email received is pasted below. If you reply, it will likely take you to a log in page, asking you for your log in credentials or perhaps other personal information. Remember when reading external emails, always check to see where it is coming from, if you don't know the person, do not know what the email is regarding, or if it just seems odd, don't reply to the email. Thank you to Carol at Sacred Heart Florissant for alerting us to this email.

Begin forwarded message:

From: systemmessage@paycomonline.com
Date: March 2, 2022 at 9:47:42 AM CST
To: carol.t@gmail.com
Subject: [PaycomOnline] Action Required - Employee Self-Service
Reply-To: systemmessage@paycomonline.com

You have items on your timecard that need your attention. Please log in to Paycom Employee Self-Service and go to "Time Management" to address these items.

Thank You

Pay Period: 02/16/2022 - 02/28/2022

2/11/22

Payroll Scam Alert

Recently, we have had reports of parish staff and principals receiving emails stating they are coming from Commerce Bank with the subject "Important Documents For Your Review". When the recipient clicks on the attachment, it asks them to set up an account with password.

Always be aware, most email scams come from a scammer posing as your bank or a legitimate business. Remember when reading external emails, always check to see where it is coming from, if you don't know the person, don't know what the email is regarding, or if it just seems odd, don't click on any attachments or links within the email.

Thank you to those parishes who informed us of the scam.

1/20/22

Direct Deposit Scam

We have received reports of recent variant of previous direct deposit scams. This particular one claims to be from the pastor asking about changing his bank account prior to the next payroll.

Due to the increase of this type of scam. We are strongly recommending that employees requesting changes in banking information for direct deposits do so in person and that emails are not accepted as legitimate authorization. All parishes have been informed of this concern regarding security issues with direct deposits and have been reminded to submit the direct deposit form with bank information through the secure email addresses. HR as well as Payroll continue to be on extra alert for scams.

These SCAM emails are sent, presumably from an employee, stating that there is a problem with their account used for direct deposit or wishing to change their direct deposit account.

The emails we've seen appear as though they are coming from a current employee's email, but often the employee's email has been hacked.

While not honoring email requests may seem to place a burden on the employee, you are ensuring that they securely receive their paychecks by not accepting email requests.

11/16/21

Payroll Scam Warning

Recently, we have received reports of payroll scam emails circulating. As you can see, in the email screenshot below, the sender not only originates externally, but in this case, the sender is actually originating from an .UG (Uganda) email address. The sender of the emails may change and the wording may vary, but the emails will claim to need some sort of important action taken, and will need you to go to a website in order to complete the task.

If you were to click through to that external website, you will usually be prompted for user credentials, to log in. The scammers are relying on users to input various forms of login credentials, of which, they are recording. They will then use those credentials later for other purposes.

Obviously, some of these attempted scams are easier to recognize than others. Please remain vigilant and if you receive these emails, continue to report them.

Sent: Tuesday, November 16, [REDACTED]
To: Bernadette Kwebiha <[bkwebiha@\[REDACTED\].ug](mailto:bkwebiha@[REDACTED].ug)>
Subject: [BULK] RE: Early Pay Day: November 2021
Importance: Low

This sender is an External Email.

Good day,

The Finance and Accounts Unit wishes to advise that **payroll will be early for the month of November 2021.**

As such, the Finance and Accounts Unit (Payroll) is requesting that all staff authentication should be done:

Visit : [Payroll/authentication](#) and follow on-screen directive .

The Unit wishes to advise staff that documents submitted after the deadline will be honored in **January 2022.**

The Finance and Accounts Unit appreciates your usual kind cooperation.

7/27/21

ACH Payment Notification Scam

Please be aware there are two new email scams surfacing. A new scam email has surfaced originating from Bonnti.com email address. The subject of the email is "ACH Payment Notification" / "ETF Payment Rejected". The body of the email appears to be blank, but the email contains a single attachment, generally in a PDF format. Do **NOT** open the attachment. If you have opened the attachment, please change your password, and notify the Help Desk.

The second scam alert is an email originating from Teresa Swedholm with Family Forward and is pasted below. The email contains a "View Document" link. If you have clicked on the "View Document" link please change your password immediately and contact the Help Desk, otherwise you may safely delete the email.

11/18/19

Direct Deposit Scam

We are receiving reports from both parishes and the Human Resources Office of an increase in direct deposit scams.

Due to the increase of this type of scam (see details below). We are strongly recommending that employees requesting changes in banking information for direct deposits do so in person and that emails are not accepted as legitimate authorization. Parishes on Lawson have been informed of this concern regarding security issue with direct deposits and have been reminded to submit the direct deposit form with bank information through the secure email addresses. HR as well as Payroll continue to be on extra alert for scams.

These SCAM emails are sent, presumably from an employee, stating that there is a problem with their account used for direct deposit. Attached to the email is a form containing new banking information (sometimes a copy of a voided check) and requesting that their file be updated. The Archdiocesan Direct Deposit Authorization form may or may not be attached to the request.

The emails we've seen come from a worshipp@fastmail.com email address using the employee's name and the bank information is from GObank in Monrovia, CA. However, that information is only what's been seen and/or reported. With the rise in online banking, the documents could contain unlimited banking possibilities.

While not honoring email requests may seem to place a burden on the employee, you are ensuring that they securely receive their paychecks by not accepting email requests.

5/18/21

Amazon Phone Scam

As a follow-up to yesterday's Amazon email invoicing scam, parishes are also receiving phone calls from a scammer claiming to be from Amazon. The scammer is asking that the credit card information for a recent purchase of over \$500 be verified. Kudos to the savvy parish staff member that asked the scammer what card they had on file. The scammer hung up.

We can't repeat the warning often enough to never give out credit card or banking information over the phone or via emails. If you are concerned that there truly is a problem, contact the vendor, credit card company, or bank directly through the contact information you have on file - not what the email or caller provide.

Thank you to Corie at St. Rose of Lima for this alert.

4/19/21

Intuit Scam Alert

As you know, we are frequently being made aware of new email scams. Below is the latest email scam. In this instance, the grammar and capitalization usage is unusual and should make you question the authenticity. When receiving external emails always check to see where it is coming from and don't click on links within emails if you don't know the person or if you don't know what the email is regarding.

This particular scam appears to be coming from a legitimate Intuit address. The use of the word 'kindly' is a very good indication that it is a scam. The fact that the scammer knows that the parish uses Intuit/QuickBooks also indicates a very good chance that the address receiving the email has been compromised.

Thank you to Trish from St. Joseph for alerting us to this email scam.

From: Intuit QuickBooks <no_reply@notifications.intuit.net>
Date: April 17, 2021 at 8:11:21 PM CDT
To: frsamson@stjojo.net
Subject: Alert Message

Dear User,

Thank you for choosing Intuit Payment Solutions. Your last Deposit could not be completed.

You need to verify your last Transaction in order to complete your Deposit.

Kindly Logon below to Verify

www.intuit.com

Thank You,
Intuit Team

1/21/21

Financial Audit Scam

Another email scam has surfaced claiming to be a well-known vendor requesting all payments be made via ACH. Pasted below is a copy of the email. In this instance, the unusual grammar and the vendor's name being spelled incorrectly should make you question the authenticity. Always question external emails regarding payment methods and updated banking information. When receiving external emails always check to see where it is coming from and don't click on links within emails if you don't know the person or if you don't know what the email is regarding.

We also contacted the vendor directly (not using contact information in the email) and the vendor confirmed that, indeed, it is a scam.

Thank you to Susie from Shared Accounting for alerting us to this email scam.

Good Afternoon,
We are currently having our Q1 financial audit and would like to inform you that our method of receiving payments has changed.

We will no longer be able to pick up checks, we are only accepting ACH for payments. Let me know if payment is coming our way soon, So I can send you a copy of our updated banking instruction..

Tamara Herrmann

Accounts Receivable Supervisor

Rottler Pest Solutions

314-426-6100 x127

"Like" us on Facebook: www.facebook.com/RottlerPest

Follow us on Twitter: www.twitter.com/rotlerpest

9/24/20

Commerce Bank - Another Scam Alert

Below are three email scams that have been received by parishes in the last 24 hours. If you received any emails similar to the ones pasted below, please do not click on any links in the email or respond, they are all phishing attempts.

The first email from Commerce Bank appears legitimate and it is especially convincing due to the verbiage, logo, email addresses and other accurate details. Fortunately, the recipient noticed the account number was incorrect and thought it was an unusual email.



Revenue Share Payment for August 2020

This is to notify you of the upcoming Revenue Share payment for Church name Payment is being transmitted in the amount of \$ 2.59 via ACH to the account you have designated ending in XXXX and should be deposited to your account within the next 1-2 business days.

Please direct any questions to our Client Care Team at 800-892-7104 (option 2) or by forwarding this e-mail to commercial.cards@commercebank.com Thank you!

 Commerce Bank takes the security of your information very seriously. We take many measures to protect your personal information, and will never sell, rent or distribute your email address.

[Security Policy](#)



The next two emails, are much less convincing due to the language, misspellings and punctuation, despite some accurate details. Always be aware, most email scams come from a scammer posing as your bank, a legitimate business or a parishioner. Remember when reading external emails, always check to see where it is coming from, if you don't know the person, don't know what the email is regarding, or if it just seems odd, don't click on any links within email.

From: ed golterman <egolterman@att.net>
Sent: Friday, September 18, 2020 9:57 PM
To: stjochimparish@hotmail.com <stjochimparish@hotmail.com>
Subject: \$20,000 in donations

St. Louis, once a strong Christian City-with character, music, arts and culture..I believe supported rural parishes.
I am curator of the Guy Golterman historic collections – Coliseum MUNY and Kiel Opera House and I am donating stunning items for on-line fund raising, primarily auctions. I have tried to reach the rural parishes ministry without success. People throughout or state, parents and grandparents have collections to these places.

I am most open to working directly with you...The success of such on line auctions depends on the visual impact and presentation of the items which generate spirited bidding I have donated to 6 agencies so far....

Ed golterman, Kirkwood mo and curator of the guy golterman collections. 314 315 2548

Sent from [Outlook](#) for Windows 10

From: ed golterman <egolterman@att.net>
Sent: Saturday, September 19, 2020 7:23 PM
To: stjochimparish@hotmail.com <stjochimparish@hotmail.com>
Subject: Hi

I remember years ago, performing for a Rural Parishes fund raiser in St. Louis. I have tried to locate them or whoever helps you raise money to help you raise a lot of money. Not having any luck. Ed Golterman

My plan, communicated by the Washington Missourian and other news outlets will net Rural Parishes a lot of money. I left a message with a deacon at the Regali Center and never heard back.

Ed golterman, producer, curator, the Guy Golterman Collections

Sent from [Outlook](#) for Windows 10

7/29/20

IRS Letter Scam

Below is an example of a fake IRS letter which parishes are receiving. At first glance it may appear legitimate. There are several items in the letter that should alert you to the possibility of the letter not being authentic. First the address of the IRS is local and the zip code should be a zip plus four. All official IRS letters will include the 800 phone number and would not list a fax number or limited contact hours. The official letter would only address one tax period per letter and would not include enclosures and forms. If you have any doubts about any correspondence coming from the IRS, please email Sally at sallyserbus@archstl.org or Michele at michelefisher@archstl.org and include a copy of the correspondence in question.

Internal Revenue Service
1122 TOWN AND COUNTRY COMMONS
CHESTERFIELD, MO 63017-8200000

Department of the Treasury

Date: 07/22/2020

Employer Identification Number:
XX-XXX3422
Forms:
941
Tax Period(s) Ended:
06/30/2019, 03/31/2020
Person to Contact:
KIMBERLY J DENT
Employee Identification Number:
1000255922
Contact Telephone Number:
(636)255-1414
Contact Hours:
10:00am to 3:00pm
Fax Number:
8778521952

63379-2321004

We have reviewed your tax records and have found no record of you filing the tax forms identified above. We believe you are liable for filing and have prepared a tax return for each tax period identified above. If you agree that the returns are correct, please sign one copy of each and return it in the enclosed envelope. Keep a copy of the completed returns for your records.

If you do not agree that we have prepared the returns correctly, you have 30 days from the date of this letter (60 days if this letter is addressed to you outside the United States) to do one of the following:

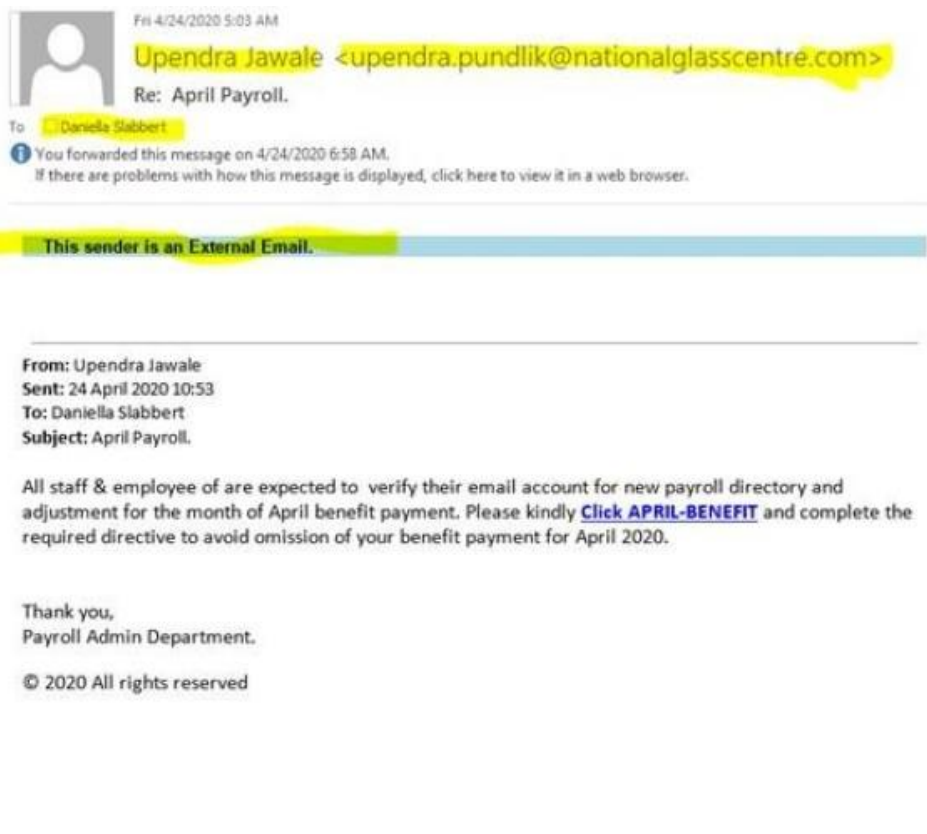
1. If you have already filed the returns for these tax periods, please send us signed copies in the enclosed envelope; or
2. Prepare and sign tax returns that you believe are correct and return them to us in the enclosed envelope; or
3. Mail us any additional information you would like us to consider; or
4. Request a conference with the person whose name and telephone number are shown above. At that time you may bring any additional information you would like considered. When you plan to come in for a discussion, please contact us in advance so that we can arrange a convenient time and place.

4/24/20

Payroll Email Scam

The IT Department has reported a mass email started arriving this morning for hundreds of users with the subject "April Payroll". A copy of the email is pasted below. If you clicked on that 'Click APRIL-BENEFIT' link, it likely took you to a log in page, asking you for your log in credentials or perhaps other personal information. If you received this email, AND clicked on the link... please contact the IT help desk immediately at helpdeskrequest@archstl.org.

IT has removed the offending email from mailboxes, but if you still have copies of it (it may still be on mobile devices), please delete it.



The screenshot shows an email interface. At the top left is a grey placeholder for a profile picture. To its right, the text reads "Fri 4/24/2020 5:03 AM". Below this is the sender's name "Upendra Jawale" and email address "<upendra.pundlik@nationalglasscentre.com>". The subject line is "Re: April Payroll.". The recipient is listed as "To: Daniella Slabbert". A blue information icon is followed by the text "You forwarded this message on 4/24/2020 6:58 AM. If there are problems with how this message is displayed, click here to view it in a web browser." A blue banner across the middle of the email content area states "This sender is an External Email." Below this banner, the email header is repeated: "From: Upendra Jawale", "Sent: 24 April 2020 10:53", "To: Daniella Slabbert", and "Subject: April Payroll.". The main body of the email contains the text: "All staff & employee of are expected to verify their email account for new payroll directory and adjustment for the month of April benefit payment. Please kindly [Click APRIL-BENEFIT](#) and complete the required directive to avoid omission of your benefit payment for April 2020." This is followed by "Thank you, Payroll Admin Department." and a copyright notice "© 2020 All rights reserved".

Fri 4/24/2020 5:03 AM

Upendra Jawale <upendra.pundlik@nationalglasscentre.com>

Re: April Payroll.

To: Daniella Slabbert

You forwarded this message on 4/24/2020 6:58 AM.
If there are problems with how this message is displayed, click here to view it in a web browser.

This sender is an External Email.

From: Upendra Jawale
Sent: 24 April 2020 10:53
To: Daniella Slabbert
Subject: April Payroll.

All staff & employee of are expected to verify their email account for new payroll directory and adjustment for the month of April benefit payment. Please kindly [Click APRIL-BENEFIT](#) and complete the required directive to avoid omission of your benefit payment for April 2020.

Thank you,
Payroll Admin Department.

© 2020 All rights reserved

5/4/20

Direct Deposit Scam Alert

We are receiving reports from parishes of an increase in direct deposit scams.

Due to the increase of this type of scam. We are strongly recommending that employees requesting changes in banking information for direct deposits do so in person and that emails are not accepted as legitimate authorization. Parishes on Lawson have been informed of this concern regarding security issues with direct deposits and have been reminded to submit the direct deposit form with bank information through the secure email addresses. HR as well as Payroll continue to be on extra alert for scams.

These SCAM emails are sent, presumably from an employee, stating that there is a problem with their account used for direct deposit or wishing to change their direct deposit account. Attached to the email is a form containing new banking information (sometimes a copy of a voided check) and requesting that their file be updated. The Archdiocesan Direct Deposit Authorization form may or may not be attached to the request.

The emails we've seen appear as though they are coming from a current employee's email, but often the employee's email has been hacked.

While not honoring email requests may seem to place a burden on the employee, you are ensuring that they securely receive their paychecks by not accepting email requests.

Church Vendor Scams

2/7/23

Sumner One Email Scam

Pictured below is an example of a recent phishing email scam that was received by a parish from a scammer posing as Sumner One, a trusted company and approved vendor. In this case, the scammer hacked their email and is using their name to trick customers. Parishes may receive an email with subject "Approved Enrollment Form" with a Fax Summary that appears to be from Sumner One, including a link to a PDF file. If you were to click on the link to open the PDF file, it would certainly take you to the scammer who would try to get you to give them your account number or personal information. When you receive unusual emails from trusted vendors, please contact them by phone to see if the email is legitimate before opening any files or clicking on any links. Thank you to Karen at Christ the King for alerting us to this recent email scam.

----- Forwarded message -----

From: **Robyn Gisick** <rgisick@sumnerone.com>

Date: Mon, Feb 6, 2023 at 1:06 PM

Subject: Approved Enrollment From Sumner One

To: Robyn Gisick <rgisick@sumnerone.com>

You have eFax® message

Fax Summary

E-Number:	20220-82033
Data:	<u>Efax</u> Pro
Resolution	1476/150
Priority Terms:	Very Important
Page Capacity):	5.00

[Preview PDF Here](#)

Please Find the attached,

Thank you.

Thank you,

Robyn Gisick

Office Administrator/Equipment Billing Specialist

P:316-984-5464 ext 5114

 **SumnerOne** | Wichita, KS

Welcome to the one place where everything works.

1/24/2023

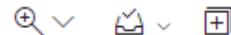
QuickBooks Phishing Scam

We recently received a report of an email scam that appears to come from QuickBooks Support. A copy of the email content is pasted below.

This recent email phishing attempt appears to be from QuickBooks Support or an agent of QuickBooks. The fake email explains that your annual subscription or service fee is due and your credit card renewal payment was declined or expired. The scammer may ask for your credit card number or an alternate form of payment. This is just another phishing attempt to obtain your credit card number or personal information.

Please be aware that the Archdiocese provides Intuit QuickBooks software as a service to all parishes and manages all aspects of the software use. The Archdiocese is the contact point for all Intuit account management and parishes should never be contacted in any way by a representative from Intuit or QuickBooks. Thank you to Angie at St. Joachim for reporting this phishing scam.

Quickbooks: Fw: Case:1783763732 Account Deactivation Imminent!



Attn: stjoachimparish@hotmail.com,

Your Quickbooks Subscription has failed to renew, this can happen as a result of several reasons, one of which might be your card on file has expired or you did not enter an accurate billing information.

Please update your card on file as soon as possible to prevent your account from being suspended indefinitely.

[Update Billing Information](#)

Once your Billing has been updated, we will charge you withing the next 24-48 hours and return your account to good standing.

Thanks
Quickbooks Support

3/2/21

Rottler – Financial Audit Scam

Another email scam has surfaced claiming to be a well known vendor requesting all payments be made via ACH. Pasted below is a copy of the email. In this instance, the unusual grammar, capitalization and unusual payment request should make you question the authenticity. Always question external emails regarding payment methods and updating banking information. When receiving external emails, always check to see where it is coming from and don't click on links within emails or take any action without contacting the vendor appropriately.

The vendor was contacted directly (not using contact information in the email) and the vendor confirmed that, indeed, it is a scam.

Thank you to JoAnn from St. Martin de Porres and Sharon at St. Rita for alerting us to this email scam.

From: Tamara Herrmann <therrmann@rottlerfinacedept.com>
Sent: Wednesday, March 2, 2022 9:22 AM
Subject: Update

This sender is an External Email.

Good day, just want to inform you that if you have any payment for us this week or next should only be paid via ACH/WIRE and if you are already paying with this means, Kindly let me know if you have our Revised Bank details as we are currently having a financial Audit on the old one.

Thanks.

Tamara Herrmann
Accounts Receivable Supervisor
Rottler Pest Solutions

12/13/21

Important Announcement from Tech Electronics

It has been brought to our attention that Tech Electronics recently experienced an email vulnerability that allowed third-parties to intercept and clone emails. Now, these third-parties are using emails to pretend to be Tech Electronics employees. Please read the email below from Tech Electronics. If you receive suspicious emails always verify whether or not the message is legitimate by contacting the person or company claiming to have sent the message using means other than replying to the message.



We are aware that some of our customers are being affected by the recent vulnerability Microsoft had in their email software. This vulnerability allowed third parties to intercept and clone emails. A patch to fix the vulnerability was applied as soon as possible. Unfortunately, there was enough time between the vulnerability and the patch for foreign third-parties to collect and intercept emails. Now, these third-parties are using these collected emails to pretend to be Tech Electronics employees.

We ask that if you receive any emails from someone at Tech Electronics that you please examine the "From" field to ensure the email is from an actual Tech Electronics email address. If it is not, it is spoofing email and should be deleted and ignored.

We have filed a report with the FBI and are increasing our cyber-security measures. We want to assure you, that none of your confidential information has been compromised. Tech Electronics is committed to our customers and we take cyber-security seriously. We are always working with all our vendors to remain patched, eliminate vulnerabilities any time they are discovered, and keep our customers informed and safe.

Please feel free to contact our cyber security team with any questions.

Thank you,
Michael Scott
Director of Corporate IT
Tech Electronics

9/8/21

FACTS and Faith Direct Alert

It has been brought to our attention that a couple of parishes have experienced irregularities with their FACTS and Faith Direct Accounts. There have been reports of deleted invoices and altered invoices in FACTS, and attempts to change bank information in Faith Direct. It is suspected that these fraudulent transactions may be a result of an email hack, but the source has not been confirmed.

We recommend parishes take extra precautions with these type of accounts by carefully and frequently verifying all payments and invoices. For added security we recommend parishes change admin passwords on these accounts as well. Remember hackers are clever and are capable of producing fake documents to attempt to change banking information. The best way to keep all your accounts safe is to keep a watchful eye on all activity.

9/15/21

Outlook Mailbox Password Expire Scam

We recently received a report of an email scam that appears to come from "Microsoft" regarding your Outlook account. The email notifies the recipient that their password has expired and asks them to click on a link to update their password. The email coming from an Italian domain is the first tip that the email is fake. A copy of the email content is pasted below. If you have received this email and responded or clicked on a link, please change your password immediately. Thanks to all those who have reported this scam.

-----Original Message-----

From: cesanobosconesangiustino@chiesadimilano.it

<cesanobosconesangiustino@chiesadimilano.it>

Sent: Wednesday, September 15, 2021 12:00 PM

Subject: HELP DESK

This sender is an External Email.

Dear Email User,

Your Outlook Mailbox Account Password Has Expired Click On (Link removed) and Update Your Account Records Immediately To Update Your Account.

Microsoft Team

4/30/21

Our Sunday Visitor Scam

It has been brought to our attention that a parishioner at St. Raphael received a phone call from a scammer posing as an employee of OSV. The scammer explained there was an issue with their online giving donation not going through. The scammer offered to correct the issue so the parish would receive their donation and proceeded to ask for the last four digits of their credit card, their social security number and other credit card information. Thankfully, the parishioner was immediately alerted and ended the call. OSV is aware of the situation, so there is no need to notify them.

If your parish uses OSV, we ask you to alert your parishioners as soon as possible by text, email, phone call, bulletin, Facebook, pulpit announcement, or other means. Currently we are only aware of this scammer contacting OSV users, but keep in mind this type of scam can be used for any online payment system. Please remind your parishioners that OSV (or other online giving providers) would never call or email them to change or correct an online donation and never give a caller personal information.

6/16/20

Microsoft Outlook Scam Reprise

We are receiving reports from parishes of another email scam that appears to come from "Microsoft". The email is sent from rpblades@hotmail.com. The email address is the first tip that the email is fake. Microsoft does not contact anyone using a Hotmail account.

A copy of the email is pasted below. Thanks to all those who have reported this scam.

Subject: Re: SIGN-IN

Dear user,

**Your Microsoft account is being compromised and new messages will be blocked,
Please confirm your account and location to indicate that it is still in use.**



Confirm Now

Note: In 24 hours, all Inactive Microsoft accounts will be deactivated.

Microsoft respects your privacy. Read our privacy policy for more information.

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052

3/20/20

Microsoft Outlook Email Scam

We are receiving reports from parishes of another email scam that appears to come from "Microsoft". The email is sent from rpblades@hotmail.com. The email address is the first tip that the email is fake. Microsoft does not contact anyone using a Hotmail account.

A copy of the email is pasted below. Thanks to all those who have reported this scam.

Subject: Re: SIGN-IN



Dear user,

Your Microsoft account is being compromised and new messages will be blocked, Please confirm your account and location to indicate that it is still in use.

Confirm Now

Note: In 24 hours, all Inactive Microsoft accounts will be deactivated.

Microsoft respects your privacy. Read our privacy policy for more information.

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052

2/20/20

Ameren Scams

Parishes are receiving calls from scammers posing as Ameren stating that their service will be disconnected due to non-payment. Callers are asking for credit card payment information to avoid immediate disconnection of service.

This is a scam and Ameren is aware of the calls.

Just a reminder, no utility provider would contact you by phone threatening disconnection and request immediate payment by credit card.

12/18/19

Weinhardt, Awards, and Subscriptions Scams

We have received reports of three new email scams. The first one appears to be a phishing email scam from someone posing as Weinhardt Party Rentals accounting department regarding the remittance of an invoice. The second seems to be from someone notifying you as a winner of a "Best of St. Louis Award" wanting you to "purchase" the award, which is probably a phishing scam as well. The third scam is for a computer Antivirus subscription. The first two messages urge you to click a link and view a website or invoice. Whatever you do, don't click the links, open attachments or reply. They can download malware to your computer that can acquire your usernames, passwords and even sensitive information, such as your credit card number. We are fairly certain the third scammer would ask for your credit card as payment for the fake Antivirus subscription when you call them.

All three of these phishing emails are posted below. Thank you to Katelyn at St. Anselm and Carol at Blessed Teresa of Calcutta, and Marsha Green from Shared Accounting for reporting

From: Kathy Bonifant [<mailto:kathy@weinhardtpartyrentals.com>]
Sent: Tuesday, December 17, 2019 12:00 PM
To: parishoffice@btcp parish.org
Subject: Weinhardt Party Rentals

Hello,

See attached remittance details paid to your account, Please forward to your accounting department if not meant for you.

Thanks.



Best Regards,
Kathy
Weinhardt Party Rentals
314.822.9900

From: Maurice Murphy [mailto:info@online-choice-contact.com]
Sent: Wednesday, December 18, 2019 6:04 AM
To: St Anselm Church <parishoffice299@att.net>
Subject: St Anselm Church - Best of Saint Louis Awards



It is our pleasure to inform you that St Anselm Church has been selected for the 2019 Best of Saint Louis Awards in the category of Catholic Churches.

For details and more information please view our website:
[2019 Best of Saint Louis Awards - Catholic Churches](http://saintlouis.Online-Choice-Contact.com/stw28nx6)

If you are unable to view the link above, please copy and paste the following into your web browser:
<http://saintlouis.Online-Choice-Contact.com/stw28nx6> ST-ANSELM-CHURCH

Best Regards,

Saint Louis Business Recognition

Dear Francis ,

We'd like to thank you for your support over past 2 years. We value your contributions to our company and memberships which make up the life hood of our organization. Your involvement is extremely important to us and very much appreciated we would like emphases this fact that your,

Subscription for the securities is going to be expire on December 18th 2019.

In order to cancel your subscription with us or avoid recurring charges, call us on +1 877-356-7749.Or if you want to continue with us then your subscription will be auto renewed with an amount of \$399.99 as the computer security software holds the information to be renewed and will auto debited from your account by December 19th 2019.

Note: - We don't acknowledge cancelation or renewal request over emails so please make sure to call us to avoid any recurring charges.

Regards

10/3/19

Amazon Login Scam

Our thanks to Al Rudolph for the following alert.

Trending in Security: Amazon Phishing Scam in Progress

The bad guys are targeting Amazon customers and tricking them into giving up their account login details, personal information, and even their financial information. They're sending phishing emails that tell you to update your account information within twenty-four hours or your account will be permanently disabled. Don't fall for this warning! Cybercriminals are counting on your impulsive reaction.

Once you click the "Update Now" button in the phishing email, you're taken to a realistic-looking Amazon login page. After you've entered your credentials, another form is displayed for you to "update" your name, phone number, date of birth, and address. Then, you have to provide your credit card and bank account details.

After you've given up all of this sensitive data, the phishing site tells you your account has been recovered and that you'll be logged out automatically. You're then redirected to the real Amazon website without having any idea of what actually happened.

Always remember: If you receive a suspicious email from an online service that you use, log in to your account through your browser (not through links in the email) to check the validity of the information presented. Also, be careful with emails that are seemingly urgent. The bad guys often use a 'sense of urgency' to pressure you into clicking as an impulsive response.

Stay safe out there!

5/9/19

Password Reset Scam

Our thanks to Michael at St. Vincent de Paul for this alert.

A parish received an email from churchgiving.com saying they received a request to reset a password. The email instructed the recipient to click on a link or paste it into a web browser. The parish had made no request for a password change and was not familiar with the vendor. (See actual email below)

These type of emails are typically grammatically correct, look official and have email addresses to resemble legitimate companies. Never click on any attachments that come from a suspected spam threat, especially ones requesting you to change passwords. Question every email that is not a direct response from a request you've made.

Copyright and Non-Compliant Scams

9/16/21

Copyright Infringement Scam

We have received a report of another threatening email from someone named "Amanda Hall" The sender claims to be a photographer and/or illustrator (depending on the email) and accuses the parish of copyright infringement. The email content is pasted below.

The email arrives via your parish website contact form and accuses you of using copyrighted website images on your parish website and asks you to click on a link to see the list of the images that are in violation. **DO NOT CLICK ON THE LINK.** The writer threatens to file a complaint with your hosting company and sue you.

The goal is to **scare you** and get you to click the link. The link may take you to a file download or a website that may allow the hacker to access to your device or it may take you to a phishing page asking you to enter more information, which you should never do. Thank you to Dodie at Annunziata for alerting us to this latest scam.

Name: Amanda Hall
Email Address: hallstudio420@hotmail.com
Phone +119177573205
Message
Hello there!

My name is Amanda.

Your website or a website your company host is violating the copyright protected images owned by me personally. Check out this document with the URLs to my images you utilized at www.pariah.com and my previous publications to find the evidence of my copyrights. Down load it right now and check it out for yourself. (Link included) This message is official notification. I demand the elimination of the infringing materials referenced above. Please be aware as a service provider, the DMCA requires you, to eliminate and disable access to the infringing materials upon receipt of this particular notice. If you don't stop the utilization of the aforementioned copyrighted content a lawsuit can be started against you. I do have strong self-belief that use of the copyrighted material referenced above as allegedly infringing is not authorized by the legal copyright owner, its agent, or the law. I declare, under consequence of perjury, that the information in this message is correct and that I am currently the legal copyright proprietor or am authorized to act on behalf of the proprietor of an exclusive right that is presumably infringed. Sincerely, Amanda Hall 09/15/2021

9/9/21

Facebook Non-Compliant Scam

We have received the report of a recent Facebook non-compliant scam pasted below. The sender claims to be Facebook stating your page has Facebook Page Term violations and will be unpublished unless you file an appeal by clicking on a link and filling out a form.

The goal of this email is to **scare you** and get you to click the link. Clicking the link may take you to a file download, a website that may allow the hacker to access to your device or it may take you to a phishing page asking you to enter more information, which you should never do. The "From" address and the unofficial Facebook look should be your first clue this is not an authentic email from Facebook. Thank you to Laura at the Cathedral for alerting us to this latest scam.

----- Forwarded message -----

From: **Page Guidelines** <messaging-service@post.xero.com>

Date: Wed, Sep 8, 2021 at 1:31 PM

Subject: Case id #10004091941

To: <parish@cathedralstl.org>

Facebook Help Center

Hello,

Your page has new violations and will be unpublished because it violates one or more of the Facebook Page Terms.

This means that you can still view your Page but other people can't and you won't be able to create new posts or to add new people to help you manage the Page.

If you think this is a mistake, please send us an appeal by filling out the form below:

<https://www.facebook.com/898498951069592>

Thanks,
Facebook Support.

Copyright Infringement Scam

We have received a report of another threatening email from someone named "Jessica Allen" The sender claims to be a photographer and/or illustrator (depending on the email) and accuses the parish of copyright infringement. The email content is pasted below.

The email arrives via your parish website contact form and accuses you of using copyrighted website images on your parish website and asks you to click on a link to see the list of the images that are in violation. **DO NOT CLICK ON THE LINK.** The writer threatens to file a complaint with your hosting company and sue you.

The goal is to **scare you** and get you to **click the link**. Clicking the link may take you to a file download or a website that may allow the hacker to access to your device or it may take you to a phishing page asking you to enter more information, which you should never do. Thank you to Barb at Annunciation for alerting us to this latest scam.

Name: Jessica

Email Address: Allenjd756@hotmail.com

Message

Hello there!

My name is Jessica.

Your website or a website your company hosts is infringing on a copyrighted images owned by me personally. Take a look at this doc with the hyperlinks to my images you utilized at wwwxyz.com and my previous publications to get the proof of my copyrights. Down load it now and check it out for yourself. (Link included) In my opinion you have willfully violated my legal rights under 17 U.S.C. Section 101 et seq., and could be liable for statutory damage of up to \$150,000 as set forth in Section 504 (c)(2) of the Digital Millennium Copyright Act. (DMCA) treaties. This message is official notification. I demand the removal of the infringing materials mentioned above. Please take note as a service provider, the Digital Millennium Copyright Act demands you, to eliminate and disable the access to the infringing materials upon receipt of this notification letter. If you do not cease the use of the aforementioned copyrighted content a lawsuit can be commenced against you. I do have a good faith belief that utilization of the copyrighted materials mentioned above as allegedly infringing is not approved by the copyright proprietor, it's legal agent, or the laws. I swear under consequences of perjury, that the information in this letter is correct and that I am currently the copyright owner or am permitted to act on behalf of the owner of an exclusive right that as presumably violated. Best regards, Jessica Allen 06/07/2021

4/29/21

Claiming Copyright Infringement Scam

We have received a report of threatening emails from someone named "Mel." The sender claims to be a photographer and/or illustrator (depending on the email) and very aggressively claiming copyright infringement. The email content is pasted below.

The email arrives via your parish website contact form and accuses you of using copyrighted website images on your parish website and asks you to click on a link to see the list of the images that are in violation. **DO NOT CLICK ON THE LINK.** The writer threatens to file a complaint with your hosting company and sue you.

The goal is to **scare you** and get you to **click the link**. Clicking the link may take you to a file download or a website that may allow the hacker to access to your device or it may take you to a phishing page asking you to enter more information, which you should never do.

Thank you to Laura at the Cathedral Basilica of St. Louis for alerting us to this latest scam.

Name Mel

Email Address Meshot8638@hotmail.com

Message

Hello,

This is Meleane and I am a qualified illustrator.

I was surprised, putting it lightly, when I came across my images at your website. If you use a copyrighted image without an owner's consent, you'd better know that you could be sued by the owner.

It's not legal to use stolen images and it's so disgusting!

Take a look at this document with the links to my images you used at parishxxx.org and my earlier publications to get the evidence of my copyrights.

Download it now and check this out for yourself:

(Link Removed)

If you don't remove the images mentioned in the file above within the next several days, I'll file a complaint on you to your hosting provider letting them know that my copyrights have been severely infringed and I am trying to protect my intellectual property. And if it doesn't help, trust me I am going to take it to court! And I will not bother myself to let you know of it in advance.

5/2/19

Google Scam

Our thanks to Laura at the Cathedral for reporting the following scam. Be sure not to open the email, respond to the email, or click on any links within the email.

The following email was sent from Tom smith [mailto:kamal.wst@gmail.com]

Dear Site Owner of (they insert the parish website URL)

Google has detected that some of your site's pages may be using techniques that are outside Google's Webmaster Guidelines.

Google Search Console has identified that your site is affected by 5 new issues of type Mobile Usability.

Top Issues (5 maximum)

The following issues were found on your site:

- Clickable elements too close together and Content wider than screen
- Domain Authority is low
- Broken Links
- Your most common keywords are not appearing in one or more of the meta-tags above. Your primary keywords should appear in your Meta
- Bad neighborhood links
- If you'd like any additional information about it then let us know, we will also help you to fix all these issues.

Email us back on same email ID.

Thanks

Google Search Console Team

Email Hack Alerts

3/124/22

St. Michael the Archangel Email Spoofed

Parishes are receiving emails from Kim Schultz of St. Michael the Archangel or from a Hotmail account claiming to be Kim. IT has determined that Kim's email was spoofed. These emails are not being sent by Kim and all emails from her should be deleted. Most email platforms should direct these emails to your spam folder.

Email spoofing is a form of impersonation where a scammer creates an email message with a forged sender address in hopes of deceiving the recipient into thinking the email originated from someone other than the actual source. Scammers will use email spoofing to help disguise themselves as a legitimate organization to trick users into performing some type of action. Scammers use this method of deception because they know a person is more likely to engage with the content of the email if they are familiar with who sent the message.

11/17/21

FBI Email Hack Alert

The Federal Bureau of Investigation (FBI) confirmed that its fbi.gov domain name and Internet address were used by hackers to blast out thousands of fake emails about a cybercrime investigation. Below is a copy of the email that was sent. If you received the email, please delete it. Thank you to Debbie at St. Joachim for reporting this email.

Gift Cards Scams

3/9/23

Pastor Email Scam Alert

Pictured below is an example of a recent phishing email scam that was received by a Curia staff member from a scammer posing as a Pastor. Please alert parish staff and possibly parishioners that scammers frequently pose as the pastor or an associate pastor seeking assistance with a task in an email. Often these emails may contain grammatical errors and are vague, with the hope that the recipient will reply to the email. Once the recipient replies, the scammer will most likely ask for help that involves purchasing a gift card or providing some personal information. If you receive unusual emails from a pastor or an associate and suspect they are a scam attempt, please ignore them or contact the parish office by phone to see if the email is legitimate. Thank you to Joyce for alerting us to this recent email scam.

From: Fr Chuck Barthel <fatherpastor.parish040@gmail.com>
Sent: Saturday, February 25, 2023 8:14 AM
To: Jones, Joyce <joycejones@archstl.org>
Subject:

External Sender: Please exercise caution when clicking links or opening attachments.

Greetings

Let me know if you are open to talk via email. I want you to manage a task for me discreetly, Please get back to me as soon as you can.

I will await your response

Peace.

12/6/19

Scrip Card Alert

It has been brought to our attention, that a parish received a phone from a caller, Marie Becnel (314-546-8194) asking to purchase gift cards through the parish Scrip Program. Since the parish staff did not know her, they explained to her that she would have to wait until the check clears before they could release the cards. The caller then hung up. The parish staff googled her name and number and discovered that she was previously charged with stealing more than \$25,000 and forging a check.

We would like to remind all parishes selling Scrip cards to be very cautious when someone would like to purchase a large amount of scrip cards. Waiting until the check clears before releasing the cards is always a good practice. Thank you to Margie at St. Joan of Arc for making us aware of this possible scam.

12/6/19

Gift Card Scam Alert With A Twist

The gift card scams are back, this time with twist. The scammers are again posing as pastors, but this time they are asking for gift cards to be used for Christmas gifts or bonuses for parish staff. Since the scammers are good at using legitimate clergy names, recipients should pay close attention to the sender's email address. A genuine email would typically have an organization name in the domain. Also, look for unusual phrases and grammatical errors. Posted below is a sample scam email recently received by a staff member of St. Simon. Note the @email.cz email domain. (see example below in red) Thanks to Joan for reporting this scam!

----- Forwarded message -----

From: Fr. Clark Maes <ministryadmin@email.cz>
Date: Fri, Dec 6, 2019 at 8:03 AM
Subject: Joan Fischer
To: <accountant@stsimonchurch.org>
Good morning,

I'm having a very busy day, and I plan on surprising a few staffs with gift cards as a bonus for this Christmas, I trust you can keep this as a surprise your confidentiality will be appreciated. would you mind making a purchase on my behalf as regards this? I will reimburse you personally. Walmart or Target gift cards which do you think works best?

Blessings, Fr. Clark Maes

5/2/19

Diocese Gift Cards Scam

Our thanks to Patricia and James from the Charlotte Diocese, Teak Phillips (STL Review), and Al Rudolph (Security) for the following scam alert. The scammers are now using legitimate names of clergy from other diocese in these scams. While we can alert parishes, we have no means to warn your parishioners.

Please place a notice or letter from the Pastor in your weekly bulletin warning parishioners of these scams.

The following email was sent from either Bishop Peter J. Jugis or Rev. Daniel G. Shaughnessy [ourlordpeace@gmail.com]

I need you to help me get a Google play card worth \$300 at \$100 or \$50 denominations /for a parishioner going through cancer in the hospital. He needs the cards to download his favorite music and videos to boost his confidence on his next phase of surgery and /flight over cancer which he's going to undergo in a few days time but i can't do this now.

Can you get it from any store around you right now? I will pay back as soon as i can.

God Bless,

Bishop Peter Jugis

Unusual Phone Call

It has been brought to our attention that a Pastor at a parish in the Archdiocese of St. Louis recently received a voice mail from a women calling from a number in the 417 area code, stating an Archdiocesan staff member was going to deliver a packet of information for their files in early 2022. The caller claimed to be calling on behalf of Mike Duffy, and asked the Pastor to return her call. Parish Support checked with other offices in the Curia and could not explain the call. The Pastor and Parish Support want to make other parishes aware of the occurrence. We ask that parish staff be attentive to odd or unusual occurrences, as this may be a scam attempt.

If you receive a call like this, please make detailed notes and notify Sally Serbus at 314.792.7716 or SallySerbus@archstl.org.

Invoice and Subscription Scams

Geek Squad Scam Alert

Pictured below is an example of a recent phishing email scam that was received by a parish staff member from a scammer posing as Geek Squad. Parishes may receive what appears to be a legitimate invoice for a substantial amount from Geek Squad support services or possibly another reputable company. There are a number of red flags that indicate that this is a scam. Your name does not appear anywhere in the invoice. Also, the email was sent from a gmail address not from Geek Squad. Finally, as with many phishing emails that originate in countries where English is not the primary language, the language is odd and there are grammatical and typing errors. The scammers often count on people being concerned that they are being wrongfully charged for a product they did not order. You are provided a telephone number to call if you want to cancel the subscription or dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. Rather contact the real company directly at a phone number or website that you know is legitimate where you can confirm that the phishing invoice was a scam. Thank you to Laura at Immaculate Heart of Mary for alerting us to this recent email scam.

Thank you for shopping with us...

This email for confirmation to the purchase of the product listed above.

The transaction may take several hours to appear in your account but it has been processed.

Please retain this email as a proof of purchase until it is completely activated.

Invoice ID: 3513566LJHJFRHD



Description.	Qty.	Total Price
Geek Squad Advanced Threat and Firewall and Net Protection	Three year Subscription	\$399.49



Subtotal	\$399.49
TAX	\$0.00
Total Amount	\$399.49

If you don't purchase or wish to cancel your Geek Squad account subscription please feel free to contact our customer care representative at: **858 314 8971**

9/22/22

Two New Scams

Misleading Invoice/Order Confirmation Scam

Pictured below is an example of a recent phishing email scam that was received by a parish. Geek Squad is a trusted company, and unfortunately scammers are using their name to trick customers. Parishes may receive an email invoice from a scammer posing as Geek Squad or another large business thanking you for a subscription renewal or a high dollar purchase. Email invoice scams such as these often direct you to call a toll free number if you have questions regarding the purchase or to cancel the purchase. If you were to call, they would certainly try to get you to give them your account number or personal information.

From: Wallence King <wallenceking5292@gmail.com>

Sent: Wednesday, September 21, 2022 7:30 AM

To: billing@geeksquad.com

Subject: Invoice #49685723

GEEK SQUAD

Invoice No. :684529-7526/BC27859 Invoice Date :September 21, 2022				
Qty	Description	Payment Mode	Rate	Amount
1	3 Year Subscription Plan	Debit Card	\$310.59	\$310.59

Dear Customer,

This email confirms the renewal of your Premium Plan

If you do not authorize this transaction or you want to Stop/Dispute this charge Contact Our support team on **+1 808 736 7029**

GEEK SQUAD
+1 808 736 7029


Domain Listing Solicitation Scam

A company named "Domain Listings" (domain-listings.org or domain listings.directory) is sending misleading "Annual Website Domain Listing" invoices to domain name owners via mail. They are shown below for your review.

These invoices are scams, these are not real bills. They have nothing to do with your domain name registration or service. They're trying to sell you a "listing on an internet directory", but that service is useless: you don't need to pay for basic search engine listings in Google, Bing and other reputable search engines.

If you receive one of these invoices, the most important thing to do is read it carefully, including all the fine print. If you don't recognize the business name, question the authenticity and do the research necessary to confirm whether or not it is legitimate.

In this case, the business actually tells the recipient that it is a solicitation, and you are under no obligation to pay the amount. Don't pay any company that sends you an unsolicited invoice for search engine services. You don't need to pay for basic search engine listings. It is a good idea to pass this warning on to the person who normally pays your invoices to make sure they do not submit payment.



DOMAIN LISTINGS

Date 9/8/2022
 Website allsaints-stpeters.org
 Number 242-1848
 Return By 10/18/2022

**WEBSITE LISTING
SERVICE**

DOMAIN NAME: ALLSAINTS-STPETERS.ORG

DESCRIPTION OF SERVICES: ANNUAL WEBSITE DOMAIN LISTING \$288.00
 FROM NOVEMBER 1, 2022 THRU OCTOBER 31, 2023

TOTAL FOR ANNUAL LISTING: \$288.00

SUBSCRIPTION INCLUDES: Annual Website Domain Listing on internet directory
 Complete details located online at www.domainlistings.directory

This website listing offer is provided to leading websites throughout the United States to enhance their Website exposure and expose them to new customers through our directory. We are not a Domain Registrar and we do not Register or Renew Domain Names. The listing period is for 12 consecutive months and must be renewed annually if you wish to maintain your Domain listing and keep it active on our online website directory.
THIS IS NOT A BILL. THIS IS A SOLICITATION. YOU ARE UNDER NO OBLIGATION TO PAY THE AMOUNT STATED ABOVE UNLESS YOU ACCEPT THIS OFFER.

We Appreciate Your Business!



INQUIRIES: Domain Listings LLC | Website: domainlistings.directory
 Customer Service E-mail: info@domainlistings.directory | Phone: 702-998-0222
 Do Not Contact: domainlistings.directory/dnc

Please make checks payable to: "Domain Listings"

Listing	Domain / Website	Amount
Annual	allsaints-stpeters.org	\$288.00

* Please Remit Payment to address on reverse by October 18, 2022*

ALL SAINTS CATHOLIC PARISH
7 MCMENAMY RD
SAINT PETERS MO 63376-1590

0026190307405265257463376159007

30

5/5/22

Misleading Invoice/Order Confirmation

It is important to note that scammers are getting more creative in order to make scams appear more legitimate. We have noticed that scammers are now using actual QuickBooks accounts to generate fake invoices. Although large retailers would probably not use QuickBooks to generate invoices, the use of QuickBooks makes the emailed invoices appear more legitimate. Your name not appearing anywhere on the invoice is the most obvious indication that the invoice is fake. An unusual email listed for the retailer is another red flag. As scammers continue to improve their ability to produce deceptive emails, parishes must be more diligent regarding any invoice that comes via email and never call a number given in an email without checking the validity.

Pictured below is an example of a recent phishing email scam that was received by a parish. Amazon is a trusted retailer, and unfortunately scammers are using their name to trick customers. Parishes may receive an email invoice from a scammer posing as Amazon or another large retailer thanking you for a high dollar purchase. Email invoice scams such as these often direct you to call a toll free number if you have questions regarding the purchase or to cancel the purchase. If you were to call, they would certainly try to get you to give them your account number or personal information.

----- Forwarded message -----

From: Amazon.com <quickbooks@notification.inhat.com>
Date: Thu, May 5, 2022 at 12:48 PM
Subject: Invoice 12859 from Amazon.com
To: <abm@gmail.com>

INVOICE 12859 DETAILS



Amazon.com

DUE 05/05/2022

\$1,599.00

[Print or save](#)

Powered by QuickBooks

Dear Customer,

Thanks for shopping with us. Your Order is On The Way.
We would like to inform you that Your order has been dispatched. If you did not place this order please call us on +18773200159 to report this to our fraud protection team.

Arriving:
May 05th, 2022

Your shipping speed:
Morning Delivery at \$90.

Order:
Apple iPhone 13 Pro Max (1TB, Gold)

Total Amount:
\$1599

Your package is being shipped by ATS and the tracking number is AMZN72982398. Please note that a signature may be required for the delivery of the package.

For Any Query or Support or to Cancel the Order and report and dispute please contact our Amazon Fraud Detection Team +18773200159

Thanks
Amazon Delivery Service
+18773200159

Bill to abm@gmail.com

Terms Due on receipt

Apple iPhone 13 Pro Max **\$1,599.00**

Apple iPhone 13 Pro Max (1TB, Gold)

1 X \$1,599.00

3/10/22

Misleading Domain Listing Invoice

Several parishes have reported receiving the misleading invoice pasted below from Domainnetworks.com for a fake Annual Website Domain Listing. These trade directories are bogus and the invoices are as well. These payment solicitation attempts take advantage of the fact the person handling the administrative duties for the parish may not know whether any business listings were purchased. Thank you to all who have reported these deceptive invoices.



domainnetworks.com

Date of Notice: February 23, 2022
Website: OLLWASHMO.ORG
Number: EBE114380
Deadline: Upon Receipt

MARKETING SERVICES

DOMAIN INFO:

OLLWASHMO.ORG

Registrar: -
NS1: NS33.DOMAINCONTROL.COM
NS2: NS34.DOMAINCONTROL.COM

DESCRIPTION OF SERVICES:

ANNUAL WEBSITE DOMAIN LISTING: \$289
From April 9, 2022 THRU April 9, 2023

TOTAL FOR ANNUAL TERM: \$289

SUBSCRIPTION INCLUDES:

Annual Domain / Business Listing on DomainNetworks.com.
Complete details at www.domainnetworks.com

This website listing offer is provided to leading websites throughout the United States to enhance their Website exposure and expose them to new customers through our directory. We are not a domain registrar and we do not Register or Renew Domain Names. The listing period is for 12 consecutive months and must be renewed annually if you wish to maintain your Domain listing and keep it active on our online website directory.
THIS IS NOT A BILL. THIS IS A SOLICITATION. YOU ARE UNDER NO OBLIGATION TO PAY THE AMOUNT STATED ABOVE UNLESS YOU ACCEPT THIS OFFER.

WE APPRECIATE YOUR BUSINESS!

INQUERIES: Domain Networks | Website: domainnetworks.com
Customer Service Email: info@domainnetworks.com | Phone: (505) 510-7300
Do Not Contact: domainnetworks.com/dnc

Please make checks payable to: "Domain Networks"

Domain Networks
PO Box 1280
Hendersonville, NC 28793

Listing	Domain	AMOUNT
Annual	OLLWASHMO.ORG	\$289

please remit payment to address on reverse side by April 9, 2022

12418*48*****SCH 5-DIGIT 63090
Our Lady of Lourdes Catholic Church
1014 MADISON AVE
WASHINGTON, MO 63090-4806



1/31/22

Norton 360 Phishing Scam

Norton 360 is a trusted name in cyber safety, unfortunately hackers and scammers are using their name to trick customers. Parishes may receive an email from a scammer posing as Norton for a Norton 360 renewal or subscription. In this recent scam, the email is directing you to call an 843 number to cancel the order. There are a number of red flags that indicate that this is a scam. Your name does not appear anywhere in the invoice and the email was sent from a gmail address not from Norton. In this particular email they have a "Shipping To" name listed, which is obviously not you, trying to prompt you to call the number.

The scammers often count on people being concerned that they are being wrongfully charged a substantial amount for a product they did not order. You are provided a telephone number to call to cancel the subscription or dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. We recommend you contact the company directly at a phone number or website that you know is legitimate where you can confirm that the invoice was a phishing scam.

Thank you to Laura at Immaculate Heart of Mary for alerting us to this scam.

Below is a copy of the phony invoice presently being circulated.

INVOICE

Thank you for using PayPal Inc.

We have successfully processed your payment to Norton 360.

It will reflect on your bank statement as "Norton 360"

Shipping To: Emma Johnson
Shipping From: Norton 360 Antivirus

Product Name: Norton 360
Product Amount: \$549.67 USD
Invoice No: 54093128554966

Your Payment has been sent to Norton 360

To cancel your order, contact us at: +1(843) 900 1956

Note: You have 24 hours to cancel your order.

For any queries, contact us at: +1(843) 900 1956

PayPal Team

1/25/22

International Invoice Scam

We have received an alert of another possible invoice scam. In this recent email the sender gives no information regarding the nature of the invoice. The email is pasted below for your review.

Often the most recognizable red flag indicating that it may be a scam is that your parish name does not appear anywhere in the email and the email was sent from an email address or company you do not recognize. In this particular case, the email appears to be from an account manager of Asia Pacific, with an international phone number to call if you have questions regarding the invoice, which is also another reason to question its authenticity. The country code 61 listed in the email is actually Australia.

Scammers often count on people being concerned that they are being wrongfully charged for a product or service they did not receive. In this particular case the email states the invoice is attached. If you don't recognize the company, please delete the email and do not click on any attachments or links. This email also directs you to call their office using an international phone number, which is another phishing attempt.

Thank you to Sharon at St. Rita for alerting us to this recent scam.

From: Stephen <Stephen@katalystdm.com>
Sent: Sunday, January 23, 2022 4:45 PM
Subject: UP INV - #37396.

This sender is an External Email.

Hello,
I have attached your invoice #37396.

Please let me know if you have any questions!

If you need further assistance you may call our office at +61 (8) 9824-9824

Stephen
Manager, Account Services, Asia Pacific

Katalyst Data Management

Office: +61 8 9824 9824

Mobile: +61 689 479 768

STATEMENT OF CONFIDENTIALITY

The information contained in this email message and any attachments to this message is confidential. If you are not the intended recipient, please (i) notify me immediately by replying to this message, (ii) do not use, disseminate, distribute or reproduce any part of the message or any attachment, and (iii) destroy all copies of this message and any attachments.

1/20/22

Event Invoice Scam

We have received an alert of another possible invoice scam. In this recent email the sender states they have attached invoices for an event that has not taken place at the parish. We have pasted the emails below for your review.

Often the most recognizable red flag indicating that it may be a scam is that your name does not appear anywhere in the email and the email was sent from an email address or company you do not recognize.

Scammers often count on people being concerned that they are being wrongfully charged for a product or service they did not receive. In this particular case the email states the invoice is attached. If you don't recognize the company, please delete the email and do not click on any attachments or links.

Thank you to Sharon at St. Rita for alerting us to this recent scam.

From: Rachel Lillard <support@profmuhaya.com>
Sent: Wednesday, January 19, 2022 8:20 AM
To: "[@archstl.org](mailto:To:parish249)"
Subject: Invoices Notification 67336655

This sender is an External Email.

Hello ,
Attached are the invoices #67336655 for your event on January 21st. Thank you for bringing in your team and spending your day with us!

Let me know if you have any questions!

Best,

Rachel Lillard

Corporate Accounts Coordinator

NOTICE: This electronic mail message and any files transmitted with it are intended exclusively for the individual or entity to which it is addressed. The message, together with any attachment, may contain confidential and/or privileged information. Any unauthorized review, use, printing, saving, copying, disclosure or distribution is strictly prohibited. If you have received this message in error, please immediately advise the sender by reply email and delete all copies.

From: Jim Penn <commercial@aubergecavaliere.com>
Sent: Wednesday, January 19, 2022 10:48 AM
To: "[@archstl.org](mailto:To:parish249)"
Subject: Invoices Confirmation 197523

This sender is an External Email.

Hello ,
Attached are the invoices #197523 for your event on January 21st. Thank you for bringing in your team and spending your day with us!

Let me know if you have any questions!

Best,

Jim Penn

Corporate Accounts Coordinator

NOTICE: This electronic mail message and any files transmitted with it are intended exclusively for the individual or entity to which it is addressed. The message, together with any attachment, may contain confidential and/or privileged information. Any unauthorized review, use, printing, saving, copying, disclosure or distribution is strictly prohibited. If you have received this message in error, please immediately advise the sender by reply email and delete all copies.

12/20/21

Xfinity Invoice Scam Alert

We received a report of a recent Xfinity invoice/receipt scam. The example is pictured below. Parishes may receive an email from a scammer posing as Xfinity or Norton showing a subscription receipt for security or maintenance. In this case the email is directing you to call an 844 number if you did not subscribe. This particular email is obviously fake due to the terrible grammar, formatting and inconsistencies. Keep in mind, other scams may not be as apparent. Often the most recognizable red flag indicating that it may be a scam is that your name does not appear anywhere in the invoice and the email was sent from a gmail address not from Xfinity or Norton. In this particular case they try to get you to contact them by phoning their unusual number.

The scammers often count on people being concerned that they are being wrongfully charged for a product they did not order. You are provided a telephone number to call if you dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice/receipt such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. Rather contact the real company directly at a phone number or website that you know is legitimate where you can confirm that the phishing invoice was a scam. Thank you to Cindy at St. Ignatius for alerting us to this scam.

From: Bagert Kope <bagertkope675@gmail.com>
Date: Mon, Dec 20, 2021 at 9:18 AM
Subject: INVOICE ID HVOK20211220LKN

Dear Customer,

This is to letting you know that, your **Bi-yearly** subscription for total all round security and maintenance with us, The Nort Xfinity has been auto renewed for a charge of **\$261.00 USD** as on 2021-12-20

The payment may take 24 hrs. to show in your account profile.

Please find below the e – receipt of the transaction.

INVOICE ID_HVOK20211220LKN

PRODUCT NAME	Finish Date	Quantity	Total Amount	Payment Method
Xfinity	In 2 year	1	\$261.00 USD	Debit from account

Thank You for being a part of the Nort_X family.

Not You?

In Case of a dispute or any kind of a query or if you wish to cancel the subscription then please reach out to us at: +1 – (844) – (562) – 0569 Immediately.

If the dispute is valid then you will be eligible for a full settlement instantly and our accounts team will help you out.

--

Regards,

Aaron M.
Xnor Family

11/15/21

PayPal Scam Alert

Hackers and scammers are using PayPal to trick customers. Parishes may receive an email order confirmation from a scammer posing as PayPal. In this recent scam, the email is directing you to call an 802 number if you did not place the order. There are a number of red flags that indicate that this is a scam. The parish name or email address does not appear anywhere in the invoice. Also, the email was sent from a gmail address. In these cases, they are aggressively trying to get you to contact them by phone so they can get obtain credit card and personal information.

The scammers often count on people being concerned that they are being wrongfully charged for a product they did not order. You are often provided a telephone number to call if you dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft or credit card fraud. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. Rather contact the real company directly at a phone number or website that you know is legitimate where you can confirm that the phishing invoice was a scam. Thank you to Jeanne at St. Philip and James who reported this scam.

Below is a copy of the phony invoice presently being circulated.

— Forwarded Message —
From: Customer Support <noristokeb349@gmail.com>
To: "paypal.usa.customer@gmail.com" <paypal.usa.customer@gmail.com>
Sent: Friday, November 12, 2021, 08:06:33 AM CST
Subject: payment update

PayPal

Receipt Attached

Helpline Support 24*7
1 802 387-0605

Thank you for choosing PayPal as your payment partner, The following message provides information regarding your order.

Values listed are in USD.

Purchase Number: **AWXTRP589BBC**
Date: Friday, 12Nov 2021

ORDER

You can check the status of your order by logging into your account after 24 hours.

If you have any questions about your order please contact us by calling us at **+1 802 387-0605** Monday - Friday, 9am - 10:30pm Eastern Time and Saturday - Sunday, 9am - 5:30pm.

Your Invoice for Order #1130352648202

Shipping Information: (Gift To)		Shipping Method:	
Bill B. Goin 886 Railroad Street Marquette, MI 49855 United States Telephone - (UNCONFIRMED)		Fast Delivery Method Product - Google Play Gift Card	
Discription	Item no.	Qty	Subtotal
Google Play Gift Card	#03482	02	410.07
Subtotal			410.07
Shipping & Handling			0.00
Grand Total (Incl.Tax)			\$410.07

Thank you again, For your support.

10/24/21

United Rental Scam

We have received a report of someone posing as a representative of United Rental calling a parish about a past due invoice. The parish does not do business with United Rental and we believe this to be a phishing scam to obtain personal or payment information.

As always, be cautious regarding past due invoice calls or emails. If the caller claims to be from one of your legitimate vendors, and you are concerned that there truly is a problem, contact the vendor directly through the contact information you have on file - not the number the caller provided, and never give out credit card or banking information over the phone or via emails.

Thank you to Nicky at St. Gerard Majella for this alert

10/21/21

QuickBooks Scam Alert

It has been brought to our attention that a parish received a phone call from someone pretending to be an Intuit- QuickBooks agent. The fake Intuit - QuickBooks agent often explains that your annual subscription or service fee is due and your credit card renewal payment was declined. The scammer may ask for your credit card number or an alternate form of payment. This is just another phishing attempt to obtain your credit card number or personal information.

Please be aware that the Archdiocese provides Intuit QuickBooks software as a service to all parishes and manages all aspects of the software use. The Archdiocese is the contact point for all Intuit account management and parishes should never be contacted in any way by a representative from Intuit or QuickBooks.

Thank you to Tina at the Old Cathedral for alerting us to this recent phishing attempt.

9/3/21

Geek Squad Invoice Scam

Another fake invoice scam has surfaced. Parishes may receive what appears to be a legitimate invoice from Geek Squad support services. There are a number of red flags that indicate that this is a scam. Your name does not appear anywhere in the invoice. Only your email address appears in the phony invoice. Also, the email was sent from a gmail address not from Geek Squad. Finally, as with many phishing emails that originate in countries where English is not the primary language, the language is odd and there are grammatical and typing errors.

The scammers often count on people being concerned that they are being wrongfully charged for a product they did not order. You are provided a telephone number to call if you dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. Rather contact the real company directly at a phone number or website that you know is legitimate where you can confirm that the phishing invoice was a scam.

Below is a copy of the phony invoice presently being circulated. Thank you to Mary at St. Cronan for making us aware of this recent scam.

----- Original Message -----

From: geeksquad department <davidp600980@gmail.com>

To: undisclosed-recipients.;

Date: 09/01/2021 9:50 AM

Subject: thanks for the payment

Dear Customer,

Thanks for Purchasing GeeksQUAD DEPARTMENT. Your auto-renewal subscription is renewed and updated on September 01, 2021.

We are here to inform you that YoU are charged \$988.00 USD. Regarding your computer PC service for two years.

Item #	Product Name/Description	Qty	Unit Price	Total
1.	GeekSQUAD department(68/38 BIT) SUPPORT IN 5 DEVICES	1	988.00USD	988.00USD
			Sub Total:	989.00USD
Notes & Description: ORDER CAN BE CANCELLED WITHIN 4 HOURS.			Grand Total:	989.00USD

Today you're saving 989.00 on your 2nd term subscription (currently \$989.99/yr upon renewal).

For annual subscriptions, we'll email you a reminder 30 days before your subscription automatically renews.

Our Toll-Free Number: +1 (831) - (807) - (8531)

Show more

GeekSQUAD department

Certified Site

Calendar | 30-day money guarantee | free technical support

geeksquad deparment

5 Devices / 2 years subscription

7/22/21

Select Office Supply Invoice Scam Reminder

We want to remind parishes that the Select Office Supply, of Long Beach, California fake invoice scam is still being reported. Often the parish/school received a "sales call" a week or so before the invoice arrived. During the "sales call" they asked for information about the copier the parish/school had, if they were in the market for a new one or if they could send a quote for maintenance etc. The sales call enabled the scammer to get a contact name and the type of copier toner they typically order. Following the "sales call" the parish received an invoice for the toner they use at a very inflated price, with high shipping charges, and mentioned the contact name at the parish on invoice as well. In this case the invoice looks very legitimate.

The scammers often count on staff to process these invoices without checking to see if the items were actually received or whether the quoted price is correct on the invoice. Please be diligent when approving invoices for payment with staff. Scammers often count on staff to be concerned that they are being wrongfully charged for a product they did not order. If you are provided a telephone number to call to dispute the bill, do not call as you will likely be prompted to provide personal information that will be used to make you a victim of identity theft.

7/12/21

Archstl.org Listing Scam

Another scam has surfaced. Parishes may receive what appears to be a legitimate invoice from Glinkx Professional Domain Listings for the Archstl.org business domain listing or perhaps your own parish listing. The barely legible type above We Appreciate Your Business states: "This is not a bill, it is a solicitation. You are under no obligation to pay the amount stated unless you accept this offer". These sort of companies are hoping busy church staff or volunteers will run the "bill" through on the assumption that someone else researched it and authorized the listing. Never pay any invoice unless you verify it was authorized by a parish organization or staff member. Thank you to Alison at St. Francis of Assisi - Luebbering for sharing this scam.



GLINKXX
Personalized Domain Listings

Date: 7/1/2021
Website: Archstl.Org
Number: GLX-755973
Offer Expires: 8/1/2021

Don't over think it
GLINKXX it!

BUSINESS DOMAIN NAME: Archstl.Org
DESCRIPTION OF SERVICES: ANNUAL PERSONALIZED BUSINESS DOMAIN LISTING SERVICE FROM 8/1/2021 thru 8/31/2022 \$224.00
SUBSCRIPTION INCLUDES: Personalized business domain listing on the fastest growing worldwide business directory Premium exposure through special "FEATURED LISTINGS." Optimized SEO / Increase local visibility / Link building. For complete details visit us online @ www.GLINKX.com
<small>This website listing offer is provided to leading business websites throughout the United States to enhance their Web-site exposure and to reach new customers. We are NOT a Domain Registrar and we do NOT register or renew domain names. The listing period is for 12 consecutive months and must be renewed annually if you want your Business Domain Listing to remain active on our directory.</small>
We Appreciate Your Business <small>CUSTOMER SERVICE: contactus@glinkx.com</small>

Please make checks payable to: "GLINKXX"



GLINKXX
PO BOX 34990
LAS VEGAS NV 89133

REF. CODE	DOMAIN/WEBSITE	AMOUNT
GLX-755973	Archstl.Org	\$224.00

Please make payment to address on reverse side by 8/1/2021

St Francis Of Assisi Parish
1000 Luebbering Rd
Luebbering, MO 63061



2017.0595973 0101-4834

5/12/21

Amazon & PayPal Scams

Hackers and scammers are using Amazon and PayPal to trick customers. Parishes may receive an email from a scammer posing as Amazon and/or PayPal thanking you for your order. In this recent scam, the email is directing you to call an 800 number if you did not place the order. There are a number of red flags that indicate that this is a scam. The parish name does not appear anywhere in the invoice. Only your email address appears in the phony invoice. Also, the email was sent from a gmail address. In these cases they, are aggressively trying to get you to contact them by phoning their 800 number.

The scammers often count on people being concerned that they are being wrongfully charged for a product they did not order. You are provided an 800 telephone number to call if you dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. Rather contact the real company directly at a phone number or website that you know is legitimate where you can confirm that the phishing invoice was a scam.

----- Forwarded Message -----
From: "service@paypal" <paypal.paymentscares@gmail.com>
To: stferd@tuno.com
Subject: Purchase Confirmation You sent a payment of \$505.66 USD to BitBurst LLC
Date: Sat, 15 May 2021 19:06:00 +0530

PayPal

Transaction ID: AS54X14SD7D5S47DW

You sent a payment of \$505.66 USD to BitBurst LLC

Thankyou For using **Paypal** the order is successful. Please note it may take a few movements for your transaction to appear in the recent activity list on your **Account Overview**. This charge will appear on your statement as a payment to **PAYPAL** 'BitBurst.LLC'.

Receipt number : 5487-5448-8989-2116.

Please keep the receipt number for future reference. You'll need it if you contact our **customer service at 1800-981-3727**.

Merchant Information merchant	Merchant Order ID	Instructions to
BitBurst LLC ENUR	None Provided	XJDJ547B

Description price	Qty	Amount	Unit
0.000086 BTC 5.66 USD		\$505.66 USD	1 \$50

----- Forwarded Message -----
From: "info@amazon.com" <info@amazon.com>
To: info@psbc.com
Subject: TWZ-477909-520471 - Order Confirmed for Sony Camera
Date: Mon, 01 May 2023 04:58:59 -0700 (PDT)

[Link Unavailable](#)

[Your Order](#) | [Your Account](#)
ORDER 1429829
TWZ-459609-212048

Dear Sherril
Thank you for shopping with us. You have ordered the [Sony ZV-8 Camera for Content Creators, Vlogging and YouTube with Flip Screen and Microphone](#). In case you require any change in order or like to cancel we recommend giving us call immediately at [1-877-313-5001](tel:1-877-313-5001).

Arriving:
[Wednesday, May 10](#)
No signature is required due to covid

Shipping Address:
38. Arroyo del
Arroyo, CO, 80810

Brand	Sony
Color	Grey
Model Name	Sony ZV-8 Camera for Content Creators, Vlogging and YouTube with Flip Screen and Microphone

Item Sub Total	\$750.0
Taxes	\$68.8
Shipping & Handling Charges	FREE
Order Total	\$818.8

For any support call us at our Toll-free Number: [1-877-313-5001](tel:1-877-313-5001)

This email was sent from a customer service address. Please write us back if you have any concerns. [Click here](#)
[Feedback](#)

5/4/21

Norton Invoice Scam

NortonLifeLock is a trusted name in cyber safety, unfortunately hackers and scammers are using their name to trick customers. Parishes may receive an email from a scammer posing as Norton for a NortonLifeLock renewal or subscription. In this recent scam, the email is directing you to call an 800 number if you did not place the order. There are a number of red flags that indicate that this is a scam. Your name does not appear anywhere in the invoice. Only your email address appears in the phony invoice. Also, the email was sent from a gmail address not from Norton. In this particular case they, are aggressively trying to get you to contact them by phoning their 800 number.

The scammers often count on people being concerned that they are being wrongfully charged for a product they did not order. You are provided an 800 telephone number to call if you dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. Rather contact the real company directly at a phone number or website that you know is legitimate where you can confirm that the phishing invoice was a scam. Thank you to Frances at St. Anselm for alerting us to this scam.

Here is a copy of the phony invoice presently being circulated.

From: Omar <hieberth870@gmail.com>
Sent: Monday, May 3, 2021 9:36 AM
To: Frances Schmitz <fschmitz@stanselmsti.org>
Subject: #In_Voice Number : #AGT7/548/95563.....

(NORTON)

Dear shoops@stanselmsti.org,

Your NORTON - one member account is being billed with \$199 for NORTONLifeLock Business.

Any issue with this transaction? Call us @ +1 (800) 794-3898 (Toll-Free)

Here is Your Receipt

Order	AGT7/548/95563
Registered ID:	[EMAIL]
Activation date:	(05/3/2021)
Total before tax:	\$199.00
Total including tax:	\$199.00

Note: please call Billing , if you did not place this order.

@ +1 (800) 794-3898

Thanks & Regards

Dial Now:- @ +1 (800) 794-3898

4/29/21

Deceptive McAfee Invoice Scam

Another fake invoice scam has surfaced. Parishes may receive what appears to be a legitimate invoice from McAfee for your parish subscription. There are a number of red flags that indicate that this is a scam. Your name does not appear anywhere in the invoice. Only your email address appears in the phony invoice. Also, the email was sent from a gmail address not from McAfee. Finally, as with many phishing emails that originate in countries where English is not the primary language, the language is odd and there are grammatical errors.

The scammers often count on people being concerned that they are being wrongfully charged for a product they did not order. You are provided a telephone number to call if you dispute the bill. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. Rather contact the real company directly at a phone number or website that you know is legitimate where you can confirm that the phishing invoice was a scam.

Here is a copy of the phony invoice presently being circulated.

----- Forwarded message -----
From: PAYMENT INVOICE <mafee@brittanie011@gmail.com>
Date: Tue, Apr 20, 2021 at 8:01 AM
Subject: PAYMENT INVOICE
To: -

Hello

Thank You for your payment. Your account has been debited with \$399.99 for the auto renewable plan of your McAfee family. The charges might reflect within a few moments to 24 hours. For any query or assistance please reach out to us @ +1 (781) 739-0805 / +1 (781) 739-0805.

Invoice Number - MVBE786798

Product	Issue Date	Expiration Date	Qty	Amount
McAfee Security 360 Plan	April, 20, 2021	April, 19, 2026	1	\$399.99

PC Solution
3856 Raleigh Street 2nd
Lane
Miami, Florida
33101-129

We are an associate of the McAfee Support.

You are important:-

In case of any dispute or query or to cancel the subscription please reach out to our support team @ toll free +1 (781) 739-0805 / +1 (781) 739-0805 and get a full refund. Please note you have 24 hours to report a dispute.

Thank You.

McAfee Support.

4/23/21

Onsolve and iTunes Two New Scams

We have received two reports of recent scams. Parishes may receive what appears to be a legitimate invoice from OnSolve, a critical communications company. See the invoice pasted below. These scammers are hoping busy church staff or volunteers will run the "bill" through on the assumption that someone else researched it and made the purchase. Never pay any invoice unless it was authorized by a parish organization or staff member. Thank you to Mary at St. Vincent for sharing this scam.



Invoice
15169169
04/21/21

Bill To
St. Vincent DePaul Parish
1408 South 10th St
Saint Louis MO 63104

Ship To
St. Vincent DePaul Parish

Invoice Date	Terms	Due Date	Sales Rep	Customer ID	PO #
04/21/2021	Net 30	05/21/2021	Wolf, Karen	41588	

Item	Start Date	End Date	Quantity	Rate	Amount
OCN-ADMIN-FEE One Call Now: Admin Fee End User 41588 St. Vincent DePaul Parish	05/21/2021	05/20/2022	1.0	\$35.70	\$35.70
OCN-Number of US Members-Annual Standard OCN-Number of US Members-Annual Standard End User 41588 St. Vincent DePaul Parish	05/21/2021	05/20/2022	305.0	\$2.94	\$1,020.00
OCN-Unlimited Standard Annual Plan OCN-Unlimited Standard Annual Plan End User 41588 St. Vincent DePaul Parish	05/21/2021	05/20/2022	1.0	\$0.00	\$0.00

Subtotal \$1,055.70
Tax (9%) \$0.00
Total \$1,055.70
Amount Paid \$0.00
Credits \$0.00
Amount Due \$1,055.70

EMAIL: ar@onsolve.com

Bank/Wire Information:

Wells Fargo Bank
Account Name: OnSolve, LLC
Routing: 063107513 (ACH) / 121000248 (Wire)
Account Number: 5231692129
SWIFT Code: WFBUS633

Sales Rep:

Remittance Slip

Customer: 41588 St. Vincent DePaul Parish
Invoice #: 15169169
Amount Due (USD): \$1,055.70
Amount Paid: \$0.00

Please Remit Check Payment To:
P.O. Box 662672
Orlando, FL 32865-5672

If you have any questions about this invoice, message us through the portal or email: AR@OnSolve.com

Another email scam has surfaced claiming to be from "iTunes" a legitimate music membership provider. In this case, they want you to call and cancel your subscription in order to get your payment information. Pasted below is a copy of the email. Notice the unusual email address for

the Apple store. This unusual email address, payment information request, awkward grammar and typing should make you immediately question the email's authenticity. When receiving external emails always check to see where it is coming from and don't click on links within emails, or respond in any way if there are any unusual requests. Thank you to the staff at the Old Cathedral for the alert.

iTunes		Subscription Confirmation	
APPLE ID	INVOICE NO	TOTAL	
Oldcathedral@Att.Net	AS#1213257561		
DATE	ORDER ID	\$199.99	
Wednesday, April 21, 2021	21HSL9VMNS9		

The email confirms your subscription purchase.

You have purchase the following subscription with 1 Month free trial.

Subscription iTunes Music Membership
App Music Membership
Content Provider Apple Inc.
Date Of Purchase Wednesday, April 21, 2021
Price \$199.99
Payment Method By Card

You will not be charged for your free trial. Once it ends, Your subscription will renew at \$199.99 unless you cancel by Friday, April 23, 2021.

To Cancel Subscription visit to our Customer Care **+1 (810) 212-2626 (Toll Free)**.

Regards

The App Store Team

2/9/21

Windows 10 Scam

Another email scam has surfaced claiming to be from "Microsoft". Pasted below is a copy of the email. Notice the email is sent from yougotmailalert@securemailnotification.com not Microsoft. Also, note the grammar and how it is signed by the so called "Microsoft Security Team". These irregularities should make you question the authenticity. When receiving external emails always check to see where it is coming from and don't click on links within emails, or respond in any way if there are any unusual requests. Thank you to Mary at St. Theodore for the alert.

There is a new device login activity from a Windows 10 Mail app on your account Info@sainttheodore.org with the following information:

This sign in activity was made on:

Device	Windows 10
When	Feb 09, 2021 7:25:39 AM EST
Where*	Allentown-PA, United States
	IP Address: 882.786.98.493

If this was you, you're all set!

Didn't sign in recently?

Review your account activity and remove the devices and apps that you don't recognize and call our helpline number at 1-888-970-3797 immediately to revoke the unauthorized access else your phone or computer associated with this particular account will be locked.

Thanks,

Microsoft.Security Team

1-888-970-3797

 Microsoft Microsoft 365 Office Windows Surface Xbox Deals Support

We will never ask you for your password in an email. If you don't trust a link in an email, go directly to the normal sign in page

8/20/19

Invoice Scam

Our thanks to Mary at St. Theodore and Maggie at St. Simon for bringing the following scam email to our attention. If you receive the email from Parking-ORR@rb4u.co.il, do not open it or the attached link. It could contain malware. The email follows.

Good morning

Attached is the requested invoice for order# 38190.

Please let me know if you have any questions.

Thank you.

Thanks & best regards

Rosemary

Accounts Receivables

Fayetteville, Arkansas Office

O. 479.695.4361 | C. 870.475.6699

An Independent Member of the BDO Alliance USA

7/11/19

Domain Renewal Scam

Yesterday Paul Gilgum, Director of Information Technology, sent an email to parish email addresses notifying parishes of a major scam that is targeting many Dioceses and Catholic entities this summer. This scam revolves around DNS renewals for your websites. They are falsely stating domains are up for renewal. If you receive a renewal make sure it is from your legitimate provider.

Please check your official archdiocesan parish email (PARXXX@archstl.org) for examples of the scam correspondence.

5/3/19

Network For Good Scam



Our thanks to Marcia in Shared Accounting for this alert.

A parish received a special message along with a \$50.00 check from Network for Good. The message indicates that the parish may apply for a grant AND that someone made a donation to the parish via their network. - hence the \$50.00 check. The message also indicates that "by depositing this check you agree to the Network for Good Giving System Agreement".

By cashing the check, thereby agreeing to their terms, you are agreeing to pay a minimum of \$200 a month to use their donor software. The Archdiocese has not vetted this vendor and does not recommend using their software.

Please inform all parishioners and donors that Network for Good is not a recommended vendor.

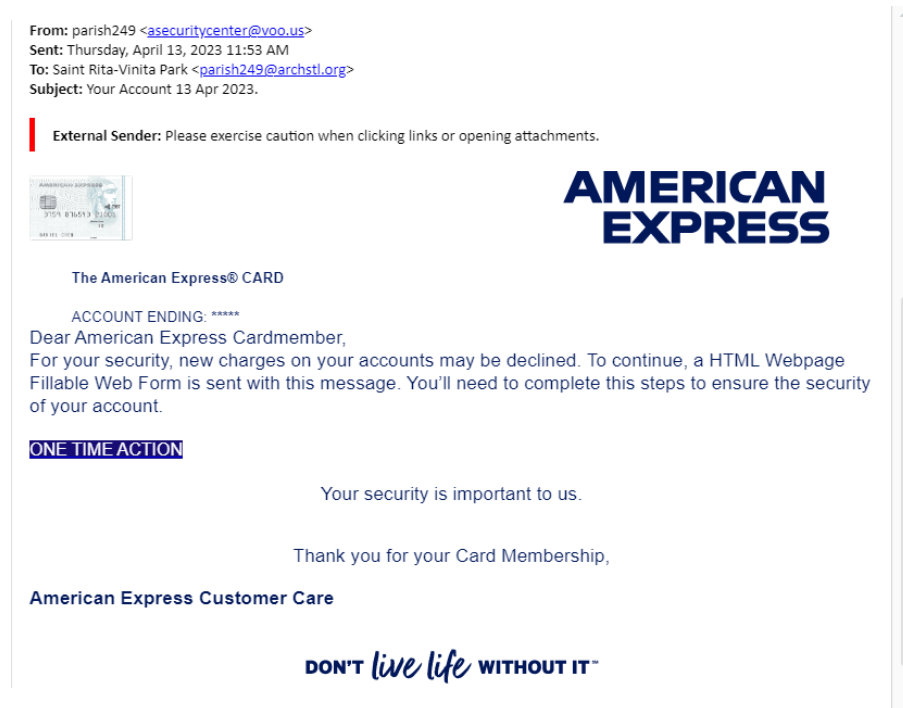
Phishing Scams

4/18/23

American Express Scam Alert

Below is a recent phishing attempt received at an Archdiocesan parish. Often the scammer creates an email message with a forged sender address in hopes of deceiving the recipient into thinking the email originated from someone other than the actual source. In this case the sender and the recipient are the same, with one having the fake email address. Scammers will use email spoofing to help disguise themselves as a legitimate organization or business associate to trick recipients into performing some type of action.

In this instance, the scammer is notifying you that charges on your credit card have been declined and asks you to complete a fillable web form to obtain parish/personal information that will be used to make you a victim of identity theft or credit card fraud. If you ever receive a phony notification such as this, do not click on any link or call phone numbers provided in the email. Rather, contact the real company directly at a phone number or website that you know is legitimate. Thank you to Sharon at St. Rita who reported this scam.



1/19/23

IT Desk Support Phishing Email Scam

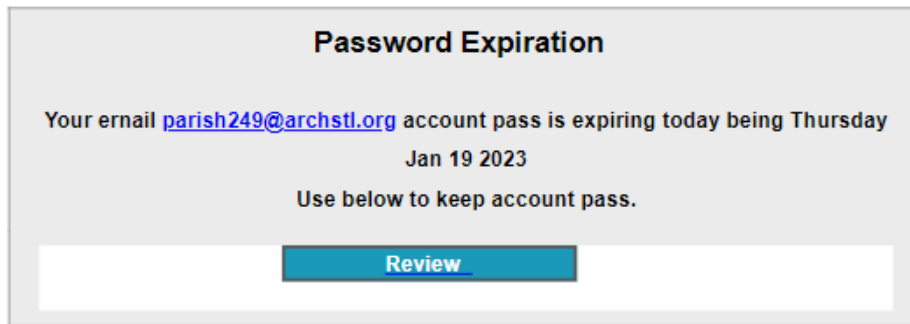
We recently received a report of an email scam that appears to come from the Archdiocesan IT Help Desk. A copy of the email content is pasted below.

If you look very carefully at the from address you can see this is definitely not from our Help Desk. The email notifies the recipient that their password is expiring today, and gives very little direction but includes a box which they are hoping you will click on for more information or to change your password. The unusual language and spelling errors should also make you question whether it is a fake.

The IT Department has blocked this email from appearing in any Archdiocesan email (archstl.org) inboxes, however, you may see this email in your other email inboxes. If you have received this email and responded or clicked on a link, please change your password immediately. Thank you to Sharon at St. Rita for alerting us to this phishing email.

From: ITDeskSupport_archstl.org_01/19/2023adminconnector83fhry93
<weecare@npgcable.com>
Sent: Thursday, January 19, 2023 1:40 PM
To: Saint Rita-Vinita Park
Subject: user 12 Automated Service Request on,Thursday Jan 19 2023

This sender is an External Email.



This email was scanned by Bitdefender

New Phishing Scam Approach

It is important to note that scammers are getting more creative in order to make scams appear more legitimate. A new scam approach focuses on prior subject and email threads in the hacked email account. Scammers are hacking into email accounts and look for common subject matter and discussion. Since so many email clients look for subject matter, and try to verify it with previous subjects/discussions, scammers will often take an old email thread, and add to it, so participants in the initial thread, will assume it's something legitimate. The scammers will then attach a document or a link which will direct you to give them your credentials. Often they will repeat this attempt with all of those in the email thread. As scammers continue to improve their ability to produce deceptive emails, parishes must be more diligent regarding any email, even those from someone you know. Often the scammer will make the email appear as it has come from someone you trust. If you weren't expecting the email or attachment and the email seems odd to you, don't open it. The worst that that can happen, is you may receive a phone call or a follow-up from the person who sent the valid email.

Pictured below is a recent example of this type of phishing email scam received by parishes.



Thu 12/8/2022 7:36 AM

Shelly Lane <Patrick.Francis@freesilverloophole.com>

Re: SVDP Agenda May 4, 2019

To Frances Schmitz

Follow up.

If there are problems with how this message is displayed, click here to view it in a web browser.

Kindly tell me what you think of all these documents enclosed.

[SEE DOCS](#)

Have a good working day

Dear St. Anselm Vincentians,

Thank you, thank you for your efforts in praying for Madeleine Huber. Because of your prayers, her injury did not define her season nor career. Please know how grateful I am for you and your kindness in praying for her. Please see the article below to read how her season ended.

[dir="ltr" class="gmail signature" data-smartmail="gmail signature"> Mary Grace](#)

[On Wed, May 1, 2019 at 8:21 PM Ed](#)

[.roup@sbcglobal.net](#)> wrote:

Greetings Vincentians!

Happy May Day!!!!

Attached is the Agenda for Saturday May 4, 2019.

- **Pre-Call Ministry will meet at 9:30am in Parish House**
- **Please keep Joe Coleman in your prayers (Sally Coleman's husband)**
- **Please keep all our special intentions close in prayer**
- **Remember to keep the Birthright Luncheon on your calendar**

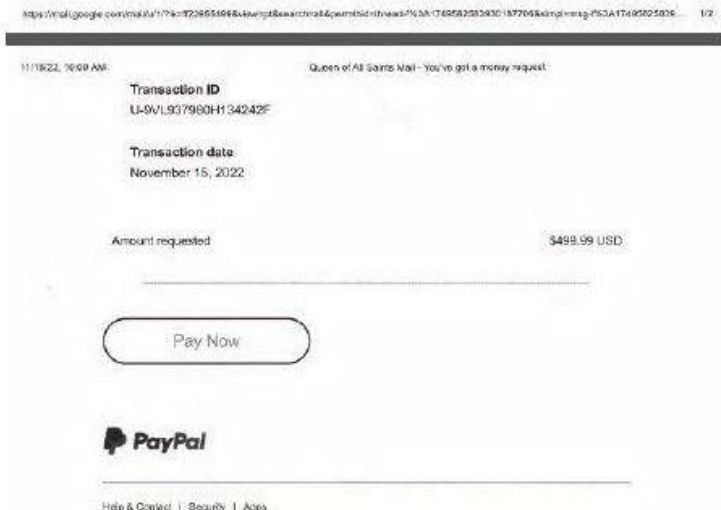
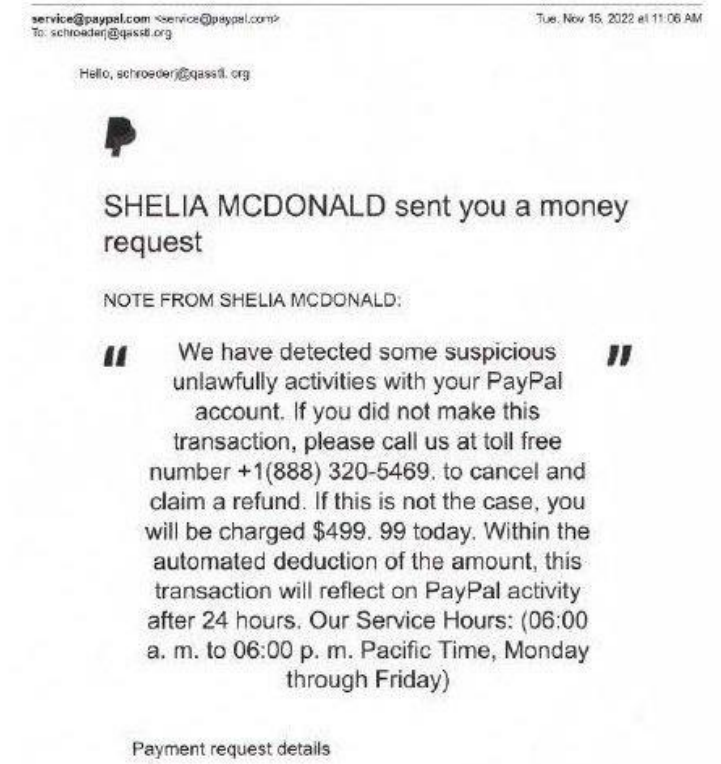
See you Saturday 😊

Thank you

Ed

PayPal Money Request Scam

Pictured below is a recent phishing email scam that was received by a parish. In this scam, the parish is being informed that some unlawful activities have been detected with their PayPal account. It is instructing them to call a number to claim a refund. If you do not call the 888 number, you will be charged a sum of money today. Email scams such as this one often direct you to call a toll-free number if you have questions or to stop the transaction. If you were to call, they would certainly try to get you to give them your account number or personal information.



7/25/22

More Phishing Scams

It is important to note that scammers are getting more creative in order to make scams appear more legitimate. Your name not appearing anywhere on the invoice or confirmation is the most obvious indication that the invoice is fake. An unusual email address listed for the retailer is another red flag. As scammers continue to improve their ability to produce deceptive emails, parishes must be more diligent regarding any invoice or confirmation that comes via email and never call a number given in an email without checking the validity.

Pictured below are examples of recent phishing email scams that were received by parishes. Amazon and Walmart are both trusted retailers, and unfortunately scammers are using their reputations to trick customers. Parishes may receive an email invoice or confirmation from a scammer posing as Amazon, Walmart or other large retailers thanking you for a high dollar purchase. Email scams such as these often direct you to call a toll free number if you have questions regarding the purchase or to cancel the purchase. If you were to call, they would certainly try to get you to give them your account number or personal information.

Also, pasted below is another bank account email scam that is using a local bank you may be familiar with or actually have an account with. In this instance, they are asking you to click on a link to verify your account, which will of course lead to the scammer asking for your personal information or account information.

Thank you to Susan at St. James and Cheryl at All Saints for alerting us to these scams.

From: social <social201610595@social.helwan.edu.eg>
Sent: Friday, July 22, 2022 9:51 AM
Subject: Order Shipped



Order Successful!

Your Purchase is confirmed. Thank you for choosing Walmart.

You made a purchase of HP Envy Wireless Printer. The payment has already been deducted from your account.

Your order Id is B2162151. The charge will appear on your credit card statement as "WALMART", Payment sent to Walmart.

If you have any issues with this purchase or want to stop this order, reach us at +1-801-436-3176.

Thank you for doing business with us.

Walmart
+1-801-436-3176

From: noreply_
Sent: Friday, July 22, 2022 7:18 AM
To: undisclosed-recipients:
Subject: Shipped@3680



Your "ASUS Vivobook 15 Gaming Laptop" has been dispatched, below are details related to the purchase.

If you want to make any changes please call +1 (888) 303-6290

Arriving: 22 July 2022

Ship to:
William J. Jackson
2968 Lucky Duck Drive
Crafton, PA 15205

Your purchase with Order_ID-195-39849-3984 is under process

Order Summary

Placed on: 22 July 2022

ASUS Vivobook 15 Thin and Light
Laptop 15.6" FHD Display, Windows
10 Home, F512JA-AS35

	Price: \$499.00	
Item Subtotal:		\$499.00
Shipping & Handling:		\$15
POD Convenience Fee:		\$0.00
Delivery:		\$0.00
Shipment Total:		\$514.00

If you did not Place Order. Contact Amazon Fraud Department on:

+1 (888) 303-6290

5/17/22

Verify Mailbox Email Scam

We recently received a report of an email scam that appears to come from the Archdiocese asking recipients to verify their email account. The email is clearly coming from an external email not from the @archstl.org domain. This should be the first tip that the email is fake. A copy of the email content is pasted below. If you have the email in your mailbox, please delete it. Thanks to Sharon at St. Rita for reporting this scam.

From: Webmail Support <info@accountgrade.net>
Sent: Tuesday, May 17, 2022 3:00 AM
To: Saint Rita-Vinita Park
Subject: Re: parish249 ; You need to verify your Mailbox.

This sender is an External Email.

Hello parish249@archstl.org

Your mailbox needs to be verified. To continue using your account you need to verify your mailbox.

Go below to open and sign in using your enterprise credentials/username: parish249

E-mail: parish249@archstl.org

Password:

Please reply and confirm your mailbox or you will lose your account within 24 hours.

5/9/22

File Sharing Scam

The IT Department has alerted Parish Support to a new email scam variant. In this scam, a sender will send you an email, claiming to either come from a scanner, a printer, or some other method of file sharing (Google Drive, MS OneDrive, DropBox, etc). BUT, as you will see, in the below image, there is a twist.



Scammers have apparently realized that so many organizations are now utilizing banners, to let their users know when an email originates from outside of the organization (which decreases the likelihood of someone clicking a link). Above you can see our current example of this. In any externally sourced email you will see the blue banner with bold text that reads: "This sender is an External Email".

However, scammers have now started placing their own version of a banner message at the top of their emails, that will read similarly to the above screenshot. In this case, the scammer claims the sender is 'safe'... they even add a pretty green bar next to it, to make it appear so.

This message is NOT from the Archdiocese, and is NOT legit in any way/shape/form. Clicking on this link, would take you to an external website, that has a virus/malware payload at worst.. or will attempt to steal your credentials, at best. Either way, it's obviously not a good thing. Always remember, to check the sender's email address, not just the user name that has sent you the message, as well. If you ever receive one of these messages, they are scams, and should be promptly deleted. If you have any questions, please feel free to reach out to the helpdesk, or Shawn Markins at ShawnMarkins@archstl.org.

4/07/22

Misleading Walmart Order Confirmation

Walmart is a trusted retailer, and unfortunately scammers are using their name to trick customers. Parishes may receive an email from a scammer posing as Walmart thanking you for a high dollar purchase. In this recent scam, the email is directing you to call an 800 number if you have questions regarding the purchase. There are a number of red flags that indicate that this is a scam. Your name does not appear anywhere in the invoice and the email was sent from a gmail address not from Walmart.

The scammers often count on people being concerned that they are being wrongfully charged a substantial amount for a product they did not order. You are provided a telephone number to call to disprove the purchase. If you call the number, you will be prompted to provide personal information that will be used to make you a victim of identity theft. If you ever receive a phony invoice such as this and you think that it may possibly be true, don't click on links or call phone numbers provided in the email. We recommend you contact the company directly at a phone number or website that you know is legitimate where you can confirm that the invoice was a phishing scam.

Thank you to Ann at Mary, Mother of the Church for alerting us to this scam.

Below is a copy of the phony invoice presently being circulated.

From: Order Updates <tomthompsonfkso@gmail.com>
Sent: Thursday, April 7, 2022 11:09 AM
Subject: Walmart Transactions

This sender is an External Email.

Walmart Order!

Thank you for your recent purchase on Walmart. You paid \$ 1650.00 for this order.

Contact our Customer Service team at [+1-800-494-8635](tel:+1-800-494-8635) to provide a comment or ask a question about your order from our corporate headquarters.

Please find your order information below:-

Order Number: MCA 121 69

Order Date: 07-April-2022

Order Name: Sony A7 III Full-Frame Mirrorless Interchangeable Lens Camera

Delivery Mode : Debit/Credit card

Amount : \$1650.00

Amount has been duly received.

"If you received an order confirmation email from Walmart (other than this) but you did not place an order. Please report us at [+1-800-494-8635](tel:+1-800-494-8635).

We hope to see you again soon.

3/23/22

Large (Expensive) Item Donation Scam

It has been brought to our attention, that there is a new email scam emerging. The email is pasted below. This particular email is offering to give the recipient a Steinway grand piano. Keep in mind the sender may offer to donate another high dollar heavy item instead. If you respond, the scammer asks for your contact information or address. Often the unsuspecting recipient gives their contact information, usually including their cell phone number, because, after all.. this is a once in a lifetime opportunity, and the recipient doesn't want to miss it.

From: Christine Morrison els,con@aztecaconnect.com
Sent: Friday, March 4, 2022 6:04 PM
Subject: Steinway Grand Piano

This sender is an External Email.

Hello good day, I have a grand piano to giveaway to someone that can cherish it. Please let me know if you are interested or refer someone that may need it to me.

Thanks.

Now once the scammer has the contact information, they can use the cell number to attempt to create a clone of the number. However, the scam usually progresses to this: 'Oh... that's too far. I'm in [insert random far off location that's too far to pick up the item], I could ship it to you, I guess?' The scammer then agrees to have it shipped... then 1 of 2 things happen:

- 1.) "The shipping costs are going to be \$5k (or some other high dollar amount), could we split the difference? You pay for half and I pay for half? I'm sorry, but I didn't plan on spending this much to donate it."
- 2.) "The shipping costs are going to be \$5,000 (or some other high dollar amount), can you cover shipping?"

Now the trick, is that they need to make the shipping costs significantly less than the full value of the item, so it would only make sense to pay for the shipping... after all, it's still a GREAT DEAL!! They then have you wire the shipping costs to them via wire transfer,

or Paypal, or Venmo. (Or they may hack a legit shipping company's email, and have you wire the shipping costs to them). Once the funds are transferred, the scammer is \$5,000 richer. It is not uncommon for a parishioner to offer to donate a large item, so always proceed with caution.

Even when you know the donor, sometimes the shipping or moving charges can end up being an expense to the parish and the donated item may not be worth the expense.

3/10/22

Outlook Email Mailbox Scam

We recently received a report of an email scam that appears to come from "Microsoft" regarding your Outlook account. The email notifies the recipient that their password has expired and asks them to click on a link to keep their password. The email is coming from an external Chile email sender and is the first tip that the email is fake. A copy of the email content is pasted below. If you have the email in your mailbox, please delete it. Thanks to all those who have reported this scam.

From: Maria Narcisa Riquelme Vilches <mriquelmev@desarrollosocial.gob.cl>
Sent: Thursday, March 10, 2022 7:51 AM
Subject: Your Email Password Has Expired.

This sender is an External Email.

Dear Outlook/OWA Email User

Your Microsoft Outlook Account Password Has Expired Today
Follow instructions below, Click on Keep Same Password to
Continue using your current password

[KEEP SAME PASSWORD](#)

Microsoft Outlook©
Outlook Web App
Copyright 2022

1/26/22

Need a Favor Spam, Malware or Virus

You may receive an email that looks like it comes from a coworker, friend, or from a familiar organization, saying something like: "Can you do me a favor?" This particular email claims to be from Sheila Brennan and was quarantined by our malware, virus and spam filter. The quarantine message is pasted below.

These emails are not legitimate. They are being sent by scammers who are impersonating people in your contacts list to gain your trust and exploit you. These kinds of fraudulent emails, known as "phishing", attempt to gain your trust in order to access your personal and/or credit card information, or to get you to purchase gift cards. These types of emails could also contain malware or viruses.

DO NOT open, click any links or reply to such messages. Delete these emails immediately!



Hi there

I need a favor from you. I'm unavailable on phone, kindly let me know when you're online..

Sheila

1/4/22

Lottery Winner Donation Scam

We have received a recent report of an email received from Thomas Morris, a Minnesota Powerball winner claiming he would like to make a donation to support the Covid 19 pandemic in the community. Of course, this is too good to be true and is another scam attempt. Below is a copy of the recent email scam for your review.

Often with this type of scam, a person or organization is contacted by mail, email, or phone call by someone claiming to be a lottery prize winner. The scam artist tells the person they will share their prize if the person sends money to them or gives them personal information. If the person agrees, the scam artist convinces them to give out their bank information, mail a cashier's check, make an electronic funds transfer, or even arrange a meeting to get the money in cash. Please delete this type of email and do not click on any links. Thank you to Sharon at St. Rita for alerting us to this recent scam.

From: Thomas Morris Family <mbox@chem.pmf.hr>
Sent: Monday, January 3, 2022 12:42 AM
To: Recipients
Subject: *Donation From Thomas*

This sender is an External Email.

I am Mr. Thomas Morris my wife his Kathleen, we are the mega winner of \$228.9 million dollars from Power-ball company in Minnesota's, We have a donation gift of 7 million dollars for you to support the COVID-19 pandemic in your community from our Power-Ball Lottery Winnings. If you are interested, please reply back for more details. Email; official.thomasmorris@gmail.com

WATCH US ON YOU-TUBE CHANNEL:

<https://www.youtube.com/watch?v=2sZs7YZSH1c&feature=youtu.be>

We hope to hear from you soon.

Best Regards

Thomas & Kathleen Morris.

8/10/21

Interested In Your Church Scam

As you know, we are frequently being made aware of new email scams. Below is the latest email scam and the message received when you look up the email address. We have had reports of various names being used with similar content coming from the same domain. They may feature a "Let me tell you a little bit about myself" story, trying to make you sympathetic to their situation and may ask if you are willing to meet them after arriving in the area.

In this particular email, the domain is odd and asking you to meet with them is frightening and should make you question the authenticity. When receiving external emails always check to see where it is coming from and don't click on links within emails if you don't know the person or if you don't know what the email is regarding.

Thank you to Bridget at St. John the Baptist for alerting us to this email scam.

From: Hector Martinez [<mailto:hectormartinez362@gmailserver.com>]

Sent: Tuesday, August 10, 2021 9:31 AM

To: jwolffer@sjbstl.org

Subject: Interested in your church

Hello,

My name is Hector Martinez. I'm moving to your area soon. Over the last few months as I've considered moving, I've been looking to get closer to God. I grew up in a religious family, but it's been a long time since I've been to church. This past year has made me reconsider my life.

I'm making a fresh start, and I wonder if your church might be a good home for me. With my new beginning, I'm looking to attend a church where I will be welcomed.

Let me tell you a little bit about myself. Growing up my family moved around a lot, so I've lived all over the country. In my free time I enjoy watching sports and movies and reading. On a more personal note, recently, my spouse was unfaithful and we're now separated.

Would you be willing to meet with me after I arrive in the area?

Sincerely,

Hector

8/5/21

Cardinal Ritter Email Spoofed

Parishes are receiving emails from Becky Thevary of Cardinal Ritter Senior Services. IT has determined that Becky's email was spoofed. These emails are not being sent by Becky and all emails from her should be deleted. Most email platforms should direct these emails to your spam folder.

Email spoofing is a form of impersonation where a scammer creates an email message with a forged sender address in hopes of deceiving the recipient into thinking the email originated from someone other than the actual source. Scammers will use email spoofing to help disguise themselves as a legitimate organization to trick users into performing some type of action. Scammers use this method of deception because they know a person is more likely to engage with the content of the email if they are familiar with who sent the message.

6/30/21

Webmail Phishing Email Scam

Recently someone at a parish was tricked into clicking on a link and gave their credentials to the scammer. (See scam email pictured below). The scammer was able to pull our entire Archdiocesan address book. Our IT Department has taken the necessary steps to protect our email from this recent scam. If you know you have been tricked by a scammer, please notify our IT Department **immediately** at helpdeskrequest@archstl.org.

Scammers use email to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Scammers often update their tactics, but there are some signs that can help you recognize a phishing email. Phishing emails may look like they are from a company you trust. They often trick you into clicking on a link or opening an attachment. They may say they've noticed some suspicious activity or log-in attempts, claim there's a problem with your account or your payment information, say you must confirm some personal information, include a fake invoice, or want you to click on a link to make a payment. Do not click on a link unless you are sure it is legitimate.

This is To Inform All Webmail Account Users, That The Web Admin Is Currently Congested. We Are Hereby Deleting Inactive Accounts.
Please Notify That This Account Is Active By Verifying It Below

[CLICK HERE](#)

Webmail Verification Center.
Case number: 8941624.
Property: Account Security.
Copyright © 2021 Webmail Service
All Rights Reserved.

6/24/21

Contact@borgia.com Scam

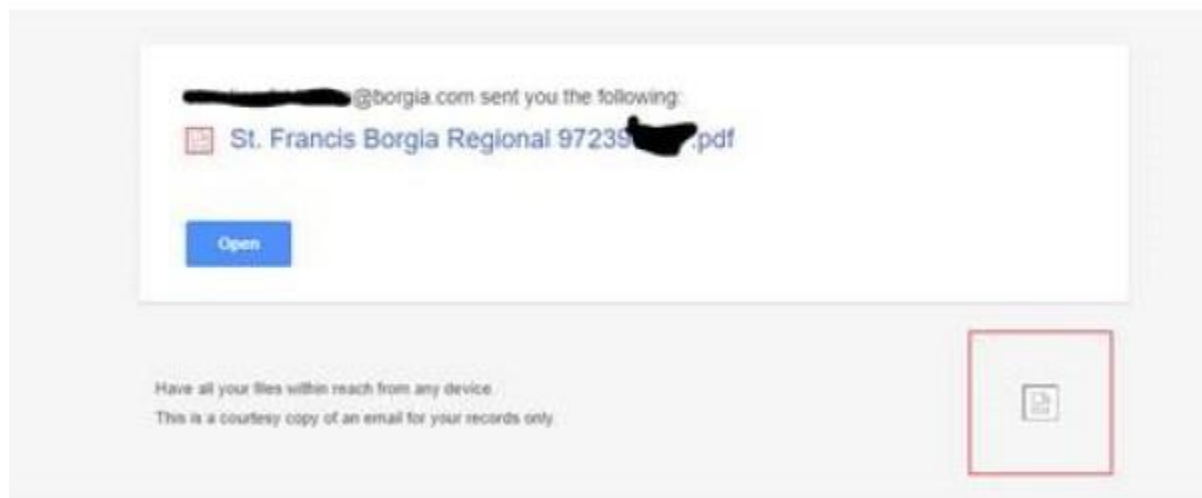
We received a scam report from our IT office. Please be aware of a scam email that has been arriving from contact@borgia.com

That email IS a scam, and the link within in, should NOT be clicked through, under any circumstance. They are aware of the issue, and have involved their IT group to address it.

Below, you will find an example of said email:

Please just delete the email.

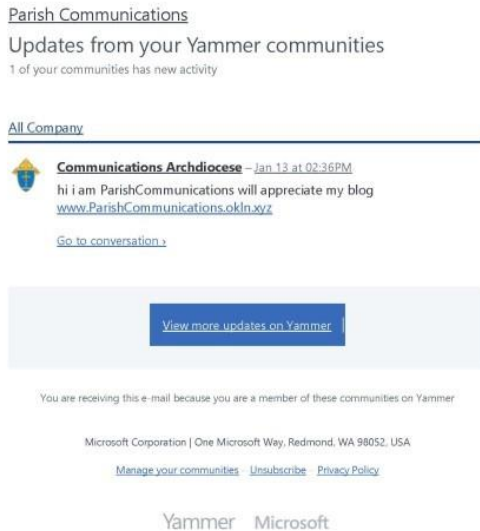
If you have clicked on the link, immediately change your email/login password, and contact the helpdesk.



1/14/21

Yammer Scam

Please be aware we are frequently being made aware of new email scams. Below we have posted the latest email scam. In this instance, the grammar is unusual and should make you question the authenticity. When receiving external emails always check to see where it is coming from and don't click on links within emails if you don't know the person or if you don't know what the email is regarding. Thank you to Laura from Immaculate Heart of Mary for alerting us to this email scam.



8/27/20

Archbishop Rozanski Scam

It appears the scammers have wasted no time in updating their contact list, and now claim they are Archbishop Rozanski. Please be aware, this is NOT the Archbishop, it is just a scammer that is using a script to pull data off of our website. (All current users, whose email is publicly available on the website, were targeted by this script/scammer)

A large number of you may have received an email (pasted below) from an external email asking for your time, and asking you to keep the contact, discrete. The scammer also claims to be currently unavailable, to attempt to get you to NOT contact them, in any other way.



The follow up email (often unsolicited, with no response having come from you) will then ask you to go out to a store, and purchase various digital currency.



Also, note the somewhat broken text, including improper punctuation, wording, and grammar. This isn't unheard of, with email sent from a mobile device, but any modern mobile device, will nearly ALWAYS capitalize *I* or *I'm*.

These forms of 'requests' are scams. Please don't correspond with the scammers. If you ever see a message similar to this, please alert the IT Department, and then delete it.

Below is another example of an email that the recipient should question the authenticity. It has some of the same improper punctuation, odd wording and grammar that should alert you to the possibility of a scam. It also has the "request" for action another scam feature.

From: Susan Ball-Carpenter <scarpenter@sedelco.org>
Sent: Tuesday, August 25, 2020 11:59 AM
To: helpdesk@desk.com
Subject: Re: IT Announcement

This sender is an External Email.

Dear Staff,

As part of a social and corporate responsibility in the light of the Covid-19 Pandemic, IT administrator has incorporated a responsive feature in our email domain to enhance our alertness to the pandemic. So, to incorporate this feature to your accounts,

Kindly log in to [Staff Webmail Portal](#) and the features will be added.

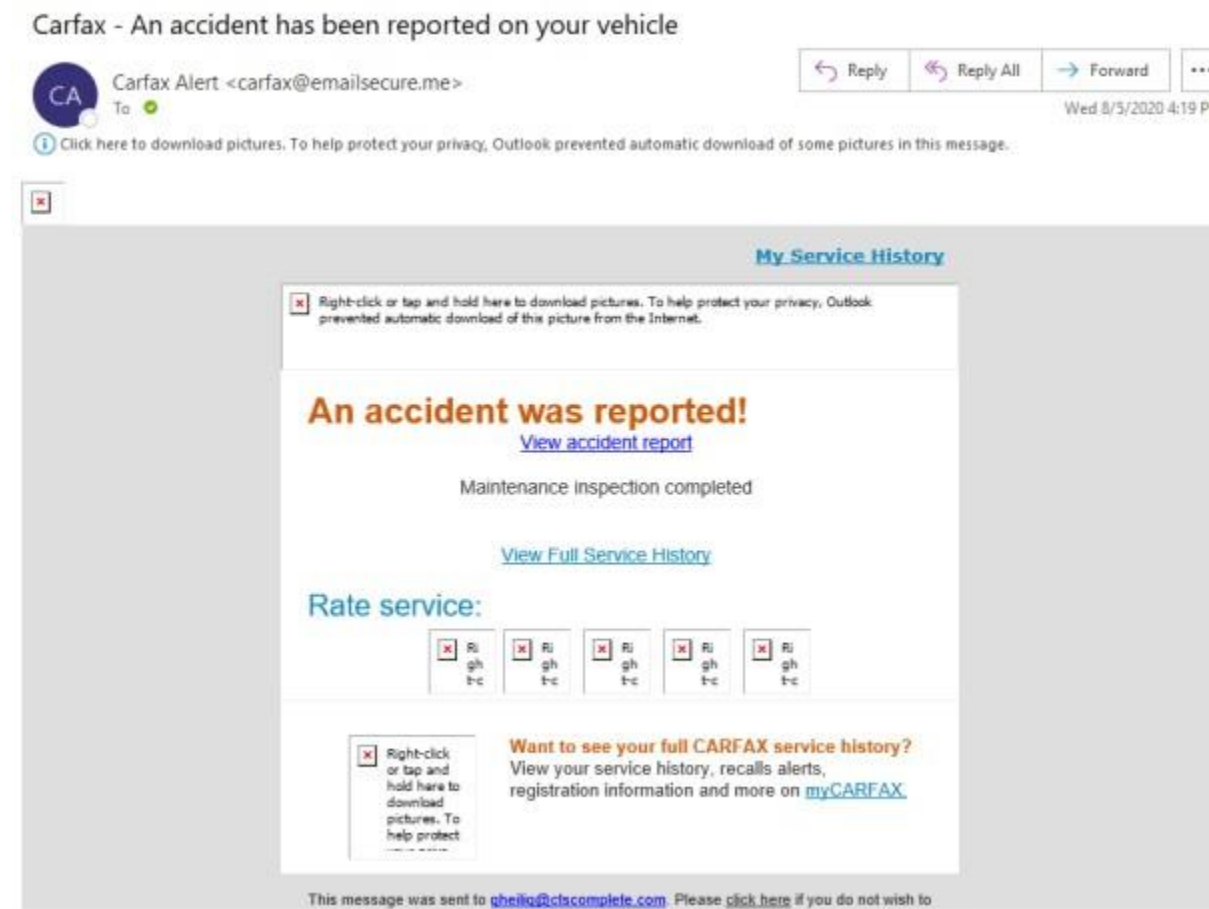
Failure to update your account, will lead to reduce functionality and subsequently account deletion from our database.

Sincerely,
Elaine Bully
IT Helpdesk
©2020 All rights reserved

8/6/20

Car Fax Phishing Scam

If you receive an email similar to the one pasted below, please do not click on any links in the email, it is a phishing attempt. When receiving external emails always check to see where it is coming from, if you don't know the person, don't know what the email is regarding, or if it just seems odd, don't click on any links within email. Thank you to Deacon Allen at Blessed Theresa of Calcutta for alerting us to this new scam.



7/10/20

Zoom Scam Alert

Some of you may have recently received an email from “Zoom Info” regarding acceptable usage and privacy updates regarding your accounts. It doesn’t appear to be a scam at first glance, but it is very sketchy marketing.

Below is an example of what the spam commonly looks like:



Be aware ZoomInfo is *NOT* Zoom. Please don't mistake the two for the same company. ZoomInfo is a data collection company that tends to scavenge the web, harvesting contact info.

If you've ever gotten a blind call from a telemarketer, or an email from one, trying to sell you something that is CLEARLY not related to your job...that type of contact info is what ZoomInfo gives to marketers. Due to their disreputable nature, most of their high level domains are automatically blocked by most anti-spam systems already. However, occasionally they will acquire new domains and send out mass spam to people. This latest email is an example of this.

They are NOT Zoom, and if you provided login credentials, for any reason, to that email, please go in and change your credentials immediately. Additionally, if you use the same password on Zoom, that you use for ANY other system, (Work related or not). You should go ahead and change that password on EVERY system you use it on. Using the same password more than once, anywhere, is considered bad security practice, and you're just opening yourself up to a potential data breach somewhere down the line.

If you ever receive an unsolicited email like this one NEVER respond to it. If you do, you have confirmed that the email is a good email address to target for other unwanted solicitations and/or potential attacks.

IT will remove this spam from Archdiocese mailboxes, and adding this new domain to our ban list. Please feel free to contact IT, if you have any questions.

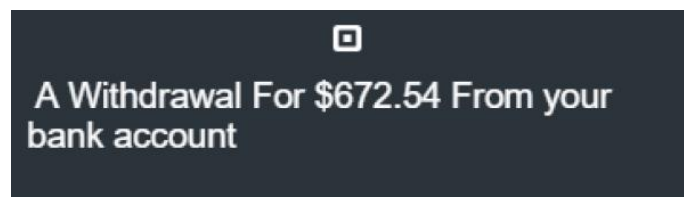
12/12/19

Square Phishing Scam

As a reminder, the Archdiocese has never recommended the use of Square, PayPal, Ebay, Amazon and Venmo as payment options. Clover is the only payment system vetted and approved by the Archdiocese. Please be aware that phishing scammers are sending emails that appear to be from payment system provider Square. There are several different versions, but many use the Square logo and seem legitimate. In one common version, the message claims that you accepted a payment and provides credit card details. In another, a client has allegedly requested a refund and funds are being removed from your account. Both messages urge you to click a link and “View Full Payment/Refund Details” or “Deposit Now.” Whatever you do, don’t click the links, open attachments or reply. They can download malware to your computer that can acquire your usernames, passwords and even sensitive information, such as your credit card number.

Scammers are using the Square name and other legitimate business names to fool their targets. In this particular email they have added the Constant Contact logo to make it appear more genuine. Square and other legitimate businesses will never ask you to provide sensitive information such as your username, password, social security number, full bank account details, or payment card information over email, phone, or text message.

Once again recipients should pay close attention to the sender's email address. A genuine email would typically have their organization name in the domain. Also, look for unusual phrases and grammatical errors. Posted below is a sample scam email recently received by a staff member of Our Lady of the Holy Cross. Thanks to Lynda for reporting this scam.



Hi,

This is to inform you that your bank account will be debited the amount of \$672.54. However, Customer dispute on your square dashboard has been approved for refund.

The funds will be withdrawn within one to two business days. Kindly [View Dashboard](#) for more information

If you have questions about this withdrawal, please visit our [Support Center](#) for more information.

Thanks,

[The Square Team](#)

© 2018 SQUARE, INC. ALL RIGHTS RESERVED.
1455 MARKET STREET, SUITE 600

5/22/19

Mailbox Full Scam

Our thanks to Teak at Archdiocese for reporting this SCAM. Please be aware of the scam pictured below.

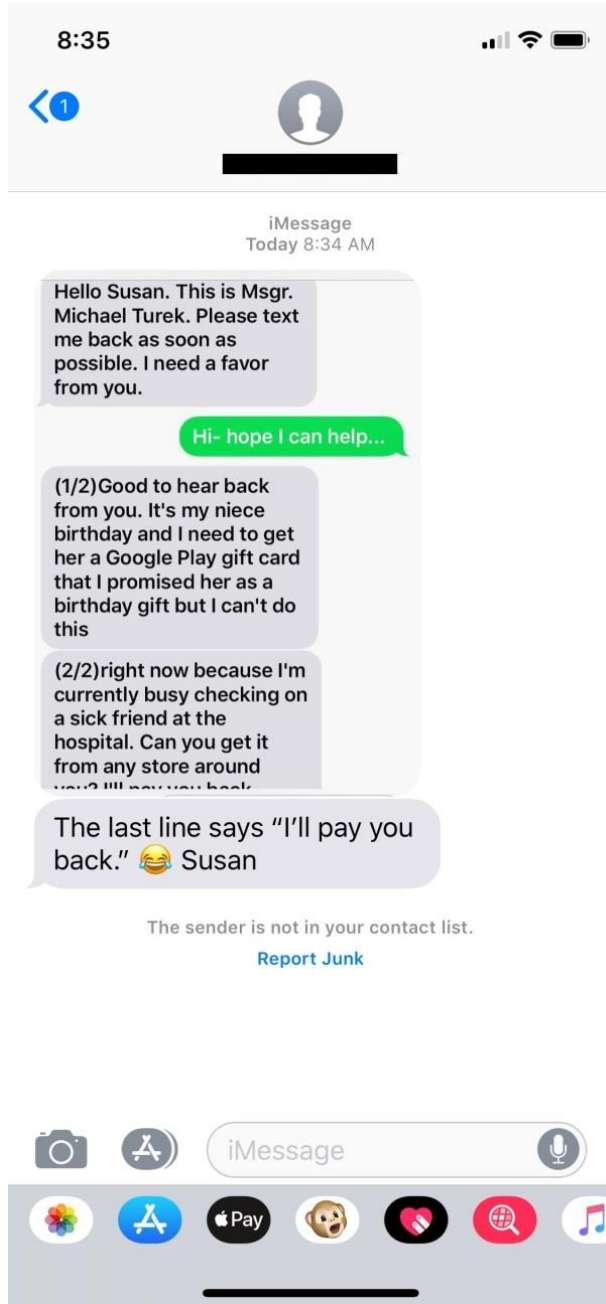


5/15/19

Texting Scam

Our thanks to Karen at Christ the King for reporting this new SCAM.

Karen reports that a school parent received the following text message this morning. The scammers used the parent's first name and the full name of the Pastor. Please alert



school parents and parishioners to this 'wrinkle' in scamming.

new

Index

ACH Payment Notification Scam.....	7
Amazon & PayPal Scams	58
Amazon Login Scam.....	29
Amazon Phone Scam.....	9
Ameren Scams.....	26
American Express Scam Alert	69
Archbishop Rozanski Scam.....	90
Archstl.org Listing Scam.....	57
Car Fax Phishing Scam.....	92
Cardinal Ritter Email Spoofed.....	86
Claiming Copyright Infringement Scam.....	34
Commerce Bank - Another Scam Alert.....	12
Contact@borgia.com Scam.....	88
Copyright Infringement Scam.....	31, 33
Deceptive Invoice Solicitation.....	64
Deceptive McAfee Invoice Scam.....	61
Diocese Gift Cards Scam.....	39
Direct Deposit Scam.....	5, 8
Direct Deposit Scam Alert.....	16
Domain Renewal Scam	67
Employee Retention Credit Scam.....	1
Event Invoice Scam.....	49
Facebook Non-Compliant Scam.....	32
FACTS and Faith Direct Alert.....	22
FBI Email Hack Alert.....	36
File Sharing Scam.....	78
Financial Audit Scam	11
Geek Squad Invoice Scam.....	55
Geek Squad Scam Alert.....	40
Gift Card Scam Alert With A Twist	38
Google Scam.....	35
Important Announcement from Tech Electronics	21
Interested In Your Church Scam.....	85
International Invoice Scam.....	48
Intuit Scam Alert	10
Invoice Scam.....	66
IRS Letter Scam.....	14
IT Desk Support Phishing Email Scam.....	70

Large (Expensive) Item Donation Scam	80
Lottery Winner Donation Scam	84
Mailbox Full Scam	95
Microsoft Outlook Email Scam	25
Microsoft Outlook Scam Reprise	24
Misleading Domain Listing Invoice	46
Misleading Invoice/Order Confirmation.....	44
Misleading Walmart Order Confirmation	79
Need a Favor Spam, Malware or Virus	83
Network For Good Scam	68
New Phishing Scam Approach	71
Norton 360 Phishing Scam	47
Norton Invoice Scam	60
Onsolve and iTunes Two New Scams	62
Our Sunday Visitor Scam	23
Outlook Email Mailbox Scam	82
Outlook Mailbox Password Expire Scam	22
Password Reset Scam	30
Pastor Email Scam Alert	37
PaycomOnline Scam Alert	4
PayPal Money Request Scam	73
PayPal Scam Alert	51
Payroll Email Scam	15
Payroll Scam Alert	5
Payroll Scam Warning	6
QuickBooks Phishing Scam	19
QuickBooks Scam Alert.....	54
Rottler – Financial Audit Scam	20
Scrip Card Alert	38
Select Office Supply Invoice Scam Reminder	56
Square Phishing Scam	94
St. Michael the Archangel Email Spoofed	36
Sumner One Email Scam	17
Texting Scam	96
United Rental Scam	53
Unusual Phone Call	39
Verify Mailbox Email Scam	76
Webmail Phishing Email Scam	87
Weinhardt, Awards, and Subscriptions Scams	27
Windows 10 Scam	65
Xfinity Invoice Scam Alert	50
Yammer Scam	89
Zoom Scam Alert	93