This is the first of a series of documents created by St. Andrew's parishioner Kelly Bourne, a retired computer security professional.

Cyber-safety Article #1 -What is Phishing?

Numerous members of St. Andrew's, myself included, have recently received text messages claiming to be from Fr. Keith. The recipient is asked to do a favor. Anyone that replies to these texts will be directed to purchase gift cards for Fr. Keith. These texts are examples of a phishing scam. No one at St. Andrew's will ever contact a parishioner by text or email asking for this type of contribution.

Phishing attacks can come in the form of a text, an email or a phone call. The essence of this scam is that the call appears to be coming from a trusted person or entity. For example, from a member of your clergy, your bank, a friend, a relative, an authority figure or a government organization. The bad guy is hoping that recipients will lower their guard if the sender appears to be someone trustworthy.

Disguising the actual source of digital communications is called "spoofing". There are several ways that phone calls and texts can display a false or misleading caller ID. The criminal may be using burner phones that will eventually be disposed of. They might be using 'disposable' or virtual phone numbers that are rented from a service provider. Calls can be made from a computer instead of an actual phone using technology called VOIP (Voice Over Internet Protocol) that allows the caller ID to be set to anything the scammer wants.

Email return addresses are also easily spoofed. Some email software lets them set the return address to anything they want it to be. A cybercriminal could use email addresses that look very similar to the one he wants to mimic. For example, email addresses keith@standrewsomaha.com or keith@st.andrewsomaha.org" are similar, **but not identical to Fr. Keith's actual email address of keith@standrewsomaha.org.** The first wrong address has the extension ".com" instead of ".org". The second has a period between "st" and "andrews". Tricks like this are used to fool unwary recipients.

There are dozens of types of phishing scams, but all of them want to manipulate you into doing something that isn't in your best interest. Examples of current scams include:

- You've missed jury duty or another court appointment, and a warrant has been issued for your arrest. You can make a payment immediately to avoid arrest and imprisonment.
- You're behind on your taxes. Paying them immediately will enable you to avoid a fine, arrest or other punishment.
- A friend claims to be traveling and has lost their ticket, passport, wallet or phone. They're asking you to send them money right away.
- One of your children or grandchildren is being held by authorities or criminals. You need to send money immediately for bail, a fine or ransom for them to be released.
- You owe a charge for traveling on a toll road in another state. Paying it right now will let you avoid late fees or arrest.
- One of your online accounts (Facebook, Instagram, Amazon, Google, Twitter, etc.) has had suspicious activity. It will be locked unless you click on a provided link and verify your identity

right away. In reality if you click on the link, you're taken to a website set up by the scammers. Your username and password will be stolen and allow them to log into your account.

- Your bank contacts you and wants your assistance is catching a criminal who works at the bank.
- A text message sent to you accidentally is meant to lead to an online friendship. Eventually your new friend will tell you about a sure-fire investment that has profited them greatly. They'll urge you to invest in it also.
- An online relationship quickly develops into romance. Surprisingly, you're never able to meet your romantic partner or see them via a video call. At some point they'll mention that they need money. Their parents might need an operation, a wrecked car needs to be replaced, or plane tickets to visit you are so expensive. Requests for money will get larger and larger until eventually the victim wises up or runs out of money.
- You're informed that you've won a lottery or other valuable prize. To receive your winnings, you must make a payment upfront for administrative fees or taxes.
- You're told that a package can't be delivered to you unless some missing information is provided. A link is provided where you can provide the required details. Any information you provide about yourself will be used for future scamming attempts.
- An email claims to have important information for you in an attached file. Opening the attachment will result in having ransomware or a virus loaded onto your computer or smart phone.
- Text or emails from social media contacts asking you to open an attachment, click a link, view photos, or send money are likely to be spoofing attempts. Before responding contact the requester via another channel, e.g., call them on the phone to validate the request.

Spoofing differs from spam email. Email spammers make no attempt to conceal the origin of their emails. Spammers just send out hundreds of thousands or millions of emails with their sales pitch. If even just a tiny percentage of recipients fall for their scam they'll make money.

St. Andrews isn't the only church that's being plagued by spoofing and texting scams. While researching this article I found that dozens of other churches are also being targeted. Texts from the rector asking parishioners to purchase gift cards for him or send him money electronically via Venmo, PayPal or Zelle are an extremely common phishing scam.

Red flags for many phone-based scams include:

1. You're asked to pay with gift cards, cryptocurrency, Western Union transfers, money orders or other unusual payment methods.
2. The caller pressures you to take immediate action.
3. You're instructed not to tell anyone else about this call or this 'deal'. The caller may insist that you remain on the phone.
4. You may be threatened with arrest, fines, penalties, etc. if you don't follow their directions.
5. The caller claims to be from Microsoft, Apple, Amazon, Google, etc. Major companies like this may respond to a request made by you but will never initiate a call to you.

Some of the best ways to protect yourself from phishing and other scams are:

6. Never open an email attachment unless you've confirmed that it's actually from the sender.
7. Don't click on links in emails. Use links in your browser's favorites list or enter the URL yourself.
8. Have a healthy skepticism of all calls, texts, emails, etc.
9. Don't accept phone calls from unknown numbers. Let the call go to voice messaging. If it's a legitimate call, they'll leave a message for you.
10. Don't respond to random text messages. Block the number and report it as spam.
11. If you're feeling pressured by someone during a call hang up.
12. Be alert for odd things. For example, why would the IRS or a legitimate company want to be paid using gift cards, Bitcoin, money orders, etc.?
13. Confirm claims about a grandchild being in trouble, a traveling friend who needs help or a pastor asking you to purchase gift cards before sending money.
14. Never forget what your mother told you - if a deal seems too good to be true, then it probably is.

Steps that you can take to help prevent scammers from contacting you again are:

15. Block the number on your phone to prevent future calls. On an iPhone tap the Info button, it's a lower-case letter 'i' inside a circle. Then tap the "Block Caller" option. On an Android phone go to your recent calls, press and hold the number you want to block and select "Block" or "Report as Spam"
16. Add your phone number to the Do-Not-Call Registry by going to the website DoNotCall.gov or call 1-888-382-1222 from the phone you want to register. Doing this puts your number on a list that registered telemarketers won't call, but it won't stop criminals from calling you.
17. Forward the message to 7726, i.e., SPAM. This will help your wireless provider to spot and block similar spoofing attempts in the future. To forward a text to 7726 do the following steps:
    1. Open the spam text then tap and hold on anywhere in the body of the message.
    2. A menu will be displayed on the screen. Tap on the "More..." option
    3. At the bottom right of the screen a right-facing curved arrow will be displayed. This is the Forward icon. Tap on it
    4. In the "To:" field enter 7726 which equates to "SPAM" on the phone keypad.
    5. Press the Send icon which looks like an upward-facing arrow on the right-hand side of the message box.
18. Set your phone to not ring when the calling number isn't in your contact list. The danger of doing this is that you might miss an important call. For example, your doctor's office might call you from a number that's different than the one in your contact list.
19. Download an application that will block unwanted robocalls. Examples of these apps are AT&T's ActiveArmor Mobile Security, Verizon's Call Filter, T-Mobile's ScamShield and US Cellular's Call Guardian. I haven't installed an app like this myself, but they have received positive reviews in trustworthy publications and websites.

Phishing and text scams are here to stay, but when you're aware of how the criminals behind them think you can protect yourself from being scammed. Taking a few precautions now can protect you from a great deal of trouble in the future.

-Kelly Bourne