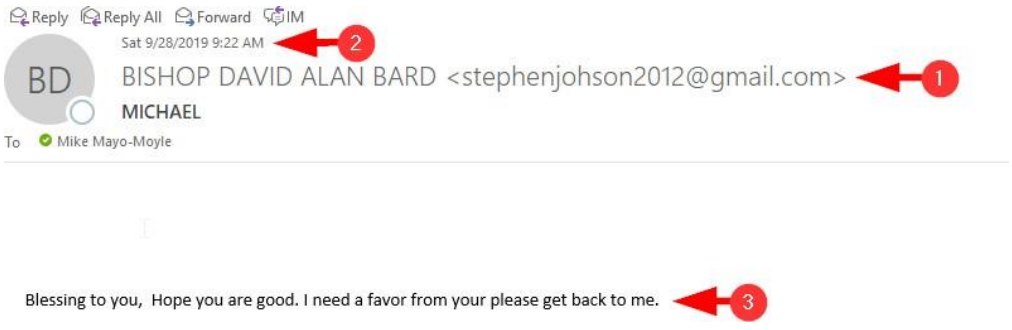
Michigan Conference
The United Methodist Church

Information Security for Local Churches:
Email

By now it is safe to assume that almost every congregation, or certainly members within the congregation have been the recipient of some sort of fraudulent email. While email provides a wonderful opportunity for quick communication, the underlying technology has been ripe for abuse for years with individuals using it with malicious intent to impersonate and defraud innocent people, both those naïve to the dangers of email, but even well-seasoned users who sometimes simply get caught off-guard.

The 2017 Internet Crime Report published by the FBI shows $1.42 Billion in victim losses for that year, though a variety of attacks including ransomware, tech support fraud, and extortion that aren't necessarily limited to email, but largely aided by it. I suspect there are a couple different factors at play behind the steady growth behind email scams. From the perspective of the scammer – creating and distributing fraudulent email is a quick and easy process – free email services are plentiful, gathering addresses of potential victims is simple and it only takes minutes to cast a wide net - sending out thousands of messages. From the perspective of the victim, our lives are so busy and we are so overwhelmed with email that we sometimes miss the clues that a particular message might be fraudulent, and all it takes is hitting "reply" or clicking a link to lead us to giving up personal information or transferring funds to the wrong people.

We are best served by viewing every email with an air of suspicion, being careful of any small details that might alert us that the sender is not legitimate. To use a real-world example, here is an email attempting to impersonate Bishop David Bard.



There are a few things to notice here:

1. Even though the email says it is from Bishop Bard, the email isn't coming from Bishop Bard's Conference email account. It seems unusual that Bishop Bard would be using "Stephen Johnson's" email to send a message.
2. While email can be sent at anytime, it is out of character for Bishop Bard to try to contact me at 9am on a Saturday morning.
3. Even though my name is used in the subject line, it is unusual that the Bishop doesn't address me by name in the body of the email. Plus, there are unusual grammatical errors that don't match my previous communications with the Bishop.

It is important to note that many scams are becoming much more refined than this one. In many cases the scammers are creating email address that try to match the person they are impersonating (i.e. something like BishopBard@gmail.com), and they will also add graphics or logos to make messages seem more authentic or insert text like "This notification was sent from a trusted source" in the body of the message. Furthermore, it is relatively easy to "spoof" the originating address to make the message appear that the message is coming from a legitimate source.

Here are some additional "red flags" to look for:

- Message has a sense of urgency ("I need you to reply right away"). Typically, if an issue is urgent the person should try to call you instead.
- Email is offered as the only means of communication ("Don't call, I'm in a meeting right now"), in an attempt to get you from verifying the communication or request.
- The email violates normal financial protocols – asking for gift cards or money to be wired from a church member instead of the Treasurer.
- The email contains an attachment you weren't expecting such as a PDF for a "refund" or an "invoice" from a company you haven't recently done business with.
- The email offers a "business opportunity" or financial windfall.
- Any government or business communication that is coming from a "free" email address like gmail.com, yahoo.com, outlook.com or hotmail.com.

Strategies to help avoid being taken in by a scam:

- If there is an attachment and you think it might be legitimate but are unsure, check it with your anti-virus program first, or upload it to https://virustotal.com before opening. (Virus Total is a service that checks files and URL's against a database of malicious programs and websites).
- If there is a link, do not click it, instead enter the address manually into your web-browser. (For example, if you get a suspicious message from "Amazon" log in directly at https://amazon.com instead of following the link).
- Always use a second means of communication when there is a request for money or personal information, using a contact other than what is provided in the email. If you get an email from your "pastor" to buy gift cards call them using their office number (or even home or cell numbers) first. If the "IRS" or "FBI" is emailing you, call the number of the local field office found in a Google search or in the phonebook.

- For church staff members – use professional email addresses for all correspondence (pastor-mike@FirstUMC.org instead of pastor-mike@gmail.com). If your church doesn't currently have their own domain and email service, they can be acquired and configured relatively inexpensively.
- Have clear policies around how financial requests are made and dispersed. Make it clear to members of the congregation that a pastor or church staff person will NEVER make an appeal for a financial gift (like gift cards or money to be wired) through email. Any unusual requests for church funds should be reviewed by at least one other person before being dispersed.

Additional Resources:

Federal Bureau of Investigation. 2017 Internet Crime Report. https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Trade Commission. How to Recognize and Avoid Phishing Scams. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Phishing.org - https://www.phishing.org/ - resource for better understanding different kinds of phishing attacks and how to better avoid them.

Virus Total - https://www.virustotal.com/gui/home/upload

For a low cost web-domain and email service consider UMCom's service at https://umcchurches.org/ which provides options for both services at a reasonable cost.

Churches can also get hosted email service using their custom domain through the non-profit offerings from Google and Microsoft, both available through TechSoup – https://techsoup.org

Got Phish - https://decentsecurity.com/#/malware-web-and-phishing-investigation/ which provides resources around evaluating and reporting phishing emails.