NEW PHISHING SCAM USES CHURCH PASTORS' NAMES AS BAIT

by Gary Guthrie

An old email phishing scam targeted at church-goers has been picked up and dusted off, hoping to find new victims it didn't hit the first time around.

The basics of the scam are that church members get an email from their minister requesting for them to make a contribution to the church by buying and sending in gift cards.

The emails seem harmless enough. They have the local pastor's name and an email address that looks legitimate, but upon further inspection, the email address is actually from a provider different than the one the church typically uses. In some instances, the sender's name may look correct but is missing a single letter.

In the new version, the phishers are using text messaging to try and fill up the collection plate in their favor.

One report out of Delray Beach, Florida asked the victim to purchase several gift cards, take a photo of them, and send those photos to the "pastor."

That sounds innocent except for the fact that gift cards contain numeric code that allows the scammers to turn the gift cards into actual purchases. In the case of the Delray victim, the phishers landed a really big fish -- $10,500 in gift cards!

"The key to protecting yourself from this scam is to first be skeptical whenever you get a request to wire money or make a payment through any form of gift card because once money has been wired or sent in the form of a gift card, it is gone forever, which is why these are favorite methods of payment for scammers," warns Steve Weisman of Scamicide. "As for gift cards, once you provide the numbers from the gift cards, the scammers utilize the gift cards to make purchases that they quickly sell in order to get cash."

“No church solicits gift cards nor does the IRS which is why when someone posing as a religious institution or the IRS asks for a payment through a gift card you can be sure it is a scam. The second thing that we all should do is to always confirm the legitimacy of any request for a donation of any kind before making a payment,” Weisman said.

Be cautious

Despite the lack of confidence consumers have in the government, the government can actually be of help in situations like this -- especially the consumer friendly Federal Trade Commission (FTC).

The agency has three important recommendations that might save you, the consumer, from being ripped off.

1. **Don’t text back**. Legitimate companies won’t ask you to verify your identity through unsecured channels, like text or email.
2. **Don’t click on any links within the message**. Links can install malware on your device and take you to spoof sites to try to get your information.
3. **Report the message to your cell phone carrier’s spam text reporting number**. If you’re an AT&T, T-Mobile, Verizon, Sprint, or Bell customer, you can forward the text to 7726 (SPAM) free of charge.

The best advice might be to forward any suspicious emails or texts to the FTC via spam@uce.gov. The FTC recommends that you also cc: the organization impersonated in the email/message -- a step that might give the scammer some pause before going ahead with their scheme.

If at all possible, include the full email header. Header information is typically hidden, but a quick search for “full email header” and the name of your email service (for example, Yahoo) will give you the steps necessary to find that information.