Six Ways Churches Can Thwart New Email Threat

Sophisticated messages can appear to come from a leader in the targeted church.

By Bobby Ross Jr.

Tim Samuel nearly fell for an email scam that has cost victims billions of dollars.

Samuel, chief financial officer for Bridgeway Community Church in Columbia, Maryland, received a message that appeared to come from the church's information technology director.

"I was blown away because... I almost got tricked," Samuel said. Not only did it look like it was from a fellow staff member, but the email had an "invoice" for a security training awareness program, and the church had been installing a new security system.

But when the CFO hit reply, Samuel noticed that the email address didn't match the one normally used by the sender (see "Actual Fraudulent Email" illustration). Something wasn't right.

The extent of the problem

The scheme that targeted Samuel's church is an example of what the Federal Bureau of Investigation calls a business email compromise scam—dubbed "BEC." According to an FBI review of domestic and international data, the growing problem resulted in 15,668 reported victims and more than $1 billion in losses from October 2013 through May 2016. Other estimates put the total monetary loss at more than $3 billion.

These fraudulent emails are often well-worded, appear to come from someone in the organization, and deal specifically with the organization being victimized—and thus do not raise suspicions about the legitimacy of the request, according to the FBI.

Victims range from large corporations to tech companies to small businesses to nonprofit organizations—and churches have become a frequent target.

"It's frightening because, for whatever reason, people are... clicking on these bogus emails, and wiring out money as a result," said Lisa Traina, a CPA and cybersecurity expert who heads the CapinCrouse subsidiary organization Traina & Associates. "It's pretty widespread."

For example, a Tennessee church lost $20,000 in the spring of 2016 when a staff member received a message appearing to be from outside the organization that a wire transfer be made in that amount.

In North Carolina last year, the state's attorney general issued a warning after scammers used authentic-looking emails to try to steal thousands of dollars from churches.
Targeting personal information

“There is a wide range of sophistication as far as the different kinds of scam messages I’ve seen,” said Douglas Ward, director of information technology for the North Carolina Conference of the United Methodist Church. “I’ve seen messages that are laughably easy to catch, that have a lot of horribly written grammar, really bad typos, incomplete sentences—things that stand out as pretty obvious forgeries.”

He’s also seen the other kind.

“I’ve seen a lot that are very complex and difficult to catch,” Ward said. “So, for example, if I wanted to pull off one of these kinds of scams, I would go to the company’s website and download a couple of profile pictures of the company’s executives. And then from that, you could create an email address and use that person’s profile picture for that account.”

Alerts by the FBI and others have made many church treasurers aware of the schemes, but criminals constantly adapt, leading to different iterations of the same scam, warned Michael E. Batts, a CPA and managing partner of Batts Morrison Wales & Lee, P.A., an accounting firm that serves nonprofit organizations. Batts also is an editorial advisor for Church Finance Today.

“For example, now they are spoofing a superior in the organization to ask for a copy of employees’ W-2 forms from last year,” Batts said. “So we’re seeing some variations on the theme, but the core element is that these crooks are spending time on an organization’s website long enough to learn what the email addresses of the superiors are, what sort of nicknames they go by, and then they use that information to create an spoof email that looks like it came from that person to ask for whatever, whether it’s money to be transferred or internal information.”

Six action steps

We asked experts and church financial leaders how church leaders can counter such scams. Here are six tips gleaned from their comments:

1. Don’t make financial payments based on email alone.

Call to verify that the individual actually requested the money, require a hand-submitted invoice or a second signature, or take other steps to reduce the possibility of fraud.

The North Carolina Conference of the United Methodist Church, for instance, doesn’t allow requests for wire transfers or money to be made by email or telephone.

“You have to fill out a piece of paper, walk it over, drop it off,” Ward said of this policy. “With some kind of physical control, you greatly decrease the possibility of a scam, if not completely preventing somebody from tricking you into wiring away $100,000 or whatever the dollar amount may be.”

Regarding his own church, Samuel has implemented a system prohibiting staff members from requesting emergency funds by email.

“At the end of the day, if you need emergency funds, there has got to be a better way,” he said.

Nick B. Nicholaou serves as president of Ministry Business Services, Inc. Nicholaou, author of Church IT: Strategies and Solutions, consults with churches about their IT needs and issues. Here, Nicholaou shares advice on how churches can avoid becoming victims of cybercrime.

What is a typical example of email fraud targeting a church?

We see churches targeted specifically with emails that look as if they’re legitimate, like, “Hey, the senior pastor told me to contact you and get a check for X amount of money.” Those kinds of things.

We also see a lot of fraudulent emails appearing to be from general vendors, like Microsoft and Apple. They look legit, asking you to update or confirm your profile information at places like LinkedIn or Facebook. And, of course, if you click the link, you’re taken to a site where your data can be collected or your identity stolen.

Is this a problem specific to churches or are churches getting caught up in something that happens to all businesses?

Everybody is being targeted, and many do not have appropriate spam filters that minimize exposure.

So spam filters will help prevent email scams?

A spam filter will prevent many of the emails that appear as if they’re from general vendors like Microsoft and Apple. A spam filter probably won’t block emails that appear to come from someone on staff. When this happens, the best approach would probably be to forward the email to the person that is referenced in it. They can then verify whether or not the request is legitimate.

What about verifying by making a phone call?

That would be wise. Sometimes you can reach them by phone; sometimes you can’t. But I would say to at least try calling them. Texting them on their smartphone is not as reliable since their phone may have fallen into someone else’s hands or been compromised. Public WiFi is not always secure, and if they get the text via public WiFi the verification is not solid. Someone could be “sniffing” the public WiFi airwaves and reading the text and other data that people are transferring via that public WiFi. In that case, it’s possible that someone could be picking up information that could compromise a system.

For a lot of pastors, coffee shops become a second office. So, it would seem that hackers would be more likely to be in those public settings.

Your observation is accurate. My recommendation is to not trust public WiFi. Instead, turn on the WiFi hotspot on your smartphone that turns it into a “MiFi.” Your connection will then go over your cellular data stream rather than over the public WiFi. When using your notebook computer at Starbucks, for instance, connect via the hotspot (or MiFi) feature of your smartphone, even though MiFi is a little bit slower and it means you may be paying for data. But you’ll know that by doing it that way your data transfers—like text and email—are more secure.

One more piece of advice: never click links in emails asking you to verify your data.

—Interview by Bobby Ross Jr.
2. Don’t make or authorize disbursements without documentation.

Traina stressed that the scammers have become more sophisticated than the elementary-level con artists once known for sending mass emails purporting, for instance, to have a $100 million inheritance in the bank if someone can just transfer $17,000 in fees.

“They are very sophisticated,” she said. “Oftentimes, the executive that these emails [allegedly] come from is, in fact, traveling. So they’re taking their time and learning who the players are, and that makes it scary.”

Regardless of who’s asking for money, every financial request should come with proper and complete supporting documentation, said the experts.

3. Allow church staff members to question any financial request.

In Louisiana last year, someone in the East Baton Rouge Parish school system was conned into wiring $46,500 to someone who claimed to be the superintendent, the Baton Rouge Advocate reported. The staffer retired after reports that she never sought verbal confirmation of the request, despite the superintendent being in a nearby office the whole time.

The bottom line: When a financial request looks like it is from the senior pastor or another person in a position of authority, paid staff members and volunteers should feel free to—and should even be encouraged to—find out if the request is legitimate, Samuel said. And they should be able to do so without fear of criticism or reprisal.

4. Create secure systems.

Secure IT systems that are regularly updated can greatly reduce the risks of bogus emails reaching staff members in the first place, Traina said.

While it sounds like something parents do to combat stranger danger, Traina said she heard of an organization using an internal code word for financial transactions that no one on the outside would know. She likes that idea.

Traina also encourages church leaders to determine what kind of information should not be shared online.

“Do you want people to be able to figure out that executives are halfway around the world?” she said. “You might want to be posting something cool that you’re doing [such as a mission trip], but by doing so, you open yourself up to more people tricking you.”

For further insights on developing security measures, see the sidebar on page 2, “More Insights on Preventing Cybercrime.”

5. Provide carefully targeted training.

Batts recommends educating a congregation’s team members about possible schemes and developing processes and policies to avoid falling victim to them.

Traina concurs, stating that members need to know how to detect schemes and should be armed with best practices that can help prevent breaches.

Specifically, training should include warnings about the dangers of clicking links from unknown email senders or opening attachments that could spread malware and steal sensitive data and financial records. Staff members should also know how to skim an email for clues that a request for money or sensitive information is bogus—such as spotting an email address that an employee wouldn’t normally use. And an entire training session or series of short workshops could be based on the Public Service Announcements on the FBI’s Internet Crime Complaint site (ic3.gov/media).

6. Take immediate action if scammed.

If your church falls victim to a scam, the FBI recommends contacting your financial institution immediately upon learning of the fraudulent transfer. Some banks have started waiting longer than normal to process such transfers because of concerns about scams.

The church also should ask that its financial institution contact the corresponding financial institution where the transfer was sent. And the church should contact the FBI and make a report via ic3.gov.

Moving beyond a close call

Looking back at his own close call, Samuel chuckles about one small sign of fraud that stood out: The sender’s address line said, “Sent from my iPad.”

The staff member whose name was spoofed doesn’t have an iPad.

Still, it was scary to think how easy it would have been for even a seasoned CFO to fall for a very costly scam. That makes it all the more important, he said, to double down on policies and procedures that protect the church from this type of cybercrime.

Q: What happens if a minister requests a housing allowance that exceeds his total salary?

We just hired a pastor, and he is purchasing a new home with a very large down payment. This will make the cost of his housing higher than his salary. How do we handle that?

A:

A church can only allocate an allowance up to the minister’s yearly salary—assuming the minister qualifies for an allowance based on IRS requirements, and the anticipated housing costs represent compensation for ministerial services, go exclusively toward paying housing expenses, and reflect fair rental value of the home (furnished, plus utilities). If a minister’s housing expenses are higher than that, it’s up to him or her to earn the difference elsewhere. If a minister does so, your church cannot designate more money for the allowance under the presumption that your minister will earn income from other jobs to make up the difference. Let’s say your minister earns $15,000 a year with your church, and he anticipates housing expenses of $17,500 for 2017. He cannot earn an additional $2,500 from working 10 hours a week at a coffee shop and have your church designate his housing allowance as $17,500. And those additional funds will be taxed like any other payroll because those earnings are not affiliated with his ministerial work at the church.

—Vonna Laue, CPA and editorial advisor for Church Finance Today

To submit a question for consideration in a future Q&A, email editor@churchlawandtax.com.
Time to Replace Dated Tech?

Churches wanting to replace dated smartphones and other tech in the coming months might experience some significant savings. “Look for an average 5 percent drop in the price of smartphones as low-cost versions from Chinese makers Huawei, Oppo, and Xiaomi flood the market,” reported The Kiplinger Letter in a special “Business Costs 2017” forecast edition. “Figure on paying 10 percent to 20 percent less for bandwidth as web providers battle it out for customers, though prices will vary by area. Satellite broadband costs . . . also down. Mobile data prices . . . down, too, by 10 percent or so.” Kiplinger also predicted that personal computer prices will drop but high-end tablets will “go higher.” As for printers and copiers, Kiplinger said prices could decrease by as much as 10 percent.

Connect Impact with Budget

It’s easy to assume attitudes around generosity have led to (decreased giving). But the truth is that today’s church members are just as generous as in years past. The difference is this: there are more organizations competing for the attention and resources of your church members than ever before. Research also tells us that people are beginning to split their charitable giving. How do we overcome this challenge?

We must give people a compelling reason to support our ministry. We must find a way to communicate the connection between the budget and ministry impact. This takes work, but it also gives us the opportunity to identify the things that inspire people to give and ultimately generate more momentum for our ministry.

—RSIStewardship.com

Giving That Goes Beyond Church Walls

Percentage of church attenders who also give elsewhere.

| Give to 1 to 3 other places | 54% |
| Give to 4 to 9 other places | 28% |
| Give to 10 other places | 7% |
| Give only to a church | 11% |

Source: 2016 State of the Plate survey, sponsored by MAXIMUM Generosity,-title by ChurchMag, Elavanto, ChurchOS, and Apollo Church Apps. The survey was conducted in 2015 and canvassed 1500 Christian pastors, leaders, and laypeople about giving and generosity in their church settings.

Key Tax Deadline

April 29, 2017

 Churches hiring their first nonminister employee between January 1 and March 31, 2017, may exempt themselves from the employer’s share of Social Security and Medicare taxes by filing Form 8274 by this date (nonminister employees are thereafter treated as self-employed for Social Security purposes). The exemption is only available to churches that are opposed on the basis of religious principles to paying the employer’s share of Social Security and Medicare taxes.

Note: If a date listed for filing a return or making a tax payment falls on a Saturday, Sunday, or legal holiday (either national or statewide in a state where the return is required to be filed), the return or tax payment is due on the following business day.

The free Tax Calendar—available on ChurchLawAndTax.com/ct—provides reminders about regular, semiweekly, and monthly withholding requirements, plus other upcoming dates and deadlines related to church taxes.

DOWNLOAD YOUR SkillBuilders!

Download the SkillBuilders on “Strategic Budgeting.” Visit CLTStore.com/SkillBuilders by April 30 and enter the code POST at checkout.