THE PARISH PAPER

IDEAS AND INSIGHTS FOR ACTIVE CONGREGATIONS

Editor: Cynthia Woolever - www.TheParishPaper.com

March 2015 - Volume 23, Number 3

What Churches Can Do to Increase Social Media Security

As email gained popularity in the mid-1990s, company leaders feared their employees would spend too much time with it and tried to limit employees' email use. Then spam came along, making people even more nervous.

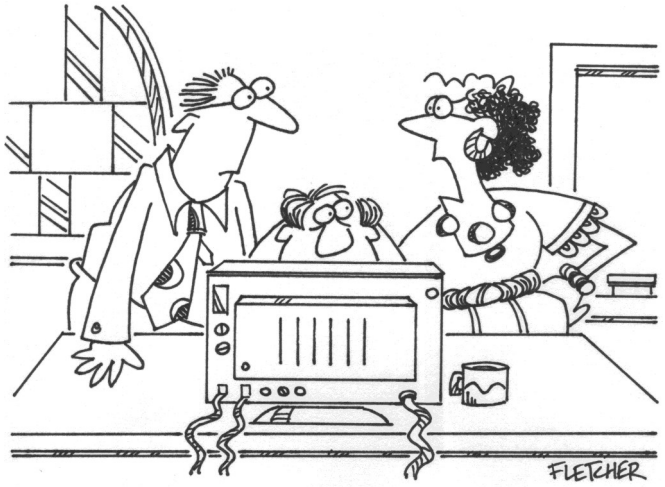
Today even the most anti-technology person knows that email is how information moves. Most also know that several commonsense safeguards go a long way to reduce risks—do not open emails or download attachments from people you don't know, nor should you trust that a Nigerian prince will give you $100,000 for allowing him to use your bank account to transfer his fortune to the United States.

Social media and online payment technology is in that "big deal" stage. Those in faith communities remain wary. Because they still do not quite know what to make of it, they would just as soon abandon social media as try to use it. However, social media and online payment systems make staying in touch and supporting the organizations we believe in far easier. But what about all those hacking horror stories recounted in the news? Could your congregation really be at risk for hackers stealing bank account numbers? Personal information? Photos? Yes. Fortunately, a few commonsense strategies help to keep you and your congregation safe.

Social Media Security Basics

No matter how you manage your social media and online payment tools, following four basic rules substantially reduce the risk of someone breaking into church accounts and stealing your congregations' personal information.

- *Create safe passwords.* This is hardly new advice but many people still ignore it. If your church's security passwords use names, common number combinations, addresses, email addresses, or common words, you are making it easy for someone to get into your account. Use a site like passwordsgenerator.net to create secure passwords that cannot be easily stolen. Write it down with pen on paper, and store it away. To make life even easier, join a single sign-on site such as lastpass.com to simplify login and vastly improve security.
- *Use the most up-to-date browser.* When you turn on your computer, a message often appears telling you a browser update is available. Because most browser updates involve closing security breaches that have been exposed, you avoid security risks by installing the update. Take five minutes and keep your browser updated. Your chances of being hacked go way, way down.
- *Do not open links from unknown sources.* Spend five minutes on social media and you are bound to see something like this—"Hi, I just saw your pictures here [link]." Do not be fooled. Hackers use these tricks to install viruses and spyware on your computer. If any anything looks suspicious, trust your gut and do not click on the link or open the file. If the note comes from a friend but looks funny, contact them and ask if they recently sent you an email. Chances are, their security has been breached and their site is being used to send bogus information.
- *Limit and protect your access information.* No one wants to believe that someone would take advantage of a church, but it happens. Therefore, limit



"I THOUGHT IT WAS A SECURE PASSWORD…
WHO WOULD HAVE CONNECTED, 'LONG_SERMON_LOVERS'
WITH OUR CONGREGATION?!"

the number of people who have access to your church's social media passwords. If your church has a professional technology person on staff, entrust that sensitive information with this person. Otherwise, the pastor and one key leader should be the keepers of passwords and account information. Although there are always people in your congregation willing to volunteer with social media, granting them access to church passwords and security information is a bad idea. Treat your passwords as you would treat your bank account. Be smart.

Added Security for Facebook and Twitter

Social media options are numerous and more are rolled out daily. Since Facebook and Twitter are the most commonly used, below are additional security guidelines.

Facebook. Churches love Facebook because it allows them to share photos, invite people to events, promote the congregation with targeted paid ads, create pages for groups within the church, and offers controls for who does and does not see posts.

But Facebook is not without its security problems. To begin, Facebook's security settings are notoriously difficult to understand. Take heart—there is help. CNET, an online tech magazine written with non-tech people in mind, offers seven keys to securing your Facebook page that should be required reading. Rather than replicate their advice, read it here: http://www.cnet.com/how-to/secure-your-facebook-account-in-six-easy-steps/. The advice includes how-to directions and will get you and your congregation in a safe space.

Several non-technical concerns arise with Facebook, such as the use of photos. There are many reasons people do not wish to have photos of themselves or, more likely, their children to appear on Facebook. People may work at jobs that require confidentiality or they may need to keep their identity secret. Parents worry, rightly, that posting photos and information about children can lead to identity theft. And some people are simply not comfortable posting their photos everywhere. When attendees join your congregation or begin to regularly participate, explain to them the social media tools currently in congregational use. Seek and secure their permission to use their photos.

Twitter. Churches are increasingly finding Twitter a useful tool for everything from connecting with the pastor to promoting events quickly among their constituency to sharing interesting information and discovering new friends. As with any other social media tool, Twitter can be hacked. Fortunately, if you follow the basic guidelines above, the congregations' security risks are minimal.

An additional step, however, will not only make your Twitter account more secure, but will make Twitter easier to use. HootSuite and TweetDeck were originally designed to help people manage their Twitter accounts and find the information they are searching for more easily. Increasingly, however, these sites are being touted for the extra level of security they bring to Twitter accounts. Both are critically reviewed, well tested, and highly reputable. Register with one of these and worry less about safety.

Securing Online Payments

Online payments are revolutionizing everything, including the way people give to their church. Multiple ways for handling online payments exist (see *The Parish Paper* issue for April 2014). In terms of security, there is obviously a lot at stake. Here are some simple tips:

- *Resist the temptation to create and manage an online payment system yourself.* Online payment systems are tricky, hard to navigate, and expensive. Instead, choose a solid third-party vendor to do this for your church. A number of organizations provide online payment options for churches. These can be a good bet, but review and watch for changes in the fees charged.
- *Consider PayPal.* This vender is often criticized, but the truth is, PayPal is an incredibly secure way for people to send your congregation money.
- *Follow the basic security guidelines.* If your congregation's staff are handling online payments, following the basic advice given above is even more important. Those four simple rules will go a long way toward protecting church leaders and the congregation.

Final Thoughts

With good reasons, many people remain jittery about social media and online payments. But fear without smart action only heightens security risks. Fear not. Basic, commonsense tactics remove the majority of your church's security concerns.

About the Writer: Martin Davis owns Sacred Language Communications, formerly directed Alban's online Congregational Resource Guide, and has twenty years of experience working with congregations (www.sacredlanguagescommunications.com).