A Dose of Humility by Tom Dedman, President/CEO
Southwest Montana Community FCU

With a strong dose of humility, I’m going to walk through our recent Web Site defacement incident. On Saturday, March 7\textsuperscript{th} at about noon, two different staff members called me saying they had been contacted by members stating our web site, www.swmfcu.org had been hacked, and our Home or Landing Page was now showing an ISIS logo with the statement “ISIS - We are everywhere.” That’s when the shock hit, and I was rendered temporarily brain dead (I know, many of you think I’m brain dead most of the time).

The image clip below illustrates what our home page looked like when browsing from an Apple based OS device. Folks browsing to it over a more traditional PC channel would have noticed ISIS Logo and statement inserted between our Home Banking Login bar and the photographs that float across the screen.

Our site is like many other CU sites in the country with marketing information about the credit union and why we’re so much better than our competitors. We have a spot to enter loan or membership application information, how to find our ATMs, etc... In our case, our website was developed by a local marketing company and hosted by Member Driven Technologies (MDT) on servers located in Helena.

We’ve had a compliance review for possible compliance issues and we knew that MDT made sure the machine hosting the site was all secure and the link to the outside world is protected and set to allow the kind of activity it was intended for, so all of that was in good shape. But, what I didn’t know or understand well enough was that the program used to develop the site’s graphics, layout, and functions was running in our folder on that server too. Many of the different components needed to have software updates. One of the pending software updates was released in February to correct a flaw that allowed anyone to inject graphics onto a site without having to provide a proper user name and password.
I happened to be out of town when all this happened and was unable to look at the site right away. One of our employees verified that indeed our site had been overtaken—SWMCFCU was broadcasting ISIS propaganda on its home page. We needed to shut it off as quickly as possible to keep from alarming too many of our members. One big problem, I couldn’t remember how to contact anyone from MDT after hours. I couldn’t even think if I had their afterhours phone number in my contacts list on my phone. (Remember, I was brain dead.) So, I reached out to one of their employees since I did remember their number. She called the tech on duty for the weekend, who then called me back in just a few minutes. We had the site shut down in about 30 minutes, which felt like an eternity for me.

While this was happening, I was also contacted by Ed Lester, Sheriff for Butte Sliver Bow County. He wanted to make sure we knew what was happening. In our visit, I acknowledged that we had been made aware of the issue, that the site was used for our marketing information, and that our member data is held on different systems. I told him that we did not believe that any member information had been compromised. My statement must have made some sense as he agreed with me. But he then promptly issued a press release to the local media. I guess nothing is more tantalizing than a financial institution with an image problem I guess.

**Communication Is Key**

In the early stages of an incident like this, it is very important to treat it like a robbery.

Make certain to ask law enforcement to keep the information confidential for the moment to help preserve any remaining evidence. It’s similar to not wanting to release details of how much cash was taken in a robbery.

**Know Your Website**

Do you know how to completely shut down your web page if it were to become necessary? Have you ever tested that process? For example, do you manually turn it off or have your tech support turn it off (preferably without pre-notice), so you know how long it will take in a live situation?

Are your members getting to your home banking page by first hitting your web site? Most of us tie these things together to make our web page more “sticky,” so people will go to it at least the Landing or Home page of the site. What happens when you have to shut your informational site down? Can members still get to home banking? Most of our home banking sites also have a unique URL (Uniform Resource Locator) address that can be used to get directly to the login screen of the home banking site. Do you know what that is? Can you publish that site’s URL in an emergency, so members can continue to access their accounts when your informational or marketing site is down?

Does the vendor hosting your website publish after hours contact numbers and procedures? If so, do you and others in the CU have this information at home or on their phones?

If something happens to your website, how or who are you going to use to perform a diagnostic or forensic analysis of what happened? This is done to find out when it happened, who did it, how far it went, and whether any member data was compromised. Perhaps someone from the CU has the skills to do this, when the compromise becomes public, you are going to want to use an unbiased third party to do this work. Who would you go to? Our friends at the NCUA, the Department of Homeland Security, and the FBI all have asked for our forensic report (in some cases we’ve gotten multiple requests from the same place). Sadly, the only way they will really believe that no member information has been compromised is by this proof.
Prior Planning is Invaluable

Plan in advance to have a really basic “Under Construction” page ready to turn on if you need to shut your main website down. Also include the address to your home banking page and tips to help members recognize that they actually reached the authentic home banking site. (Use the image and text verification part of the user’s id credentials.) Let members know any other procedures and be sure to include contact information, so members can contact the credit union and confirm the emergency site is legitimate. In some cases, a fail over page can be set to respond when the main webpage does not.

I’ve been reminded that things are now happening instantly. Be sure to have a plan for using alternate member communications channels before an event occurs. Radio or newspaper ads cannot be published quickly enough and cannot reach our target members without also spreading the news of a problem to a whole lot of other people.

Do you have phone numbers, email addresses, or other specific contact information? Can this information be used to reach out to your members by SMS text messaging, or email? Who on your staff knows how to do this? Have you ever tried to send out bulk messages as a test? Look for multiple ways to reach out to your members as no single channel should be depended on. Your host DP system, or home banking system may be able to do this. You may also be able to leave an announcement message on the login screens of the home banking system. With multiple channels to use, you have a much better chance of success.

What other communication alternatives do you have? Does the CU have a Facebook page or Twitter account? Who on staff knows how to post to these accounts? Do you have a sample or preset message that can be used in such an emergency?

It’s all about working with the media. You’ve just been in a train wreck and EVERYONE loves to gawk. You would think reporters are accurate, but they generally are not. Put the specific points of the issue into a press release. It helps you stay on point and can help to eliminate errors in reporting. We DID NOT use a press release and should have. While I clearly stated my name and spelling of my last name, the published reports called me Todd, Tom, and Tim. Not a big deal, but a great example of the confusion that can be created.

In a press release just state the highly distilled points of the issue at hand and K.I.S.S. (Keep It Simple, Stupid)

Vendor Management

Make sure you fully understand who does what for you with your website. We use two different companies, one to develop the site content, and another to host the site. While we had a great handle on the security of the equipment, the communications channels to and from it, and the operating system of the server, we did not fully consider that a special program used by the developer would also need to be monitored for updates and security. You know, that piece that allows you to update your own content (rates, product descriptions etc…). The developer’s job was finished when the website was brought up and all of the bugs were worked out. No one monitored for updates. The ONLY person that I could point a finger to was me. And, honestly, I should have caught this gap.

Do you have anything in place for a contracted response time from your website development company for emergency situations? Do they have a backup of your website as it was finished and accepted by you? It took about four hours from the first call for the site host to move the damaged site off, have an analysis done, and reset with a good backup. We had the development group change out a few items
and we were not able to turn the site back up until Sunday evening -- almost 30 hours after our initial call.