CYBERSECURITY

Why and how to protect your ministry from online attacks

Photo courtesy of Word of Life Fellowship

by Rebecca E. Sheriff

We keep money in banks, valuables in a fire-proof safe and we lock our car doors and homes. What do we do to protect our organization's digital assets and data? Likely not enough.

Photo courtesy of Word of Life Fellowship

According to a 2021 Cyber Peace Institute research study, three out of four nonprofits and nongovernmental organizations do not monitor their computer networks, and four out of five do not have any cybersecurity plan in place. With over 2,800 cyber threat groups currently at work across the globe, cybersecurity is an ever-present concern in today's digital world.

The Computer Security Resource Center defines a cyber threat as, "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service."

One Colorado Springs-based nonprofit, 10,000 Fathers and Mothers (10KFAM), recently experienced a costly and time-consuming cyber attack. The ministry of 10KFAM focuses on raising and releasing spiritual mothers and fathers who creatively shape the future of the Church through worship and discipleship schools. For two and a half months, from December 26, 2022 through March 8, 2023, 10KFAM spent more than 700 manpower hours and thousands of dollars to rectify a cyberattack from a group in Bangladesh.

The first indication that something was wrong was an inability to send internal company emails due to their company domain name being stolen. It quickly progressed into the 10KFAM team losing all control over customer databases, email marketing software, digital forms, social media accounts, Google Workspace data, website management and donor software.

Lauren Settembrini, executive director of 10KFAM, explained, "Because the hacker had control of the primary domain, they could intercept any email coming to us, send emails as us and lock us out of any site for which we had created a login (by resetting those passwords)."

Settembrini went on to say, "Within the first week, the hacker made contact through my personal email and Instagram account, apologizing for the 'mess' they had made and asking if we wanted our domain back. We were also alerted by Kindful (our database and donor platform) that the hacker had gotten in and tried to set up their own payment gateway to receive end-of-year donations themselves. It became clear very quickly that the hackers wanted money."

The access the hackers had gained gave them contact information for everyone in the organization's network, around 30 Social Security numbers, the organization's bank account information, passwords, email history and profile information for donors.

Settembrini said, "The cyberattack brought all normal business operations to a screeching halt within days. We had to cut off access to our customer and donor database and sever its connection to Stripe and our bank account, essentially canceling all recurring donor plans for their own safety."

While trying to fix their systems and recover access, 10KFAM worked with three different cybersecurity firms. The first was able to communicate with the hacker but couldn't move forward after the initial communications because the hacker still had administrative access to everything. ▸

With over 2,800 cyber threat groups currently in work across the globe, cybersecurity is an ever-present concern in today's digital world.

Settembrini was able to contact representatives at Google and Tucows Domain Compliance to get control back, however, the second firm was unable to ensure that the access was secure and private. "The hacker still had access somehow," explained Settembrini, "which I deduced from things they were saying in their correspondence that they shouldn't have known, like our attorney's name for instance."

At that point, 10KFAM brought in Mile High Cyber and worked with Terry Bradley, the organization's president and co-founder. "Within just a few minutes of having access to our Google Workspace, Terry found our smoking gun. The hacker had set up a 'rule' within our Google account at the very start of the hacking so that they were getting every inbound, outbound, internal and external email across the entire organization forwarded to them."

Bradley found that several safety notifications in Google had been turned off, "such as the notifications that are delivered when a password is changed or an unusual login attempt is made," Settembrini said. "Once Terry fixed that, on March 8, 2023, we haven't had another occurrence or word from the hacker since."

Bradley was a signals intelligence officer in the United States Air Force and worked at the National Security Agency after his military service. Mile High Cyber's mission is to "help businesses build and manage cybersecurity programs that avert painful and expensive security incidents so organizations can focus on their core business."

Bradley explained, "All cyber threat groups are financially motivated. The bulk of attacks are email account compromises, which the Federal Bureau of Investigation calls 'Business Email Compromises.' In a BEC attack, the hackers gain access to an organization's email system and perpetrate a scam to transfer money or payments."

Ransomware, which is a widely used term, "is when hackers lock up an organization's computers and data with strong encryption, demanding an extortion payment to release them," said Bradley.

Settembrini, following the advice of 10KFAM's lawyers and the first cybersecurity firm, negotiated with the hacker and agreed to pay the bitcoin ransom. However, the hacker did not follow through and give control back to the company and instead kept increasing the ransom amount.

Organizations of all sizes are vulnerable to cyberattacks, it's not just large multimillion dollar companies that are at risk. "Cybersecurity might seem like a luxury to a small nonprofit organization, but it's not," said Bradley.

"Cybercrime is an existential threat to small- and medium-sized businesses that needs to be addressed in advance to avoid expensive and painful security incidents," Bradley explained.

Many organizations that undergo a cyberattack have to shut down or rebrand entirely if they're not able to recover critical data. Sixty percent of small businesses that suffer a cyber attack go out of business within six months, reports the National Cybersecurity Alliance. ▸

"The cyberattack brought all normal business operations to a screeching halt within days." —Lauren Settembrini, executive director of 10KFAM

Top Cybersecurity Tips

How to better protect your ministry right now

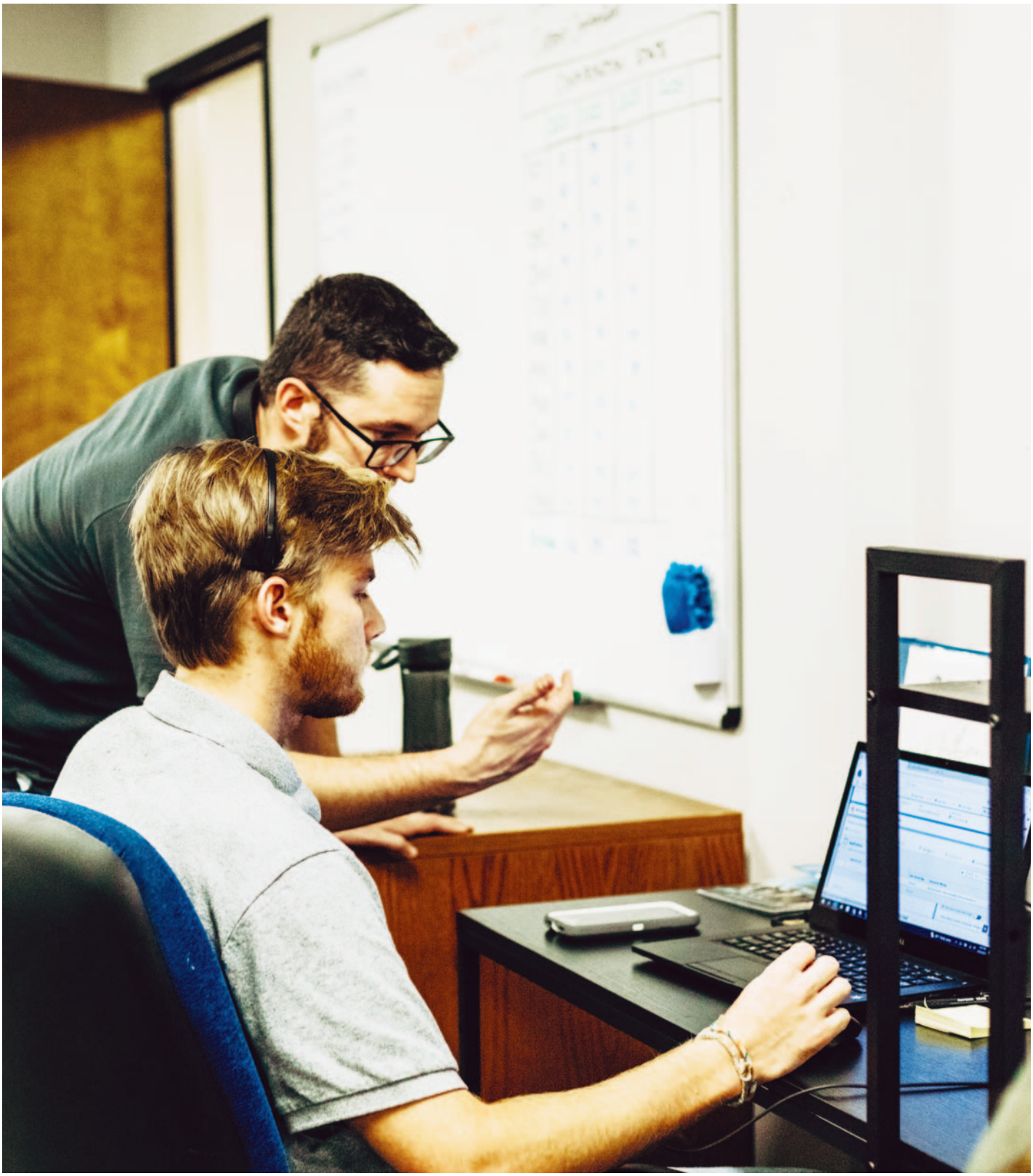
According to Terry Bradley, president and co-founder of Mile High Cyber, every organization should "have a baseline cybersecurity assessment performed by an experienced cybersecurity firm, then build a plan to address the identified risks."

Bradley offered a few tips your camp or conference center should implement now:

1. Utilize a password protection program, such as LastPass or Dashlane. Security Intelligence reports that just under two-thirds of data breaches could have been prevented by better password practices.
2. Enable 2FA/MFA (two-factor authentication/ multi-factor authentication) on every login that offers that option.
3. "Educate your entire team to be on the lookout," explained Lauren Settembrini, executive director of 10KFAM. "Tell them never to share sensitive information over email (it's not encrypted), never give information to someone claiming to be a customer service representative and enforce password requirements for them as well."
4. Schedule regular cybersecurity training for your team. "Training should cover real-world cyberattacks, how to recognize them and what to do if someone spots suspicious activity," shared Bradley.

Photo courtesy of Word of Life Fellowship

Photo courtesy of Word of Life Fellowship



"Cybersecurity might seem like a luxury to a small nonprofit organization, but it's not." —Terry Bradley, president and co-founder of Mile High Cyber

During the cyberattack, 10KFAM alerted their audience about the data breach. "We had to let them know for their safety because the hacker was sending emails pretending to be us, asking for payment information and checks to be mailed to an address they provided," Settembrini said. They also worked with their attorney to "provide identity theft monitoring for those who had sensitive information compromised."

According to 10KFAM, once the hacker had access to the ministry's Stripe account, they attempted to charge nearly $20,000 across dozens of donors. "Thankfully, between Stripe and the credit card companies, we do not believe the hackers received any money from anyone besides the initial ransom amount we chose to pay in an effort to get things back," said Settembrini.

Handling a cyberattack quickly becomes all-consuming. Settembrini shared, "It was all I lived and breathed for months; I almost forgot what my *actual* job was supposed to look like."

In retrospect, Settembrini said, "If I'd known how much difference some fairly simple, inexpensive steps would have made for me and 10KFAM, I would have done it in a heartbeat. It just wasn't the highest priority in my mind until it suddenly became the *only* thing in my mind."

Taking an active role in your organization's cybersecurity is one of the best ways to protect against a possible cyberattack. "Being proactive is prudent," said Bradley. "At a very basic level, nonprofits need to perform a cyber-risk assessment to document their risks and the potential damage they might suffer if successfully attacked. Once they've had a risk assessment, then they need to create a cybersecurity program to address the identified risks."

For more information on cybersecurity and how to protect your organization, visit Mile High Cyber at www.milehighcyber.com. ■

Rebecca Sheriff is passionate about experiential education, the power of camp and using horsemanship as a tool for ministry. She operates Sheriff Horsemanship, a riding lesson and training business out of Buena Vista, Colorado, and writes about faith and leadership. Rebecca received her M.A. in outdoor and adventure leadership at HoneyRock, Wheaton College's Center for Leadership Development.