THE DEACON'S BENCH®

BROTHERHOOD MUTUAL®

Practical risk management guidance
to help today's Christian ministries thrive

CAN YOU SPOT THE HIDDEN DANGERS?

Which of the following represents a type of cyber attack attempting to steal data from your ministry? *Find out on page 4.*

A: Spearphishing
B: Smishing
C: Phishing
D: Spoofing

Severe weather causes a power surge at a church and damages its A/V equipment. When lightning's a threat, _____ can protect your systems from damaging fluctuations in power. *Find out on page 6.*

Using realistic training scenarios with your safety and security team is a form of _____.
Find out on page 8.

True or False
Domestic Violence affects about 1 in 3 women in the U.S.
Find out on page 10.

TRUST *but* VERIFY

Defeating Cyber Criminals Before They Break In

One of your pastors is leading a group of volunteers on an overseas mission trip. You receive an urgent email that a volunteer was injured in a terrible accident. The email instructs you to send funds for life-saving medical treatment and provides a link to electronically transfer the money. Sensing the urgency of the situation, you take immediate action. Two hours later, the pastor calls to check in. You ask him about the injured volunteer. After a short pause, he asks, "what injured volunteer?"

Scenarios like this happen all too often. "Scammers use emotion to get people to act quickly to solve or prevent a seemingly serious issue – medical emergencies, late payments on a critical service like internet or utilities, even ransom payments for team members traveling abroad," shared Matt Cohee, a network security analyst with Brotherhood Mutual.

The technique is called social engineering, and the goal is simple – to get you to act before you have time to think. The result can be stolen funds, stolen information, or ransomware placed on your computer network, any of which can tie up your organization's resources or even cripple your operations.

Five Common Tricks of Cyber Scammers

Scammers use many schemes when attempting to steal your data, but you can outsmart them by understanding their methods.

Phishing emails are one of the most common ways scammers try to get data or gain access to your network. They typically incorporate elements of surprise, scare tactics, or fear of imminent danger.

Spearphishing is a targeted phishing attack that uses personalization in the email to make it appear legitimate. Hackers may even use information from your organization's website or social media account, or your pastor or head of school's social media account, to craft an email specific to your church, school, or camp.

Spoofing imitates an email address or website to make you think you're interacting with someone you know and trust. Hackers typically change one letter and hope you won't notice. An example email address could be: pastor@dtchurch.org (real) and pastor@dtchurch.com (fake). Once they gain your trust, they can lead you to download malicious software, release funds, or disclose sensitive information.

Vishing and Smishing are another form of phishing. The scammer uses phone calls or text messages instead of emails.

Pretexting creates a story in order to gain your trust. The story, or pretext, uses trust to manipulate you into thinking the scammer is legitimate. For example, someone might impersonate a vendor you typically use to gain access to your building or computer systems.

Outsmart the Hackers

Scammers can be very sneaky, which makes it difficult to spot their tricks. Managing passwords and using two-factor authentication are just two ways you can outsmart their treachery.

Manage Your Passwords

Passwords help protect systems and data from unwanted access, but they can create a false sense of security. With so many separate accounts that require passwords, it's common for people to use the same password across multiple systems and accounts.

When companies experience a cyber breach, it can expose your username and password.

If you use the same password everywhere, hackers will use software to automatically search other accounts and attempt to break in with the stolen password, which is called **password stuffing**. They can even get into your email account and send emails on your behalf, essentially using ministry email to attack other businesses or people.

Page 2 Quiz Answer: Trick question! It's all of the above (spearphishing, smishing, phishing, and spoofing).

"Hackers are constantly trying to steal your passwords. If they steal one, and you use it everywhere, they now have access to all the accounts that use the same password," said Chris Harvey, chief information security officer with Brotherhood Mutual.

A simple remedy is to use a password manager. It comes as software and an app so you can use it across your computers and mobile devices. Password managers allow you to place all your accounts in a single, encrypted and password-protected vault. Once you link your accounts, the software creates new, unique passwords for each. You'll only need to remember the single master password.

Cohee advises, "With passwords, the length is really the difference. Make sure it's complex, and it could even be a sentence, which is even more secure."

Two-Factor Authentication

Two-factor authentication takes security to a new level. It requires users to have a password and an *additional* method of verification, such as a pin number, texted to a smartphone, before they can gain access to an account. This is a very effective way of securing your accounts.

"If an account offers two-factor authentication, use it," encouraged Harvey.

This type of security places an additional step to gain access to accounts. This means that even if your password is stolen, hackers won't be able to access your account because they won't have access to the pin on your smartphone.

Think Before You Click

Whenever you receive an email, text message, or phone call that requests immediate action, especially a transfer of funds, take a minute to run through the following questions:

✓ Were you expecting it?

✓ Is it a known problem that you need to address?

✓ Did you receive an email when a phone call or in-person conversation would have been more appropriate?

To add an additional layer of protection, check any hyperlink before clicking it by hovering your cursor over the link. "If it looks strange or contains misspellings, simply avoid clicking," cautioned Cohee. "And if you get a text message asking you to call a phone number for a business, such as a bank, always do an online search and call the listed number so you know it's legitimate."

Secure Systems and Data

1. Avoid using personal accounts for ministry activities.
2. Avoid emailing sensitive data and make sure it is only accessible to those who need it.
3. Make sure you can access password protected data if someone leaves the church or vacates a position. Change passwords to secure the account.
4. Keep the software on your smartphones and computers up to date so you have the latest security patches.

Cybersecurity Coverage

While theft through email phishing scams may be covered under your ministry's theft coverage, losses from many types of cyber threats are not. Should a breach occur, your ministry could have costs associated with required notifications, credit monitoring services, and data retrieval for litigation.

Brotherhood Mutual offers multiple coverage options for cyber liability, as well as a partnership with a global leader in cyber response and remediation services. If a breach exposes personally identifiable information, remediation services help fulfill legal requirements to report the hack to those potentially affected. Kevin Rainear, senior claims adjuster, Brotherhood Mutual, advises to alert your insurance agent first if you have a cyber incident. *"If there's concern personal information stored on your systems has been compromised, the breach response services provided with Brotherhood Mutual's cyber liability coverage may help your ministry investigate the breach and determine if there is a legal obligation to report to those who may be impacted," said Rainear.*

MAJOR DAMAGE in *less* than a SECOND

A power surge reveals a church's hidden truth

A typical late-summer storm in Pennsylvania rolled over the Riverside Community Church campus on an otherwise quiet Sunday afternoon. Earlier, a minimal crew streamed Sunday services and went home. Now, the church was empty.

Don Greb wasn't in the area to witness the pop-up thunderstorm. When Greb, Riverside's business administrator, received an alert on his phone that a network switch had failed, he wasn't overly concerned. Switches had gone down in the past, and usually were down for a few minutes or so. The system would reset itself.

By late in the morning the following Monday, the extent of the storm damage was just beginning to unfold. Along with the network switch, employees reported that the sanctuary lights weren't working. A copier was down. "I wasn't sure what was going on," said Greb. "That's when neighbors told us about the storm the previous day. We started to suspect a lightning strike caused a power surge."

A power surge can occur in several ways:

- **Sudden voltage spikes.** A direct or indirect lightning strike can destroy electronics and wiring in a flash.
- **Fluctuations in voltage.** These can occur during utility company maintenance or nearby construction. High-power devices, like a commercial refrigerator, can also trigger a fluctuation when powering up or down. Over time, those voltage pulses can damage electronics.
- **Blackouts and brownouts.** Whether a large-scale interruption in power or a reduction of service, both can create a crippling surge once the power is restored.

Severe weather is the single leading cause of power outages in the U.S.

Billion-dollar disaster events 1980–2020: 18 Wildfires, 28 Droughts, 52 Tropical Storms, 128 Severe Storms, 33 Flooding Events, 17 Winter Storms, and 9 Significant Freezes[1]

[1] "Billion-Dollar Weather and Climate Disasters: Events." National Oceanic and Atmospheric Administration, National Centers for Environmental Information. Accessed 10 March 2021. https://www.ncdc.noaa.gov/billions/events.

Page 2 Quiz Answer: Uninterrupted power supply

A Hidden Truth

Riverside's main building spans 15,000 square feet. Greb enlisted employees, volunteers, and electricians to help discover the breadth of the damage. The process involved several days as the team looked at the entire electrical system, including lights, breaker panels, and outlets. But they weren't prepared for one shocking detail: of the six electrical panels, only two were equipped with surge protectors. "Some of our panels were less than five years old," said Greb. "That we didn't have them protected from a surge came as a surprise to everyone."

Stop the Surge

Protecting electrical panels and network switches from a power surge is, in effect, protecting your ability to communicate and operate. Electrical panels are first to receive the main power feed as it passes into a building. Other utilities, like an internet provider, pass their service through a network switch that can then be connected to other electronics like audio-visual-lighting (AVL) equipment.

Generally, protection comes in two forms: a surge protector that's mounted to a main electrical panel and an uninterrupted power supply (UPS).

Blame the weather.

Large-scale power outages related to weather have increased significantly. 679 outages, each affecting at least 50,000 customers, occurred in the U.S. between 2003–2012.[2]

A surge protector works like an interrupter. It diverts sudden power surges to a grounding wire before the surge can reach and damage critical equipment. However, a sudden shutdown can still damage sensitive computer equipment.

A better option is to install UPS units on all network switches, along with a main panel surge protector. UPS units protect network switches — they signal your computer systems to power down orderly and safely after an outage. When accompanied with a generator, the UPS unit can keep your systems running until the generator kicks in, often several minutes later, or until you can manually power down affected equipment. A UPS unit also continually protects your systems from those smaller, damaging fluctuations in power.

Don't Assume. Find Out.

With little protection, the lightning strike dealt a heavy blow to Riverside and took several months to resolve the issues. "We had to replace two of our electrical panels, a network switch, and a wiring board on the printer," said Greb. "We also had to replace every light in our sanctuary. Some wouldn't come on. Some wouldn't shut off." Workers then installed surge protectors on the remaining four panels.

Greb has a tip for churches and religious organizations: Hire a licensed electrician to audit your systems. Ideally, a surge protector or UPS should be installed on all electrical panels and network switches and tailored to your systems' needs. "The first thing you should check on is your high-end equipment. Don't assume just because you've recently remodeled or installed new AVL equipment that you're protected."

Look for the Coverage Gap

Are you covered for direct physical damage to covered property or equipment caused by failure or resulting/related losses? If not, ask your agent about Systems/Equipment Breakdown Coverage.[+]

- ◯ Damage to boilers, HVAC
- ◯ Electrical surge/disturbance
- ◯ Communications & computer systems
- ◯ Spoilage
- ◯ Fungus, mold, dry/wet rot
- ◯ Lost business income/extra expense
- ◯ Water damage
- ◯ Hazardous material cleanup

[+] All coverages are subject to their terms, conditions, coverage limits, limitations, and exclusions. For precise detail of coverage, please refer to actual policy forms.

[2] "Economic Benefits of Increasing Electric Grid Resilience to Weather Outages." President's Council of Economic Advisers, U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability, White House Office of Science and Technology, August 2013. https://www.energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

PRACTICE TURNS CHAOS TO *calm*

Benefits of Scenario Based Training

"The body won't go where the mind has not already been." We've heard a lot of security professionals say something very similar to this statement when they talk about how important it is to not only train, but to practice different scenarios that could happen at your church or school. While training for a high impact situation like an armed intruder is key, safety and security teams also should practice scenarios such as a medical emergency, disruptive individual, severe weather, and lost child.

"This helps pressure test your policies and practices to improve your team's effectiveness," said Eli Hernandez, pastor and head of safety for Bridgeway Community Church in Maryland. "When we train at our church, it's designed to keep our volunteers engaged and to think through how we can better serve our people."

Setting up scenarios in the environment where the event is likely to occur helps volunteers see the opportunities and challenges in that space. For example, practice disruptions in the sanctuary, kid-based scenarios in the children's ministry area, or medical emergencies in gathering spaces.

"Training is the learning ground, it's where you can make mistakes and explore ways to improve," said Craig Cable, a church safety specialist and professional trainer who works for American Church Group of Colorado.

Whether it's a couple arguing in the parking lot, disruptive individual during service, or custody dispute in the children's wing, emotionally charged situations can quickly escalate. If volunteers aren't trained to deal with the added stress, their own emotions can take over, leading to poor decisions and the potential for injury or liability for your ministry.

Training also is an opportunity to see how team members will react during stressful situations. This enables the team to practice appropriate responses to verbal challenges and allows participants to adjust their approach to help calm the situation. It also helps volunteers see the ministry opportunity in helping people through stressful or emotional situations. "We want our volunteers to see the person, not just the problem," said Pastor Hernandez.

"Using your words to help find common ground, and getting people to comply with the ask, can resolve issues peacefully, and that's what we call the WIN," said Cable. WIN stands for What's Important Now, and it's a helpful reminder to maintain proper perspective. For most situations, Cable advises, "You need team members who can pull back on the things they want to say and focus on the things they need to say."

To help security team volunteers learn how to safely de-escalate potentially threatening situations, they need to first learn how to control their natural reactions. Realistic training scenarios introduce stress in a controlled environment, helping your team prepare to handle chaotic

Page 2 Quiz Answer: stress inoculation

scenes with composure and calm. Using this de-escalation strategy can equip your volunteers to approach scenes with a heart for ministry and a clear goal of protecting your people.

Stress Inoculation

Without proper preparation, even small disagreements can turn into full-blown shouting matches. What starts as a request to leave the building can end in a physical altercation. Even mild-mannered volunteers can unintentionally escalate a situation if they lack the training to keep their emotions in check.

To help successfully resolve situations, security team members need to be inoculated from the stress. Using realistic training scenarios can help volunteers become more accustomed to controlling their emotions. As a result, they can think more clearly and stay focused on safely resolving the confrontation. This helps protect the volunteer, the ministry, and the individual causing the disruption.

Adding to Your Team

If you need to replenish your security team volunteers, consider adding the following interview questions to your onboarding process:

- ✓ Tell me about a time when you were under a lot of stress. How did you manage the stress?
- ✓ Tell me about a time when someone was really upset with you. How did you work through that situation?
- ✓ Have you ever had a disagreement with someone at work? How did you resolve the issue?

TRAINING SCENARIOS

The following scenarios test "tactical communication," which is how your team uses words strategically to get individuals to willingly comply with a request. While this is a good place to start, get creative, adding variables and new scenarios as your team becomes more proficient.

1 SANCTUARY

During regular church service, an individual draws the attention of your security team. He's not disruptive, but he is acting abnormally. He's wearing sunglasses, a ball cap, and long coat. He's mumbling to himself.

What's your plan for monitoring him? What's your plan if he walks toward the stage or retrieves something from his vehicle? How will you engage him in conversation?

2 YOUTH ROOM

A father thinks his daughter's boyfriend is a bad influence and asks that she not see the teen anymore. The teen shows up to a Sunday service and is stopped by the father in the lobby. An argument breaks out.

How will your team navigate this potentially volatile situation? Who is the aggressor? What is your goal for this situation (What's Important Now)?

3 LOST CHILD

Following worship, a mom attempts to pick up her daughter from the nursery. The volunteer is unable to find the child. The mom immediately becomes frantic. The dad learns of the situation and becomes outraged.

How do you get productive info from the upset parents? How will your team locate the child? How will you coordinate bystanders that want to help?

WHEN DOMESTIC VIOLENCE LEADS TO CHURCH VIOLENCE

Many ministries go to great lengths to protect their people from physical harm. One specific area that demands renewed focus is the potential for harm as a result of domestic violence that spills over into the church. While many churches seek to help domestic abuse victims emotionally through ministry programs, it's important to also consider the physical safety of victims and the broader church body during ministry activities.

The Startling Reality of Domestic Violence

Domestic violence takes many forms, but physical violence is among the most common. According to the CDC, physical violence affects 1 in 5 women and results in more than 1,500 deaths annually in the U.S. What's more, violence in the home can result in violence at church. One of the deadliest examples is the Sutherland Springs tragedy, where the suspect's second wife and mother-in-law attended.

Domestic violence affects about 1 in 3 women in the U.S., making it possible that someone in your congregation is experiencing or has experienced domestic violence. While caring for abuse victims emotionally may be a ministry priority, it's also important to protect their physical safety and the safety of your congregation. This is one area especially suited for a safety and security team.

Domestic violence incidents in the U.S. increased 8.1% during 2020.

National Commission on COVID-19 and Criminal Justice

The Role of Your Safety and Security Team

Ministries can help protect their people by sharing critical information with leaders and members of the safety and security team. It's especially important for your team to know of any current domestic violence situations. This helps your team protect victims and potentially their children by enabling them to recognize perpetrators, especially those who may have temporary or permanent loss of custody. It is beneficial to obtain the victim's permission before sharing sensitive information regarding a domestic situation with individuals who need to know, such as ministry leaders and security team members.

Current or former partners accounted for nearly 33% of women killed in U.S. workplaces.

National Domestic Violence Hotline

Additionally, if your church has a ministry for victims of abuse, closely coordinating with your safety and security team can enable them to be onsite to provide security during any mid-week classes or counseling sessions. Having people present who are trained in de-escalation techniques can help minimize the potential for violence.

Addressing Domestic Abuse and Violence

If your ministry doesn't currently offer any support for domestic abuse victims, there are many organizations that specialize in domestic violence training for staff and offer support for victims. One ministry helping abuse victims is Focus Ministries. They offer support for victims and training opportunities for pastors and staff. Learn more at www.focusministries1.org. Connecting victims with specialized advocates can help protect them from further harm.

More than 70% of U.S. workplaces don't have a formal program or policy to address workplace violence.

National Domestic Violence Hotline

Page 2 Quiz Answer: True

National Domestic Violence Hotline. https://www.thehotline.org/stakeholders/domestic-violence-statistics.

EVEN MORE ARTICLES ONLINE

brotherhoodmutual.com/db/hiddendangers

We couldn't fit everything in this one issue, so visit The Deacon's Bench Online for even more articles and resources about finding hidden dangers in your ministry. We've highlighted a few topics below.

HANDYMAN MINISTRY — If your organization is looking to jump start a handyman ministry, rev up an existing one, or just take on a few service projects, consider these eight tips to avoid trouble.

CYBERSECURITY RESOURCES — Cyber criminals are constantly on the lookout for easy targets. Defend your ministry's data and computer systems against hacking and theft by implementing several key cybersecurity strategies.

POWER SURGE — Power surges can damage more than just sensitive electronic equipment. Take steps to protect your building, and systems, from damaging electrical surges.

SAFETY AND SECURITY RESOURCES — Whether you're ready to develop a safety and security team, or you're looking to take your existing team to the next level, we've provided several helpful checklists, articles, and a webinar to get you started.

DOMESTIC VIOLENCE — Domestic violence often hides in the shadows, but it doesn't stay confined to the home. Abusers frequently follow their victims through social media, website search history, or even GPS tracking. When abuse victims seek help from ministry, their abusers often know their location. Learn about important steps your ministry can take to help protect its people and safely minister to victims.

BROTHERHOOD MUTUAL®

6400 Brotherhood Way
Fort Wayne, IN 46825

Ministry Routing List

- ☐ Pastor
- ☐ Administrators
- ☐ Office Staff
- ☐ Board Members
- ☐ Other

Reveal Hidden Dangers in Your Ministry.

Cyber threats and power surges are just two of the hidden dangers we've revealed. In this issue of The Deacon's Bench, you'll learn about these threats, and more. Plus, discover how to protect your people, outsmart cyber scammers, and defend your property against electrifying damage.

The Deacon's Bench is a magazine created for churches and related ministries.

Volume 1, 2021
Published by the Marketing Communications Department of Brotherhood Mutual Insurance Company.

Insuring America's churches and related ministries®

800.333.3735
brotherhoodmutual.com

Find us on social media: