SPECIAL REPORT:

HOW TO PROTECT YOUR CHURCH OR MINISTRY AGAINST CYBERATTACKS

By Leonard Kelley, GuideStone
Senior Manager of Information Security

WHY WE CARE

At GuideStone Property and Casualty, **our goal is to serve evangelical churches and ministries** like yours by providing trusted ministry protection and risk management solutions to guide you.

We want to empower you to be proactive in protecting your ministry and those you serve from any unforeseen risk management issues. But the reality is that accidents do happen. Injustice takes place. And disasters may strike.

In this document, we are focusing on **how to recognize, prevent and respond to cyberattacks** — an increasingly important topic that must be a priority for you as you grow your church or ministry's online presence through online services, virtual children's programming, and online networks for staff to work from home, as well as any public Wi-Fi offered in your building.

GuideStone® believes when the body of Christ is healthy, it's free to transform the world — and we want to help guide and equip your ministry and its people to do just that. **We designed these cybersecurity resources to empower your ministry and people to stay protected.**

Churches and ministry organizations like yours face a growing and overwhelming number of risks. With GuideStone on your side, your organization can manage risks while focusing on spreading the good news.

TABLE OF CONTENTS

These days, having an online network helps churches and ministries stay connected and keeps all systems running. But with increased online connectivity comes additional security risk. This risk can involve the personal information of staff and church members, ministry financial accounts and even networked security systems for physical church buildings.

As churches and ministries increasingly move online for ministry and worship services, financial giving and general communications, it's imperative that your organization be protected from cyber threats. We want to help your ministry not only stay safe in the physical space but also stay safe online.

ARE YOU AT RISK?

It seems as though we cannot go a single week without hearing about a new cyberattack or ransomware campaign affecting the information of millions. Yet, in all the news surrounding cybersecurity, we rarely hear about churches and other nonprofits being impacted by this global threat — which can understandably lead to a false sense of security for the leaders of these organizations.

Ministries and other nonprofit organizations account for almost 43% of all cyberattacks in the United States and Canada.[i]

This is of growing concern for ministries, especially considering how seemingly unprepared many organizations are right now for defending against cyberattacks.

In fact, NTEN's *State of Nonprofit Cybersecurity Report 2018* revealed 68.2% of respondents did not have documented policies and procedures in place in the event of an attack, and 59.2% indicated they do not provide any cybersecurity training to staff at all.[ii] With the exponential increase in cyberattacks across all sectors and with the lack of cybersecurity education and resources at many ministries, your ministry is likely to experience a data breach unless preventive measures are in place.

You may be thinking, "My church doesn't have the staff to run such an effort against this enormous threat." Regardless of your church's size, GuideStone wants to help you prepare for and respond to this risk by helping you:

- Gain insight into current cybersecurity threats
- Understand the impact of those threats
- Proactively protect your ministry in the digital age

As mentioned before, GuideStone believes when the body of Christ is healthy, it's free to transform the world — and we want to help guide and equip your ministry and its people to do just that. A big way we can help with that now is to provide cybersecurity resources and education.

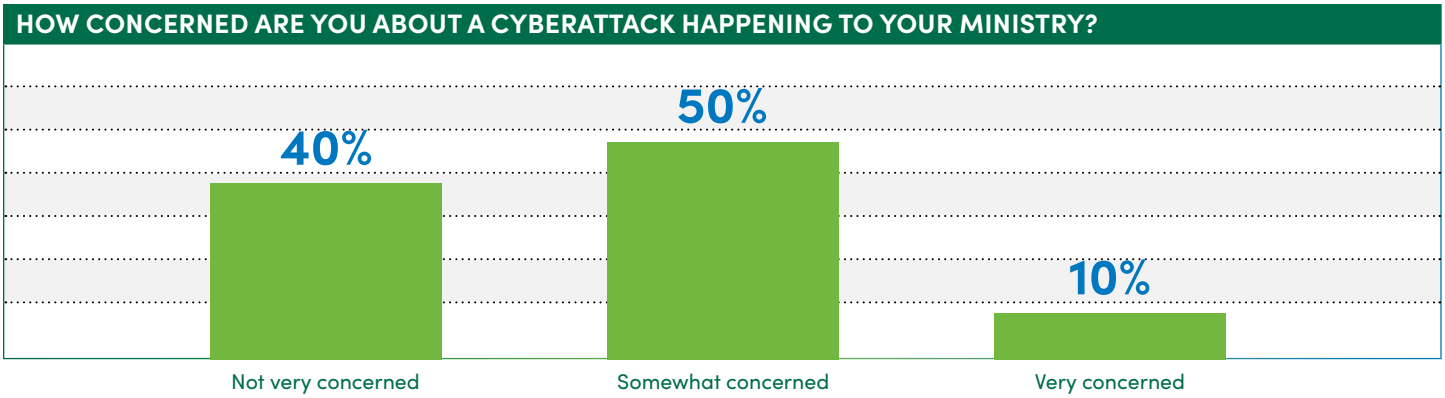
---

[i] Modern Security for Non-Profits - FSi Strategies: Washington DC: Herndon VA https://www.fsistrategies.com/modern-security-for-non-profits/.

[ii] Morgan, Steve. "Cybercrime Damages $6 Trillion by 2021." Cybercrime Magazine, Cybersecurity Ventures, 10 Dec. 2018, www.cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

UNDERSTANDING THE THREAT

The key to protecting your organization from cybercriminals is to first understand and acknowledge the threat, often referred to as the "threat landscape". The threat of cyberattacks is real and not just for lucrative businesses. Roughly 40% of churches[iii] mistakenly believe that they are too small to be a target for cybercriminals and cyberattacks or that they do not have the type of data a hacker would be interested in stealing.



Cybercriminals target common technical weaknesses and known vulnerabilities, as this enables them to cast the widest net possible. It's important to remember that cybercriminals see your organization as nothing more than an IP address. So it doesn't matter if you're the biggest ministry in the country or the smallest church in town — the hacker is simply looking for vulnerabilities. These vulnerabilities can come in the form of everything from a misconfigured router, a weak firewall or smart lightbulbs to capitalizing on the good nature of potential victims. Additionally, cybersecurity issues are not limited to only monetary or theft concerns but extend to intellectual property, violation of privacy and the exploitation of nonprofits such as your online ministry. The fact is, where there's money or information to be gained, cybercriminals will attempt to take advantage of those opportunities.

CHURCH SIZE DOES NOT MATTER

As previously stated, an estimated 40% of churches mistakenly believe that they are too small to be a target for cybercriminals and cyberattacks or that they do not have the type of data a hacker would be interested in stealing. Unfortunately, as the above examples highlight, ALL churches and ministries are at risk. Most cyberattacks are random, with cybercriminals simply searching for vulnerabilities across internet-connected devices. Additional factors that make churches vulnerable to a cyberattack include easy access to:

- **Highly desirable data**
  This includes usernames, passwords and personally identifiable information (PII) such as names, addresses, dates and places of birth, and Social Security numbers (SSNs).
- **A diverse group of network users**
  This includes staff, volunteers, members and visitors with their own devices.
- **Online financial transactions** for tithes and donations
- **Online bank accounts**
- **Electronic connections** to vendors and other organizations
- **A network or resources** to influence others for socially or politically motivated purposes — otherwise known as hacktivism

78% of churches accept donations, tithes and/or payments online.

Depending on the type of cyberattack, your ministry could lose data, be locked out of your network or have the personal information of employees and ministry members compromised. This can result in not only significant financial loss but also reputational damage that can be difficult to restore.

[iii] August 2020 Cybersecurity in Ministries Survey.
https://guidestone.ca1.qualtrics.com/results/publicZ3VpZGVzdG9uZS1VUI9IRDZOSGxPWmd4UzdZeXctNWUzMjAwM2JiMTA5M2EwMDBmZmFhZjBl#/pages/Page_a8b091d9-1644-482a-aa83-705ad304a656

MINISTRY THREAT LANDSCAPE

The following examples are ways churches and other ministries have been victims of cybercriminal activity in the real world:

- An Ohio ministry was **scammed out of $1.75 million** in a business email compromise (BEC) attack while the ministry's facilities were undergoing a $4 million renovation. Hackers gained access to two employee email accounts and used the accounts to convince other employees to wire funds to a fraudulent bank account.[iv]
- A church in Iowa had **seven years' worth of files encrypted** in a ransomware attack after an employee clicked on an email titled "job application – please see attached CV." Churches in Bristol, England, were victims of a similar attack.[v]
- **A church's online giving system was hacked, and someone gained access to their usernames and passwords.** The first day, $17,000 was taken. Each day after, approximately $3,000 more was stolen, until the thefts were discovered by the ministry. The grand total stolen was $181,709.
- A hacker was able to gain access to and place malicious computer code on a church's shopping site. This **allowed the hacker access to any new credit card information entered in the system.** The church had to spend $15,000 to research the damage. In addition, it was required, by law, to offer its 1,800 customers professional ID protection.
- A church bookkeeper received a message on her screen that she had been the victim of a computer breach. As a result, she was locked out of the system. The message prompted her to call an unknown phone number to restore access to the computer. She **allowed access to the hackers and immediately saw SSNs show up on the screen.** At that point, she knew something was wrong. Experts were hired to monitor credit for those affected.
- A church received a notice that its records were frozen and held for ransom. The church did not pay the ransom, **lost access to the records (which were not physically backed up)** and was forced to rebuild all its records from scratch.
- A church had its website hijacked by ISIS/ISIL. The terror group **posted graphic images and videos of shootings and beheadings.**

These examples are just a glimpse into the threats facing ministries and churches. In fact, over 20% of churches have experienced a successful cyberattack.[vi] Furthermore, that number may be higher considering many churches may not even be aware they have been compromised.

Though daunting, this information also provides us with valuable understanding and insight into the methods most used by cybercriminals to infiltrate ministries and cause harm.

In most attacks, the initial method of intrusion is social engineering and phishing. Organizations can use this knowledge as they build out their cybersecurity and security awareness programs.

[iv] O'Donnell, Lindsey. "Threat Intelligence Highlights: Cyber Attacks Target Individuals as Well as Business, Education, and Religious Organizations." Threatpost, 30 Apr. 2019, *www.threatpost.com/bec-hack-cons-catholic-church/144212/*.

[v] Smith, Jonathan. "Phishing Attacks Keep on Coming: Are You Safe?" ChurchLeaders, 4 June 2020, *churchleaders.com/ministry-tech-leaders/376834-phishing.html*.

[vi] August 2020 Cybersecurity in Ministries Survey. *https://guidestone.ca1.qualtrics.com/results/publicZ3VpZGVzdG9uZS1VUI9IRDZOSGxPWmd4UzdZeXctNWUzMjAwM2JiMTA5M2EwMDBmZmFhZjBl#/pages/Page_a8b091d9-1644-482a-aa83-705ad304a656*

CYBERSECURITY IMPACT ON INTERNATIONAL MISSIONARY WORK

The rapid expansion of technology has enhanced and strengthened the work of missionary and outreach programs within the church. However, this has not come without its fair share of cybersecurity concerns. **Many mission leaders are unaware of the full implications of the rapid and pervasive adoption of so many electronic devices and online services,** often utilized by users with little understanding of the underlying technologies.

Additionally, according to a cybersecurity report by Media Impact International,[vii] **over 50% of missionary ministries polled** stated not only financial loss but also missionaries experiencing arrest or harassment, prison, expulsion and worse due to cybersecurity breaches. Much of the guidance within this document can be easily scaled to mission work with a great first step toward cyber resiliency being an adherence to the cybersecurity best practices outlined in the appendix.

Another thing for missionary programs to consider is the **differing cybersecurity and data privacy laws that may exist in the host nation** in which missionary work is being conducted. This information is available from the U.S. Department of State, as well as in additional resources at the end of this publication.

[vii] "Cyber Security Report" Media Impact International, 14 February 2017. *https://www.mii.global/cyber-security-report-download*

HOW SHOULD CHURCHES AND MINISTRIES RESPOND TO THE THREAT?

STEP 1 CREATE A CULTURE OF SECURITY

It is important for all employees and volunteers with access to your network to understand the importance of cybersecurity. Most of the attention and security budgets are paid to devices and virus protection, when in fact the greatest protections against hackers and cybercriminals are the employees, volunteers and members using those devices.

Almost 90% of cyberattacks are caused by human error or behavior,[viii] yet few ministries base security measures around employee best practices.

Additionally, over 85% of churches allow use of personal devices to access ministry emails and the network.

We recommend that you provide frequent training on trending cybersecurity threats as well as smart, preventive measures. Some best practices include frequent training and communication on topics such as:

- The latest cybersecurity threats
- The importance of using, and regularly changing, complex passwords
- How to identify and report phishing emails
- The dangers of visiting malicious websites
- The risks of using public Wi-Fi networks

RECOMMENDED CYBERSECURITY VENDORS AND PARTNERS

- **LARGE CHURCHES & MINISTRIES**
  - **Security Awareness Training:** KnowB4

- **SMALL CHURCHES & MINISTRIES**
  - **Security Awareness Training:**
    - National Initiative for Cybersecurity Education (NICE), Employee Awareness Training
    - National Cybersecurity Alliance, CyberSecure My Business

Appoint a cybersecurity champion within your church or ministry who is responsible and accountable for ensuring the security of the ministry's systems and data. Depending on the size of your ministry, this person would ideally be someone who has the authority to allocate appropriate resources to the protection of information security systems.

We encourage you to not only look to staff but also toward your volunteers or congregation for qualified and motivated individuals who can help formulate a plan for moving forward, individually or also in the form of a committee.

[viii] Spadafora, Anthony. "90 Percent of Data Breaches Are Caused by Human Error." TechRadar, TechRadar Pro, 8 May 2019, *www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error*.

STEP 2 FORMULATE A PROTECTION PLAN

You cannot develop a plan of protection until you first know what exactly you have that needs protecting. The first step your committee or cybersecurity champion should take is making a full systems inventory of all devices and software your ministry has active. Consider the following:

- Identify the systems in your inventory including:
  - Phone systems
  - Physical security systems
  - Online directories
  - Donation portals
  - Mobile apps
- Identify current system users.
- Identify and implement procedures governing the use of these systems, ensuring only those who need the data have access.

Once you have identified and documented your systems, your committee and/or champions can begin to develop a prevention and incident response plan that details what steps staff need to take to prevent an attack and how to respond in the event of an attack. Use these steps to get started:

- **TO PREVENT A CYBERATTACK**
  - Set up antivirus protection, password rules, etc. for your working environment. In the next section, we will outline more specific recommendations for this step.
  - Become familiar with your cybersecurity insurance policy or invest in such a coverage if you don't currently have one.
    - Feel free to reach out to GuideStone to learn more about how to protect your ministry with cybersecurity insurance.
  - Identify reputable vendors that could help your security efforts. You will also find a list of free resources at *Risk Management Review Resources*.
    - If you have Extended Broad Scope Liability Coverage from GuideStone through Brotherhood Mutual Insurance Company, it includes a CyberScout® subscription service for ongoing security support.
  - Task your committee or cybersecurity champion with staying aware of what your state/province and federal laws are in relation to cybersecurity.

- **IN A RESPONSE TO A CYBERATTACK**
  - Create step-by-step, documented instructions for dealing with potential situations such as a data breach or a compromised system. Begin with these questions to help you outline a procedure:
    - Do people know whom to inform of a breach or a suspected breach?
    - Who will be responsible for dealing with the vendor(s), authorities and members if/when you have a data breach?
    - Have you contacted your insurance company to file a claim?

STEP 3 STRENGTHEN EXISTING PRACTICES

Good news! You have probably already taken some steps toward cybersafety without even knowing it. We've compiled some quick tips on how to leverage the security you may already have in place.

Within the settings of the computer systems you already use:

- Set up all devices (laptops, desktops, tablets and phones) to require login with a password.
- Schedule regular password changes and add password complexity requirements.
- Do not allow users to share their access credentials. (This may cost more in licenses on the front end, but that is a small price to pay compared to the cost of a single breach.)
- Disable/Deactivate all user accounts that are not actively being used.
- Upload and set antivirus and anti-malware scans to run on a regular basis.

If you want to get even more detailed in your security measures — especially for larger churches — we recommend these additional steps:

- Require long and complex passwords and require password changes on a regular basis.
- Enable two factor or multi-factor authentication and encryption where available.
- Apply all security patches recommended by any external vendors (for operating systems or for software programs or hardware).

60% of breaches involved vulnerabilities for which a patch was available but not applied.[ix]

FINAL THOUGHTS

Cyber threats are evolving every day, and defending against those threats is becoming more important than ever, especially considering what's at risk. Every ministry, no matter how big or small, is a target. Therefore, it's crucial that ministries ensure they're doing everything they can to increase their ability to stay protected against these threats. A church's cybersecurity is like a castle wall — the more layers of security, the better.

The information and best practices outlined in this publication will help you implement multiple security controls in a layered fashion, so that when one fails, others exist as a failsafe to protect your ministry. GuideStone would like to help you fortify your defense by providing cybersecurity insurance protection.

[ix] *https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html*

NEXT STEPS

You're managing your church's future. GuideStone can help you manage the risks and help you ask the right questions ahead of time.

- **What would you do if your church was hit with a lawsuit for religious freedom or a serious injury?**
- **What would you do if fire or theft destroyed valuable church property or even part of the church itself?**

If your church insurance company hasn't addressed these questions, you need help before something happens.

At GuideStone Property and Casualty, we offer unique cybersecurity coverage through our strategic alliance with Brotherhood Mutual®.

GuideStone understands the risks churches face, and our desire is to help you be proactive in protecting your ministry and those you serve. We'll help you understand church insurance, show you how to anticipate areas of risk, and then help you mitigate that risk with a proven risk management program tailored for your church.

For more information, visit *GuideStonePropertyCasualty.org*. You may also call us at (214) 760-2868 or email us at *InsuranceSolutions@GuideStone.org*.

ABOUT GUIDESTONE

At GuideStone, our mission is serving you. We are committed to equipping churches, universities, hospitals, mission-sending organizations and other ministries, as well as ministry-minded individuals, with products and services that promote financial, health and spiritual wellness — all while honoring the Lord.

Since our beginning in 1918, we have existed to *serve those who serve the Lord with the integrity of our hearts and skillfulness of our hands* (Psalm 78:72). This means we are driven by more than just the bottom line. GuideStone is committed to Do well. Do right. Do MORE.™

So, how can we help you do more?
Visit us at *GuideStone.org*.

ADDENDUM A: A STEP FURTHER: EMAIL AND VIRTUAL SECURITY

PHISHING, SMISHING, VISHING . . . OH MY!

Phishing, in all its various forms, is one of the most frustrating threats any organization faces because, though it's well known how it works, it nonetheless proves to be the most effective way for cybercriminals to infiltrate an organization. In a typical phishing scenario, a cybercriminal sends a message that masquerades as originating from a trusted entity such as an organization, leadership within your church, your bank, etc. That message directs the recipient, via a link, to a falsified website that captures the recipient's personal information or contains a malicious attachment that will infect the recipient's computer, device and network.

As we identified earlier, the motives of each cybercriminal vary; however, one thing remains consistent — cybercriminals want information. Once the cybercriminals acquire the stolen information, other motives such as financial gain, reputation impact, political statement, etc. materialize as they take next steps in their crime.

The statistics surrounding phishing are staggering, with well over 300 million phishing emails sent globally every single day. **Of those, almost 20 million make it through security and spam filters, 10 million are opened, 900,000 links are clicked and almost 90,000 people fall for a scam every day, unknowingly sharing their personal information with cybercriminals.**[x]

Email phishing isn't the only social engineering method used by cybercriminals, however. As smartphone use has grown, so have the methods used by criminals to extract private data. "Vishing" and "smishing" scams are variations of phishing that use voicemails and SMS messages instead of email.

These are the four most common types of phishing attacks:

EMAIL PHISHING

Most phishing attacks are initiated by way of email. The cybercriminal will register a fake domain that emulates a trusted organization and then send thousands of generic requests. The fake domain will often involve some sort of character change, such as using an "r" and "n" next to each other to create "rn" rather than "m". Additionally, the cybercriminal may use the trusted organization's name as part of the email address. Phishing emails have become quite difficult to spot as threat actors continue to refine their tactics. Only by practicing a high level of security awareness and checking emails with extra scrutiny can organizations better identify these malicious tactics.

SPEAR PHISHING AND WHALING

These two methods of phishing are more targeted and sophisticated than your typical phishing email.

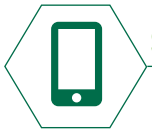
Spear phishing is a method in which a cybercriminal sends a phishing email to a specific person. Typically, the criminal will have already gathered PII on the person, such as:

- Name
- Place of employment

[x] Kumaran, Neil. "Protecting against Cyber Threats during COVID-19 and Beyond | Google Cloud Blog." Google, Google, 16 Apr. 2020, *cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond*.

- Job location and title
- Email address
- Specific details about his or her job role within the organization

Whaling attacks are even more targeted and take aim at senior executives and high-ranking individuals within an organization. The techniques used in a whaling attack differ slightly from spear phishing in that fake links and malicious URLs aren't typically used. Rather, the criminals rely on scams involving fake tax returns/forms, as these contain highly useful information, such as names, addresses, SSNs, bank account information, etc.



SMISHING AND VISHING

Both smishing and vishing involve the use of telephones in the place of traditional computer-based email as the form of communication.

With themes similar to phishing emails, **smishing** involves a criminal sending malicious text messages, typically using malicious links that lead to a fake login page to steal credentials.

Similarly, **vishing** uses telephone conversation and often exploits the voicemail feature. Vishing scams often involve the cybercriminal posing as a fraud investigator from the victim's bank, informing the victim that his or her account has been breached or is showing signs of unusual activity. By sharing this fabricated story, the cybercriminal hopes the victim will provide account and/or payment card details to rectify the situation.

ANGLER PHISHING

With the explosion of social media over the past decade, it's no wonder cybercriminals have begun shifting their malicious tactics to that medium. Social media offers many ways for criminals to trick people into divulging personal information. Fake URLs, tweets, instant messaging, cloned websites and individual posts themselves can all be used to trick people into giving up sensitive information and/or downloading malware.

Furthermore, cybercriminals can use the data that people post willingly on their social media to create highly targeted and advanced social engineering attacks. Ministries should be very cognizant of the information they share on official social media accounts, as well as that of their employees and volunteers. According to Experian, the most often used **angler phishing** tactic is the practice of "masquerading as a customer service account on social media, hoping to reach a disgruntled consumer. With the name of the company or its social media account handle included in the post, scammers are ready to strike. They will then reach out to the victim using an account like [Name of Company] Customer Support Team, hoping the victim doesn't realize it's not a real account."[xi]

Awareness and the ability to recognize suspicious messages, such as those identified above, are paramount to the ability to defend against social engineering threats.

[xi] Velasquez, Eva. "What Is Angler Phishing and How Can You Avoid It?" Experian, 14 June 2018, *www.experian.com/blogs/ask-experian/what-is-angler-phishing-and-how-can-you-avoid-it/*.

ADDENDUM B: CYBERSECURITY BEST PRACTICES

Cybersecurity is everyone's responsibility. Without proper security awareness, individuals put not only themselves but the entire organization at risk. Luckily, there are a few cybersecurity best practices that individuals can follow to better protect themselves and their ministry.

USE STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION

Complex passwords can go a long way toward thwarting a cybercriminal from accessing your information. Consider a strong password that contains at least 10 characters and includes a combination of numbers, symbols, and capital and lowercase letters. Multi-factor authentication should be utilized with any service that offers it, which includes most email providers, financial institutions and even social media platforms.

CAREFULLY CONSIDER SOCIAL MEDIA CONTENT

Be very cautious with the use of social media. It's all too easy to post too much information that can be used by cybercriminals. Even sharing a post and/or pictures of the whole family being away on vacation announces that the house might be empty for days. This extends to your internet browsing habits as well; strongly consider the use of a virtual private network (VPN).

UPDATE SOFTWARE AND ANTIVIRUS

Keep your security software, web browsers and operating systems updated with the latest protections. Antivirus and anti-malware protections are frequently revised to target and respond to new cyber threats.

AVOID PUBLIC WI-FI AND CHARGING STATIONS

Public Wi-Fi can easily be taken over by a threat actor. Once in control, he or she can use it as a hotspot to steal your credentials and other confidential information. Public phone charging stations can also be used by criminals to siphon off your private data.

USE MOBILE DEVICES SAFELY

We rely on our mobile devices now more than ever, making them a prime target for criminals. The following guidelines will ensure you are best protected from these threats:

- Never leave your device unattended in public.
- Lock your device with a PIN and/or password.
- Only install apps from trusted sources (Apple® App Store, Google Play, etc.).
- Keep the operating system up-to-date.
- Utilize encryption if offered.
- Enable loss and anti-theft tools, such as Find my iPhone or Android Device Manager, on your device to help prevent a criminal from being able to utilize your data.

ADDENDUM C: CYBERSECURITY CHECKLIST

Cybersecurity is an increasingly prominent area of concern in churches and ministries today. From storing financial information to securing wireless internet access, please use this checklist to be sure that your ministry is up-to-date with its standards for cybersecurity.[xii]

CYBERSECURITY	YES	NEEDS ATTENTION
Do you perform monthly backups of business and financial information and store it in a secure, off-site location, such as a safe deposit box or a reputable cloud-based storage service?		
Do you have policies in place to protect confidential information like contribution records, counseling notes and other sensitive information?		
Do you have policies in place to report data breaches in accordance with state law and to protect your ministry from legal action?		
Do you encrypt all credit care account information stored on church computers?		
Do you password-protect financial records?		
Do you change computer passwords at least once every six months and share them only on a need-to-know basis?		
Do you work with a qualified computer support company to secure your computer systems?		
Do you update your operating system for security reasons?		
Do you update virus and spyware protection software?		
Have you installed hardware and software firewalls that are designed to prevent unauthorized access to your computer network?		
If you offer wireless internet access to your attendees, have you created a separate, private network for the church's administrative computers?		
Do you protect against objectionable or illegal Wi-Fi use by blocking questionable websites, password-protecting the wireless network and asking users to agree to an Internet Usage Policy?		

[xii] Based on and/or excerpted from materials created and developed by Brotherhood Mutual Insurance Company. Used with permission of Brotherhood Mutual Insurance Company.

GuideStone®