Adventist Risk Management, Inc.

CYBERSECURITY

A typical statement in the technology security industry is, "It's not *if* you will be hacked, but *when*." The reality is that if someone wants to get in, they will find a way. It's just a matter of how difficult you make it for them and if you make yourself a likely target. Once a hacker has your information, they can use it to blackmail you or others, steal identity or money, hold your systems hostage until ransom is paid, or destroy your data or systems.

When it comes to cybersecurity, many of us can feel unsure how to protect our churches, schools and ministries against risks in the digital world. Here are steps you can take to protect your ministry systems and data from cyberrisks.

SECURE YOUR WI-FI

Wi-Fi is often one of the most vulnerable points in digital ministry. Unsecure Wi-Fi networks can be used for criminal activity or to access other devices also on the network, such as company computers. There are several ways you can make your network more secure:

1. Restrict access by not posting or sharing the Wi-Fi password.
2. Have a separate guest network for the congregation and a business network for church computers.
3. Enable device isolation. This prevents users from seeing other users who have connected.
4. Change the Wi-Fi password quarterly to prevent network abuse.

EDUCATE YOUR MEMBERS AND EMPLOYEES

Education is essential to help members understand the importance of protecting the private network and their information. Instruct members to not share the business Wi-Fi or other connectivity information with visitors or anyone not authorized to have access.

USE STRONG PASSWORDS

Use passwords to prevent unauthorized access to your computers, devices, or network and change those passwords every three months. A password should be a minimum of 8–10 characters and include one capital letter, one lowercase letter, one number and one special character.

PROTECT MEMBER INFORMATION

If your church decides to publish its member directory online, incorporate some obstacles to make sure hackers don't access the information. For example, create a member only login to access that information.

Be vigilant and alert to any suspicious activity. If someone calls and asks about church members and an individual's name, take note of who the caller is and why they are seeking information. Think carefully and be cautious of who you share church information with including names, numbers and passwords.

ENCRYPT EMPLOYEE DEVICES

Encrypt any sensitive church information, especially on company mobile devices and laptops. Mobile devices are vulnerable to theft because of portability. Once someone has physical access to devices, it is not difficult to break into them. Drive encryption is something to consider strongly for all mobile devices. Both free and paid applications are available. Carefully evaluate each program to find the best fit for your church.

LINK TO SECURE TITHE-PAYING SITES

To protect electronic tithe transactions, make sure the systems you are using are secure. The link should begin with "https" indicating that it is a secure connection. The North American Division of Seventh-day Adventists provides an online giving website for each church to collect funds. The site is AdventistGiving.org. The IT department at the North American Division oversees the security of this site. Encourage your congregation to refrain from storing credit or debit card information anywhere.

MAINTAIN YOUR FIREWALLS

Firewalls are another way to make hacking your system more difficult. There are three things you must diligently do to maintain your firewall.

1. Protect all passwords.
2. Don't use default settings.
3. Always keep the software and firmware up to date. All too often, these devices are taken through an initial setup and forgotten.

MAINTAIN YOUR SECURITY SYSTEMS

Evaluate your technology security systems regularly as part of your quarterly seasonal maintenance. Two questions to ask:

- Is there any maintenance I should be doing?
- Is my software obsolete (no longer produced or used, or out-of-date)?

Replace or update your equipment before the product vendor ends technical support or the equipment is no longer capable of protecting you against the threats that exist. Threats are always changing, so it's important you are also constantly vigilant.

HAVE THE RIGHT AMOUNT OF PROTECTION

Many cybersecurity software exist to enhance the protection of your systems and make them less vulnerable to attack. The amount of cybersecurity insurance your ministry needs depends on the size of your ministry. Evaluate:

1. the size of your church,
2. the extent, and amount of technology you have and
3. how much information you store on that technology.

That should give you a clearer picture of how much to invest in cybersecurity efforts.

FIND OUT IF YOUR CONFERENCE HAS CYBER LIABILITY INSURANCE

Cyber Liability Insurance can help your ministry recover from a cyberattack and assist your ministry in notifying and assisting any constituents who were also affected by the attack, such as members or employees whose data your ministry stores. If your conference has Cyber Liability Insurance from Adventist Risk Management, Inc., church ministries in your conference have cyber liability coverage. Contact your conference office to find out if you have cyber liability coverage.

REPORT YOUR CLAIM RIGHT AWAY

1.888.951.4276 • CLAIMS@ADVENTISTRISK.ORG

STAY INFORMED

ADVENTISTRISK.ORG/SOLUTIONS