Aardsma Archives

*prepare well. protect well.*

# Protecting Ministry Data and Computers

## IS YOUR CHURCH VULNERABLE?

Churches commonly collect and store members' personal information. Everything from mailing lists and donation records to Social Security numbers and payment card information may be kept in the average church database or filing cabinet. Unsecured, this data could make church members vulnerable to thieves—putting ministries and church members at risk. Carefully protecting data not only makes business sense, but it also can reduce the likelihood of crippling data loss, embarrassing public disclosures, and lawsuits.

### Physical Security

Physical security is a vital aspect of data protection. The *Better Business Bureau* offers these data safety tips for small businesses:

- Shred papers containing personally identifiable information before throwing them away.
- Send and receive business mail from a secured mailbox or post office box.
- Verify a church member's identity before providing any personal or financial information by telephone or email.
- Secure your building with locks and alarms.
- Store business, employee, and membership records in locked cabinets.
- Limit staff and volunteer access to sensitive information.
- Train office workers how to protect the privacy, confidentiality, and security of personal information.

### Computer Security

Data housed on computers is particularly vulnerable to theft—especially when computers are connected to the Internet. One errant click can leave an entire congregation open to identity theft. Because hackers go to great lengths to ensure that you can't easily shake them off, the best medicine is prevention. Here's what you can do:

(Continued page 2)

- **Limit access with passwords.** Use passwords to limit employee and volunteer access to sensitive information. Train office workers to keep passwords private. Be sure to issue new passwords when an employee or volunteer stops working in the office and no longer needs to view ministry records.
- **Keep software up to date.** Windows and Mac computers can be set to automatically apply security updates. Many of the individual programs and apps on your computer can also be set to automatically apply updates. Taking the time to enable the automatic settings now will ensure you don't forget when you are busy later.
- **Install a dependable firewall.** Both hardware and software firewalls are designed to prevent unauthorized access to a network.
- **Secure your wireless network.** If your church uses Wi-Fi for staff members and you would like to offer Wi-Fi Internet access to the congregation or visitors, make sure to set up an additional and separate guest network that only has access to the Internet. Wi-Fi networks should always be password-protected. The password for the guest network can be shared each week via the church bulletin, slides, signs or other method. As with all passwords, they should be changed regularly.
- **Keep up with anti-virus software updates.** Anti-virus software can prevent or reduce the impact of virus infections. Paid anti-virus software generally keeps itself up to date if you pay your subscription fee each year. Check periodically to ensure the license period hasn't expired. Some free anti-virus software is available—check the licensing terms to make sure that the free use includes use in a church or non-profit entity.
- **Fine-tune your browser settings.** Adjust your browser to use a higher security setting. Most browsers can automatically check for security updates and install the newest version.
- **Scan computers weekly for malicious software.** Most virus and spyware protection software can be programmed to do this automatically.
- **Preserve critical data.** Back up business records daily, weekly, or monthly, depending on how often data is edited and your tolerance for risk of losing the data. Store backups in a secure, off-site location, such as a safe deposit box. This protects your ministry from losing records to computer breaches and other events, such as tornadoes, floods, or fires.
- **Know what you're installing.** Ask yourself, "Do I know and trust the source of this software?" Reputable software publishers will either avoid including adware/spyware with their products or clearly tell you how to download the software without the "extras."
- **Protect your website.** It's best to host your ministry website—and online giving platforms—with a trusted vendor that uses industry-standard security measures. Be sure to thoroughly screen the vendor and review any contract before signing it.

(Continued page 3)

## Beware of Scams

Scammers are finding more ways to entice people into giving up personal and organization data. From sending emails pretending to be the pastor or other ministry leader asking for money to be wired immediately to sending emails demanding W-2 files be send via PDF format, scammers are targeting nonprofit organizations. Take steps to protect your ministry:

- **Watch what you click.** Though it can be time-consuming to read pop-up messages, it's important you know what you're doing before you click. Many fraudsters are counting on you to be in the habit of simply clicking on links or selecting “OK” or “Yes” on everything you see. When in doubt, avoid clicking the link. Instead, call the company or visit its website, using contact information you already know to be genuine. Do not enter usernames or passwords if you don’t know why you are being asked for them.
- **Never send personal information through email.** Avoid sending personal information through email. Before submitting financial information on a website, look for the “lock” icon, often located in the browser’s address bar. This icon indicates that your information will be transmitted securely.
- **Monitor financial accounts.** Review credit card and bank accounts online for unauthorized charges. Call your credit card company or bank immediately if you notice unauthorized charges.
- **Hire an expert.** Find an established information technology (IT) support company that has a good reputation, stands behind its work, and comes highly recommended by other clients.
- **Report scams.** Report suspicious activity to the Federal Trade Commission (FTC) via their website, ftc.gov. If you receive spam email that asks you to supply sensitive information, forward it to spam@uce.gov. Visit the FTC's website to learn other ways to avoid email scams and deal with deceptive spam.

## How Do I Know If My Computer Is Affected?

Sometimes, data breaches are caused by software programs known as adware, spyware, or hijackers.

How can you tell if you’ve been affected by these programs? Look for these warning signs:

- **New homepage or search page.** The pages you're used to seeing when your browser first opens or when you search the Web have suddenly changed. Often these new pages pop up several ads and messages about viruses, and then offer a download to fix the problem for just $19.95.

(Continued page 4)

- **New toolbars.** Suddenly your browser software displays new toolbars across the top of the screen that you didn't put there.
- **Unwanted ads.** Advertisements frequently and randomly pop up on your computer, even when you're not surfing the Internet.
- **Browser troubles.** Web browsing programs no longer work properly.
- **Freezes.** Your computer "freezes up" or "crashes" more frequently.
- **Slowdowns.** Overall, your computer performs much more slowly.

## Prepare for the Worst

Even if you've done your due diligence, thieves may find their way into ministry data. Create procedures that describe how to handle a security breach, should one occur, to help limit negative effects. Here are a few ways to prepare:

1. **Seek help in advance.** When you suspect that a breach occurred, it's good to have an experienced, trustworthy IT professional on call to investigate. This professional also can lend advice on how to handle the situation.
2. **Review state laws.** You may be required to notify the individuals who may have had their information stolen. The National Conference of State Legislatures provides a resource listing state security breach notification laws. A local attorney can explain how your state's law applies to your ministry.
3. **Prepare a sample notification letter.** If you have to notify people that their information may have been stolen, having a sample notification letter ready can help meet these requirements quickly. The Federal Trade Commission's Bureau of Consumer Protection offers a helpful resource that gives guidance on how to respond to a data breach and identity theft. It also provides a sample notification letter.
4. **Review your ministry's insurance policy.** This will help you determine if it includes coverage for data theft. Most standard insurance policies do not include cyber liability coverage unless the customer specifically asks for it. Some insurers provide special stand-alone cyber liability policies.

*If your ministry's data is hacked, contact law enforcement immediately. This is especially critical if financial information has been compromised. Notify your insurance agent or insurance company's claims department, as well.*

*The Aardsma Agency is making this material available to you for information only. It is not intended to provide legal or professional advice, and assumes no liability in its use.*