An ***Equipping for...*** resource

CYBERSECURITY
Best Practices for Churches

THE PRESBYTERIAN CHURCH IN CANADA

presbyterian.ca/eq4

You have probably noticed that there is a lot of news about cyber threats and attacks lately. We hear about these attacks affecting banks, hospitals, stores and government systems. But, did you know that congregations are also at risk?

Many congregations mistakenly believe that they are not at risk when, in fact, cyberattacks are a threat to anyone who uses a computer that is connected to the Internet. Organizations and businesses that retain people's personal and sensitive information need to be particularly vigilant against cybercrime.

When you stop to think about it, congregations often hold a great deal of data that is highly vulnerable to cybercrimes, such as Internet and email fraud. Congregations may possess or have access to commonly targeted data, including:

- Personally identifiable information from congregation members and staff (e.g., names, addresses, pictures, phone numbers, email addresses). These records often include information on minors.
- Donation information (e.g., credit card information, bank account numbers, donor profiles and records)
- Financial records (e.g., church banking information)
- Security data (e.g., computer passwords, building security systems)

For more information about preventative measures churches need to take to ensure that financial information is kept secure, please see appendix A of this resource.

Congregations are responsible for maintaining the safety and integrity of the data stored on their computers with the same standard of care and confidentiality applied to paper records. Paper records need to be kept under lock and key and away from prying eyes. The same goes for digital records.

There are a few key things you can do to strengthen your congregation's cybersecurity defenses. This document is by no means an authoritative or comprehensive compendium on cybersecurity, as cyber threats are always changing and therefore require best practices to be updated regularly, but here are some helpful tips to help mitigate the risk.

continued

Spread Awareness

The old saying, "an ounce of prevention is worth a pound of cure" is very true when dealing with the risk of cyberattacks. The first step in prevention should be to make sure that anyone who works with computers or other devices connected to your church's network is aware of the risk. Whether the congregation is small or large, urban or rural, financially stable or struggling, cybercrime is a real threat. Regularly train and provide information on the latest cybersecurity threats, how the threats are likely to present themselves, and what to do when they are identified.

The Session, working with the Board of Managers (or appropriate equivalent), may choose to appoint someone to be a cybersecurity champion for the congregation. The cybersecurity champion's responsibilities will include keeping up to date about new threats, informing all staff and volunteers about the risks, and helping to put necessary preventative measures in place. If there isn't anyone in the congregation who could fulfill this role, consider hiring an IT professional to check the congregation's computer system and train any system users. The costs of doing this training could be shared with another congregation.

What Are the Types of Risk?

Currently, there are three main types of cyber threats that are most likely to affect congregations:

PHISHING SCAMS

- Sending an email to someone falsely claiming to be a legitimate company or organization in an attempt to scam that person is known as "phishing." It is an attempt to persuade people to disclose personal information, like usernames, passwords or credit card information. Often, the emails will contain a link or attachment that, if clicked on, will open the door to hackers to infect your computer with malware.
- These emails take many forms, some of which are not easy to identify as scams because they are designed or created to look like emails from reputable companies or they include personal details that the scammer has somehow found online.
- Some of the more common phishing scams include emails that claim to be from Canada Revenue Agency (CRA) or various banking institutions.
- Another common scam is the prepaid gift cards scam. This is usually an email purporting to come from someone you know, such as your boss or some other person in a position of authority, co-worker, business associate, friend, or family member. It usually starts with something like, "Let me know when you are available," "Can you do me a favour?" or "There is something I need you to do," and asks you to reply. The victim is usually asked to purchase gift cards—most commonly from Google Play, Amazon, Apple iTunes, Home Depot or Walmart—and is then instructed to scratch and send the codes to the fraudster by email.

MALWARE

- Malware is malicious software installed without a user's knowledge, typically when a user clicks on a link in a phishing email or visits an infected website. The malware seeks to invade, damage or disable computer systems or networks. It can also invade other devices that are connected to the Internet (e.g., tablets and mobile devices).
- Malicious software functions by stealing, encrypting, or deleting data, altering or hijacking computer functions, and/or spying on your computer activity without your knowledge or permission.

continued

- It is often used to extract money from the computer user. Sometimes, this happens sneakily in incidents where the malware enables cybercriminals to steal passwords or sensitive information that will allow them to gain access to your financial accounts. Other times, it is not sneaky at all; ransomware will announce itself with a message directly to the computer user that informs them that their data has been stolen and that they must pay a certain amount to get it back.

TECHNICAL VULNERABILITIES

- A software vulnerability is a glitch, flaw or weakness present in the software or operating system. Vulnerabilities in the software that your computer or device is using can allow cybercriminals to access your system.
- These can exist in any software, including reputable software. Many software vulnerabilities are only discovered after the software has been used by lots of people. When a vulnerability is discovered, the software developer will often release a correction in the form of an update. If an update is available and you do not install it, you are leaving a hole in your software that cybercriminals can use to access your system.

What Can Congregations Do to Mitigate the Risk?

Cyber threats are changing regularly so there is no way to ensure that you are 100% protected, but there are several ways to mitigate the risk of cyberattacks.

EMAIL BEST PRACTICES

- Do not open and delete any suspicious emails. If it is claiming to be from someone you know but still seems suspicious, contact the person or organization to ask if they sent it before opening.
- Never give out banking information, passwords or other personal information over email.
- Be suspicious of every link in an email. Don't click on the link in an email unless you were expecting it, even if it is from someone you know. Instead, directly contact the person, company or organization that the email is purporting to come from and ask if they sent you the email.
- Always be wary of emails from financial institutions, Internet service providers and other organizations asking you to provide personal information. If in doubt, call the company directly and ask them to verify the email.

continued

- Don't reply directly to a suspicious email that appears to come from someone you know to verify its authenticity, as the "from" email address might be different from the "reply" email address. Instead, you should create a new email using the email address you have for the person.

PASSWORD BEST PRACTICES

- Create unique passwords that use a combination of words, numbers, symbols, and both upper- and lower-case letters.
- Never use the same password for multiple websites. Each of your passwords should be unique.
- Change your passwords regularly.
- Always log out of websites and apps when you are done using them.
- Never use automatic login features that save your username and password on the websites you are visiting.
- Consider using a secure password manager. Reputable password managers, such as LastPass, allow you save your passwords in one place, meaning that you can make long and complicated passwords without worrying that you won't be able to remember them. This software will assist you in choosing strong passwords and then encrypt the passwords and store them online in a safe, cloud-based storage system. Be sure to do your research before choosing a password manager. Read the reviews and pay careful attention to the security features of the software.

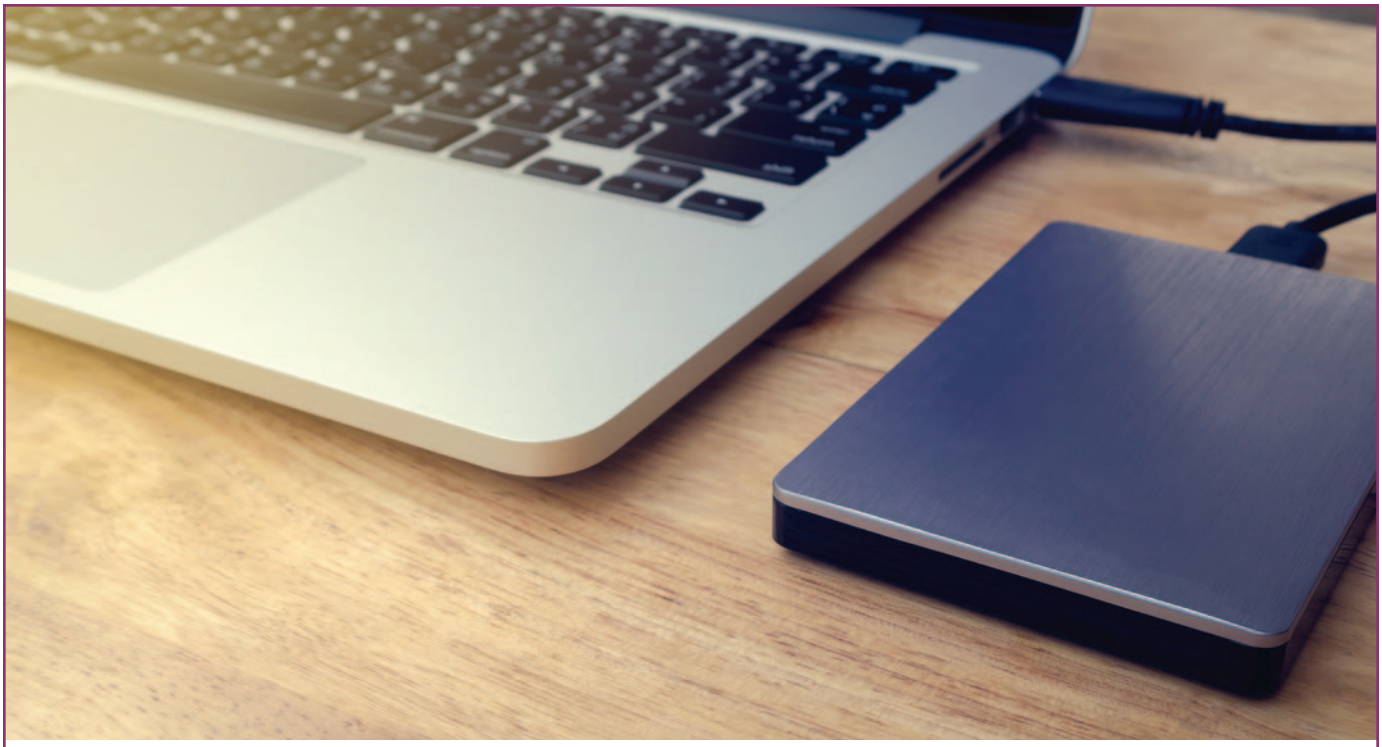
SECURITY SOFTWARE BEST PRACTICES

- A firewall acts as a barrier between your computer and any threat from outside your system. Ensure that the firewall on your computer is turned on and keep it updated. If you do not have a firewall on your computer, install a reputable one.
- Also install reputable anti-virus and anti-spyware software and keep it updated. The software will likely run regular scans on its own; just be sure to check that it is working properly and scanning at regular intervals.
- Two options for free, reputable anti-virus software that also include a firewall option are: Avast (https://avast.com/) and AVG (https://avg.com/).
- It is also important to install an Ad blocker extension on your web browser. While many ads on websites are not harmful, there are some websites that use ads to hide malware. Installing an Ad blocker on your browser will block potentially harmful ads from showing up.

INTERNET BROWSING BEST PRACTICES

- When accessing websites, always look for the "padlock" icon and an https:// to be sure you have a safe and secure connection during online banking, shopping, or while sending personal information.
- Adjust your web browser safety settings for optimal security. On most browsers, such as Firefox, Google Chrome, Internet Explorer or Safari, the security menus can be found in the upper right-hand corner of the browser window. If you are unsure of how to maximize your security settings, search on Google for how to do it (e.g., "how to choose maximum security settings on Firefox").
- Clear your browser cache after banking or shopping online to make sure your personal information isn't stored on your computer.

continued



- While browsing the web, you might suddenly encounter something on a web page that appears to be warning you about a problem with your device. It might even look like the alert is coming from your device. It isn't. These alerts are pop-ups designed to trick you into calling a phony support number or buying an app that claims to fix the issue. Don't call the number. Simply navigate away from that page.

BACKUP YOUR COMPUTER

- Always keep an up-to-date backup of your computer data stored on an external drive so that the data could be restored if the computer was stolen, damaged, or malfunctioned. Once the hard drive has been corrupted by a cyberattack, it is too late to do a backup, so it needs to be done regularly.
- The need for regular backups cannot be overemphasized. The hard drive of your computer is a mechanical device that can and may well fail—sometimes at the most inconvenient time—and can result in a loss of software programs and data.
- Automate the process if your software has a scheduler so the onus is not on you or others to initiate the backup process, but please make it part of your regular routine. Remember not doing backups is similar to leaving paper records out on the picnic table; it will rain!
- Practice retrieving data from the backup device so that you know it is working properly.
- The backup media should be stored off-site from the source computer.

CONSULT WITH AN IT PROFESSIONAL

- It is good practice for churches to consult with an IT professional once per year to ensure that their computer systems are up to date, and they are aware of the latest cybersecurity risks. You may have an IT professional in your congregation who is willing to help as a volunteer. Or there are plenty of paid professionals who are willing to come in to offer advice and maintenance.
- When facing a security issue with your computer systems, it is better to play it safe than be sorry, so be sure to seek professional advice when needed.

continued

What if We Experience a Cyberattack?

Because cyber threats are always changing, it is possible that, despite your best efforts, the computer(s) at your church may be compromised in a cyberattack. If this happens:

CONTACT AN IT PROFESSIONAL AS SOON AS POSSIBLE

- A professional who works with computers regularly and is familiar with cyber threats may be able to retrieve some of the lost information and restore your computer(s).
- Be sure to ask them to also put the appropriate measures in place to ensure maximum security in the future.

DISCLOSE BREACH TO THOSE AFFECTED

- Privacy Legislation in Canada that is designed to safeguard the personal data of Canadians requires that companies and organizations disclose when a breach has happened to those whose data has been compromised.
- Familiarize yourself with the *Personal Information Protection and Electronic Documents Act* and its requirements here: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

Appendix A: KEEPING FINANCIAL INFORMATION SECURE

- All paper records of donations should be kept under lock and key and accessible to authorized people only. Databases used to keep track of donors should be secure. Most database software will have security features built into it. Be sure to ask about that when you are acquiring software. The Session should be clear about who has authority to see these records.
- If your congregation is receiving gifts by credit card, it is important that this data is kept secured. Online giving forms should be on secure https:// web pages and ensure that your provider is PCI DSS (Payment Card Industry Data Security Standards) Compliant. Online donation programs will encrypt the credit card information (number, expiry date, CSV) when it is entered, and the congregation will never know the complete details (they may be given the last four digits of the credit card number). However, some programs allow you to manually enter the credit card information. If your congregation ever receives credit card information over the phone or on paper for manual input, the data should be entered into a system/program which encrypts the information immediately. Any paper it was written on should be destroyed. (Note: Many programs will store the encrypted information so it can be used to process another donation at a different time.) It should be clear who can receive donations and enter credit card information, and those authorized should be aware of best practices to ensure donor privacy.
- After the PAR contact person transcribes donor bank account information to the PAR confirmation letter, it is wise to file the original application under lock and key or simply destroy (shred) the application documents and void cheque.
- Interac e-Transfer donations via email are often the preferred method of digital giving for donors and churches alike. However, many banks prefer that churches receive e-Transfers by automatic deposit only. When an e-Transfer uses "question and answer" based password security, funds can be easily redirected to the wrong bank account, either by mistake or by fraud. Talk to your church's bank about the best way to secure Interac e-Transfers for your account.

50 Wynford Drive, Toronto, ON M3C 1J7
1-800-619-7301 | presbyterian.ca/eq4
canadianministries@presbyterian.ca