

Cyber Crime

Best Practices for Congregations

There is a familiar joke about the emails that appear in our spam folders from the “king” of a distant country offering a large inheritance in exchange for a small upfront payment.

Unfortunately, the humor fades when a church becomes the victim of such a scheme, losing significant sums of money that may never be recovered. Many victims are simply unaware of the risks associated with online activity or the threats that originate from the “Dark Web.”

Education, awareness, and proactive guidance are essential for prevention. By providing resources and training, organizations can help ensure individuals enjoy a safe online experience rather than falling prey to cyber crime.



INSURANCE BOARD
Partners in Protection

www.InsuranceBoard.org

Below are recommendations to help protect your congregation.

- 1. Use Strong Passwords:** Ensure all devices and online accounts are secured with passwords, including device lock screens. A strong password should contain at least 12 characters and include a combination of letters, numbers, and symbols. Avoid using personal information. Always log out or close sessions when finished.
- 2. Secure Account Access:** Because passwords can be compromised, enable multi-factor authentication whenever possible. This adds an additional one-time security code to help verify that the correct person — not just someone with a password — is accessing the account.
- 3. Pause Before Responding:** Communications that create pressure or a sense of urgency — such as warnings about bank accounts or taxes — are often fraudulent. When in doubt, contact the company directly using a verified phone number. For financial requests, confirm details internally through multiple trusted sources.
- 4. Delete Suspicious Messages:** Clicking links in unsolicited or unusual emails is a common way scammers obtain personal information. Even if an email appears to be from someone familiar, it may be spoofed. When unsure, delete the message. Activate spam filters to reduce the number of suspicious emails received.
- 5. Be Cautious with Online Sharing:** Limit the personal information shared on social media. Adjust privacy settings to control who can view posts, and avoid sharing real-time locations or other sensitive details.
- 6. Use Reliable Security Software:** Install reputable security software and keep it up to date. Run antivirus and anti-spyware tools regularly. Avoid downloading updates from pop-ups or unsolicited emails, as these may contain malware. Hosting informational sessions to help individuals secure their devices may also be beneficial.
- 7. Adjust Browser Safety Settings:** Review and update security settings in each internet browser. These options are typically located in the upper-right menu. Clear browsing history at the end of each session to help minimize exposure of sensitive information.
- 8. Enable Firewall Protection:** A firewall serves as a barrier against unauthorized access to internal systems. Many antivirus programs include customizable firewall features. When necessary, consult a computer professional for assistance with configuration.
- 9. Log Out Regularly:** Always log out of apps and websites when they are no longer in use. Leaving accounts open increases vulnerability to unauthorized access.
- 10. Seek Professional Support:** If your congregation does not have an internal IT specialist, consider hiring a trusted service provider to monitor systems and provide expert guidance.

Please remember to consult qualified experts — including attorneys and licensed financial or cybersecurity professionals — for advice specific to your ministry and its members.

Scan for
additional
Loss Control
Resources

