5 CYBERSECURITY RED FLAGS EVERY CHURCH SHOULD WATCH FOR

IS YOUR CHURCH AT RISK?

Focus Points	The Risk	Why It Matters	How to Fix It
Outdated Software & Systems	Running outdated operating systems, unpatched software, or unsupported devices.	Older systems lack security updates, making them easy targets for hackers.	Regularly update software and enable automatic security patches.
No Multi-Factor Authentication (MFA)	Relying only on passwords for staff and volunteer logins.	Weak or stolen passwords are the leading cause of breaches.	Enable MFA on all church accounts, especially for email, donor databases, and financial tools.
Lack of Cybersecurity Training for Staff & Volunteers	No formal security training for staff, pastors, or volunteers.	Phishing and social engineering attacks target human error more than technical weaknesses.	Conduct basic cybersecurity awareness training at least twice a year.
Weak or Reused Passwords	Staff and volunteers using the same passwords across multiple logins.	If one account is compromised, hackers can access multiple church systems.	Use password managers and require strong, unique passwords for each account.
No Incident Response Plan	No documented plan for handling a cyberattack or data breach.	Delays in response increase damage and recovery costs.	Create a clear incident response plan, including who to contact and immediate steps to contain a breach.

☎ 720-927-1997

zach@lambtele.com

www.lambtele.com

LAMB TELECOM