5 CYBERSECURITY MYTHS CHURCH LEADERS BELIEVE

1 CYBERSECURITY IS A TECHNOLOGY PROBLEM, AND THE JOB OF THE IT DEPARTMENT.

BUSTED: Cybersecurity is important to everyone. As church leadership, you taking cybersecurity seriously sets the tone for everyone else. The truth is that end-users are your best defense AND your worst vulnerability.

BEST PRACTICE: TRAIN YOUR STAFF with an ongoing program for both training and testing.

2 WE'RE JUST A CHURCH. NOBODY WANTS OUR DATA.

BUSTED: Church data is valuable, because of PII. Cyber-criminals can use the Personal Identifiable Information stored in a church's database to gain a foothold.

BEST PRACTICE: Use unique, strong passwords and require/enable Multi-Factor Authentication on every account that you can.

3 OUR PEOPLE ARE SMART ENOUGH TO NOT WORRY ABOUT PHISHING OR SOCIAL ENGINEERING.

BUSTED: Hackers are SMART, and they prey on people's distraction. No one is perfect – we all do things without thinking at times. Cyber-criminals know what to say; sometimes their efforts are obvious, but oftentimes not!

BEST PRACTICE: Implement SPAM email filtering and use IRONSCALES for anti-phishing and awareness.

4 OUR SITE AND/OR CHMS IS ENCRYPTED, SO OUR ONLINE GIVING IS SAFE.

BUSTED: Payment Card Industry Data Security Standards (PCI-DSS)

BEST PRACTICE: Process transactions on the processor's secure site. For onsite donations, make sure the kiosk or POS product supports point-to-point encryption or a secure virtual terminal for card entry. Have someone knowledgeable of PCI-DSS requirements and your network and software environment assess your situation to be sure you meet the requirements.

5 A DOLLAR SPENT ON TECHNOLOGY IS A DOLLAR NOT SPENT ON MINISTRY.

BUSTED: Technology is an integral part of delivering ministry.

BEST PRACTICE: You need a distinct, dedicated IT budget. Ideally, this is coupled with a multi-year "Technology Roadmap" to help you plan for proactive replacements, upgrades, cybersecurity spending, and church/staff growth.