UMC INFORMATION TECHNOLOGY SUPPORT

DIGITAL STEWARDSHIP

Protecting Your Church Online

SPEAKER

Lori Baughman
Learning and Development Instructor

CYBERSECURITY FOR CHURCHES

Best Practices to Protect Your People, Data & Mission

Strategies to Safeguard Congregations and Sensitive Information

Overview

Building a Strong Culture of Cybersecurity

Understanding the Importance of Cybersecurity for Churches

Critical Cybersecurity Risks and Best Practices

Real-World Examples of Church Cyberattacks

Maintaining Secure Systems and Data Recovery

UNDERSTANDING THE IMPORTANCE OF CYBERSECURITY FOR CHURCHES

WHY ARE CHURCHES INCREASINGLY TARGETED BY CYBERCRIMINALS?

Limited Cybersecurity Resources
Many churches have limited budgets and outdated systems, increasing their vulnerability to cyberattacks.

Valuable Information Held
Churches store sensitive personal, financial, and donor data, making them prime targets for cybercriminals.

TYPES OF SENSITIVE DATA AT RISK

Member Records

Churches keep personal member data which must be securely protected to ensure privacy and trust.

Financial Donations

Financial donation information is sensitive and requires protection against unauthorized access.

Payroll Records

Payroll details including birthdates and social security numbers are critical data that necessitate stringent security measures.

Communications

The protection of confidential communications is vital to ensuring both individual privacy and organizational trust.

DISPELLING THE MYTH

'Too Small to Be Attacked'

Common Misconception

Small churches often believe they are safe from cyberattacks due to their size, which is a dangerous misconception.

Targeted by Cybercriminals

Cybercriminals exploit smaller organizations because of their typically weaker cybersecurity defenses and protocols.

Importance of Cybersecurity

All churches, regardless of size, must prioritize cybersecurity to protect sensitive information and maintain trust.

REAL-WORLD EXAMPLES OF CHURCH CYBERATTACKS

RANSOMWARE INCIDENTS INVOLVING CHURCHES

Impact on Churches

Ransomware attacks encrypt church data, leading to disruption of services and operations.

Financial Consequences

These incidents impose significant financial burdens due to ransom demands and recovery costs.

Need for Preparedness

Robust cybersecurity measures are needed to protect church data and services.

SCAMMERS IMPERSONATING CHURCH LEADERS

Nature of Impersonation Scams

Attackers pose as pastors or church staff to fraudulently solicit donations from congregants.

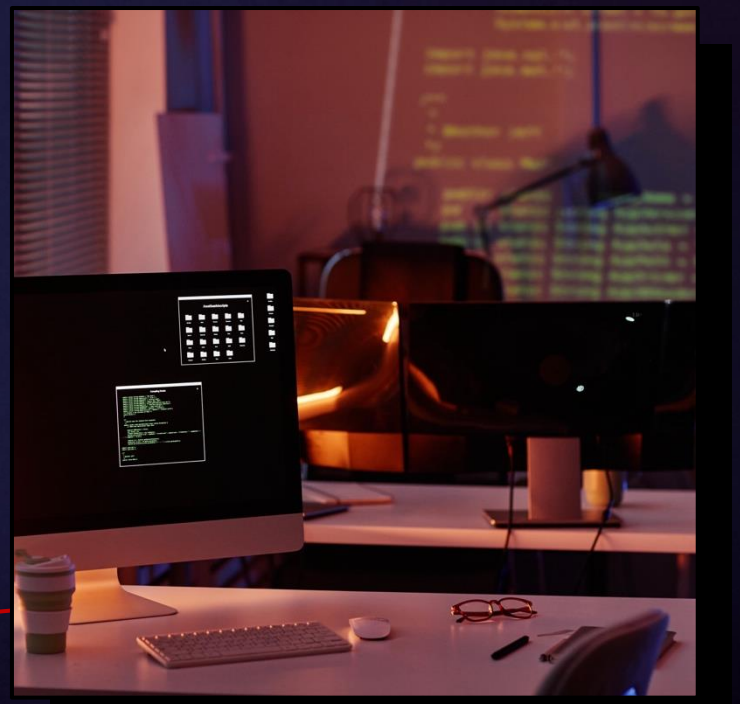
Importance of Awareness

Educating church members on scams helps reduce susceptibility to fraudulent solicitations.

Verification Protocols

Implementing verification steps ensures legitimacy before transferring funds or sharing sensitive information.

DATA BREACHES



Exposure of Sensitive Information

Data breaches have revealed confidential employee and church financial data, increasing risks of identity theft.

Consequences of Data Breaches

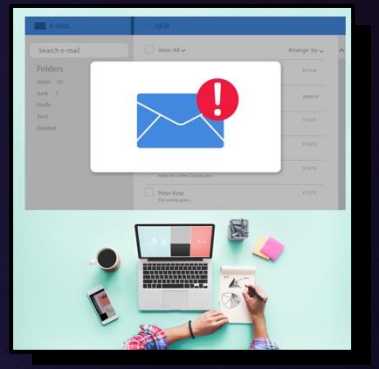
Breaches cause reputational damage and loss of trust for organizations such as churches.

Importance of Data Protection

Implementing strong data protection measures is essential to safeguard sensitive information.

BUILDING A STRONG CULTURE OF CYBERSECURITY

CYBERSECURITY DISCUSSIONS AND AWARENESS



Consistent Cybersecurity Communication

Regular discussions keep staff and volunteers updated on current cybersecurity threats and best practices.

Fostering Vigilance and Proactivity

Ongoing awareness encourages vigilance and proactive behavior against security risks

APPOINTING A CYBERSECURITY CHAMPION

Dedicated Leadership

Appointing an expert ensures focused leadership for cybersecurity initiatives and continuous risk monitoring.

Risk Identification

A cybersecurity champion actively identifies and assesses potential security threats to the organization.

Coordinated Protection

The champion coordinates protective measures to strengthen the organization’s security posture effectively.

INTEGRATING CYBERSECURITY EARLY AND OFTEN

Early Cybersecurity Awareness
Integrating cybersecurity education during onboarding ensures new members understand security risks from the beginning.

Ongoing Security Training
Continuous training helps maintain strong defenses as staff and volunteers transition or roles evolve

CRITICAL CYBERSECURITY RISKS & BEST PRACTICES

STRONG PASSWORDS & MULTI-FACTOR AUTHENTICATION (MFA)

Strong Unique Passwords

Creating strong and unique passwords is essential to protect accounts from unauthorized access and cyber threats.

Multi-Factor Authentication

Enabling multi-factor authentication adds an extra layer of security beyond passwords to safeguard user accounts.

PHISHING

IDENTIFYING AND AVOIDING ATTEMPTS

Phishing Email Risks

Phishing emails are designed to steal personal credentials or install harmful malware on devices.

Recognizing Suspicious Messages

Learn to identify red flags in emails such as unknown senders, urgent requests, and suspicious links.

Avoiding Dangerous Links

Avoid clicking on unknown links in emails to protect your credentials and device from compromise.

UNDERSTANDING & PREVENTING RANSOMWARE ATTACKS

01

Impact of Ransomware

Ransomware can lock essential data and stop business operations, causing significant disruption.

02

Regular Data Backups

Maintaining regular backups ensures data recovery and reduces the impact of ransomware infections.

03

Software Updates

Updating software frequently helps fix security vulnerabilities that ransomware exploits.

04

User Awareness

Educating users to avoid malicious links and attachments is critical to prevent ransomware infections.

MAINTAINING SECURE SYSTEMS AND DATA RECOVERY

KEEPING SOFTWARE, APPS, AND TOOLS UP TO DATE

Importance of Regular Updates

Regular software updates fix security vulnerabilities and prevent potential exploits effectively.

Automation Benefits

Automating updates or scheduling them ensures timely patching and reduces manual effort.

ESTABLISHING REGULAR AND TESTED DATA BACKUP ROUTINES

Consistent Data Backups

Regularly backing up data ensures availability after data loss incidents or attacks.

Secure Offsite Storage

Backing up data securely offsite or in the cloud protects against local failures or disasters.

Backup Restoration Testing

Regularly testing backup restoration confirms data integrity and recovery readiness.

EFFECTIVE RECOVERY STRATEGIES AFTER A CYBER INCIDENT

Clear Incident Response Plan

A well-defined incident response plan enables quick and efficient reaction to cyberattacks in organizational settings.

Minimizing Damage

Prompt response reduces the impact of cyberattacks and limits potential system and data damage.

Restoring Operations

Effective recovery strategies help restore normal business functions as quickly as possible after an incident.

CONCLUSION

Growing Cybersecurity Risks

Churches increasingly face cybersecurity threats targeting their data and communities.

Building Security Culture

Fostering awareness and best practices within church communities enhances security resilience.

Importance of Vigilance

Ongoing vigilance and preparation are essential to safeguard mission and data integrity.

PANEL DISCUSSION

Sharon Asmus
Chief Information Officer

Rob Jett
Technology Services Manager

OUR MINISTRY

We focus on administration so YOU can focus on Ministry

UMC INFORMATION TECHNOLOGY SUPPORT

"Your people have sorted out the problems and I feel much happier coming to worship on Sunday knowing that the computer will not cause me problems.“

Pastor Dave

When JC came in to prepare for preschool worship on Monday at about 8 a.m. she found the screens in the sound booth black and no response whatever she did. She tried everything to get the system up and finally called UMC Support and Kyle had her going within five minutes, another time we were glad to have your expertise."

COMING SOON
TECHNOLOGY VALUE PACK!

Protect your ministry. Simplify your tech. Gain peace of mind.

Cybersecurity Essentials

24/7 monitoring, antivirus, and data backup to keep your computers and ministry files protected.

Service Desk Support

Access to our IT team for help with software, connectivity, or device issues.

Advanced Security

Protection from phishing and email scams, password management, and intrusion prevention.

Scan QR code or email connectionalrelations@gcfa.org to get started!

RESOURCES

- Create and Use Strong Passwords - National Cybersecurity Alliance
- What is Multifactor Authentication (MFA) and Why Should You Use It? - National Cybersecurity Alliance
- What Is Phishing and How To Avoid It - National Cybersecurity Alliance
- How to Update Your Software - National Cybersecurity Alliance

THANK YOU!

For more information visit:

https://www.gcfa.org/technology-support-services

UMC INFORMATION TECHNOLOGY SUPPORT