

Protecting the Church

Cybersecurity, AI, and how they affect the local church



How to Use This Guide

Treat each slide as one conversation, one decision, and one next step.



01

Read

Understand the practice in plain language.



02

Discuss

Identify who owns the decision and who needs to participate.



03

Act

Complete the practical actions listed on the slide.



04

Record

Document the decision so it survives staff transitions.

The checklist is designed to become a repeatable ministry process, not a one-time project.

Critical Systems Inventory Documented

Know which systems ministry depends on and who is responsible for each one.



**You cannot protect
what you have not
documented.**

WHAT THIS MEANS

Create one reliable inventory of every critical system used by the church or conference.

WHY IT MATTERS

If essential knowledge exists only in one person's memory, the ministry may lose access, miss a renewal, or struggle to recover when that person is unavailable.

WHAT TO DO NOW

- List email, giving, accounting, church management, website, livestream, member database, and cloud storage systems.
- Record the account owner, hosting location, renewal date, support contact, and recovery information.
- Assign someone to keep the inventory current.

Administrative Access Reviewed

Every elevated permission should have a clear ministry purpose.



**Access should follow
responsibility, not
convenience.**

WHAT THIS MEANS

Review administrative privileges and confirm why each person needs the level of access assigned.

WHY IT MATTERS

Unused accounts and excessive permissions increase risk. Documented access decisions improve accountability and make future reviews easier.

WHAT TO DO NOW

- Ask, “Why does this person need access?” for every administrator.
- Remove unused accounts and permissions that no longer match a ministry role.
- Document who approved access and the reason it was granted.

MFA Enabled and Password Plan Established

Protect accounts with consistent authentication and recovery practices.



**A password is stronger
when it is unique and
backed by MFA.**

WHAT THIS MEANS

Use strong, unique passwords, multi-factor authentication, and a consistent plan for account ownership and recovery.

WHY IT MATTERS

Shared or personally owned ministry accounts can create continuity problems during staff transitions. Reliable recovery information keeps church leadership in control.

WHAT TO DO NOW

- Enable multi-factor authentication wherever it is available.
- Use a password manager for shared ministry accounts.
- Avoid personal email addresses for church-owned services.
- Keep recovery information accessible to authorized leadership.

Access Guidelines Defined

Give staff the minimum access needed.



Access should be specific, understood, and reviewed.

WHAT THIS MEANS

Set clear rules for the permissions, acceptable use, confidentiality, and data protection expectations.

WHY IT MATTERS

Ongoing process that ensures that only authorized people can access specific systems, data, applications, or physical locations.

WHAT TO DO NOW

- Provide only the permissions required for the current role (reviewed with every transition).
- Explain acceptable use, confidentiality, and data handling expectations.
- Review accounts regularly (quarterly).
- Remove access when responsibilities change.

Device Security Standards Documented

Protect church information on both church-owned and personal devices.



Ministry data deserves protection wherever it is used.

WHAT THIS MEANS

Document minimum security expectations for every device used to conduct ministry work.

WHY IT MATTERS

UMC organizations often operate in mixed-device environments. Clear standards reduce ambiguity and make protection consistent across UMC-owned and personal equipment.

WHAT TO DO NOW

- Keep UMC-owned devices updated, protected by antivirus, advanced threat detection and secured with screen locks.
- Set expectations for passwords and software updates on personal devices used for ministry.
- Define how organizational information may be stored, accessed, and shared.

Files Stored in Approved Locations

Keep sensitive records in managed storage with appropriate access and backup.



**Good record
management protects
trust.**

WHAT THIS MEANS

Store ministry records in approved cloud platforms rather than personal drives or unmanaged storage locations.

WHY IT MATTERS

Employee and financial records deserve special care. Managed storage supports restricted access, retention, and dependable backup.

WHAT TO DO NOW

- Move important records to approved only authorized locations.
- Limit sensitive information to authorized individuals.
- Establish retention guidelines.
- Confirm that backups are performed regularly.

Website and Domain Ownership Verified

Protect the organization's digital front door and communication channels.



The ministry should control its domain, website, and email.

WHAT THIS MEANS

Confirm that leaders can access and recover the website, domain registration, and communication platforms.

WHY IT MATTERS

Losing control of a domain or communication account can significantly disrupt ministry. Shared institutional knowledge makes recovery possible.

WHAT TO DO NOW

- Ensure more than one trusted leader knows how to access domain and website management.
- Protect email communication platforms with multi-factor authentication.
- Review public staff directories, forms and contact methods to reduce spam and fraud.

Financial Platform Access Review

Apply heightened scrutiny to giving, banking, accounting, and payment systems.



**Financial access is a
stewardship
responsibility.**

WHAT THIS MEANS

Review everyone who can access giving platforms, banking systems, accounting software, and payment processing services.

WHY IT MATTERS

Financial systems are frequent targets for cybercriminals. Separating responsibilities reduces the chance that one person controls every part of a transaction.

WHAT TO DO NOW

- Verify that each person's access is current and appropriate.
- Separate financial responsibilities whenever possible.
- Remove access promptly when a role changes.
- Schedule periodic access reviews.

Off-boarding Checklist Created

Remove access and transfer ministry information when someone leaves.



Departure should trigger a documented process.

WHAT THIS MEANS

Use a consistent checklist whenever a staff member leaves a ministry role.

WHY IT MATTERS

Delayed off-boarding can lead to unauthorized access, missing files, and confusion about ownership. Prompt action protects continuity and ministry information.

WHAT TO DO NOW

- Disable accounts promptly.
- Collect organization-owned equipment.
- Transfer files and account ownership.
- Update shared passwords.
- Remove system permissions.

Onboarding Checklist Created

Help new staff and volunteers begin ministry safely.



**Good security habits
should begin on day
one.**

WHAT THIS MEANS

Provide accounts, security expectations, authentication, and awareness training through a documented process.

WHY IT MATTERS

A consistent start helps new team members understand both the technology they use and their responsibility to protect ministry information.

WHAT TO DO NOW

- Provide accounts through an approved process.
- Explain organizational procedures and acceptable-use expectations.
- Enable multi-factor authentication.
- Offer new hire security awareness training.

Security Review Schedule Established

Make cybersecurity a routine part of ministry operations.



**Small, regular reviews
prevent larger
problems.**

WHAT THIS MEANS

Set a quarterly or semiannual schedule for reviewing accounts, permissions, devices, vendors, and critical systems.

WHY IT MATTERS

Routine reviews identify changes and small issues before they become major problems. Documented findings also make follow-through visible.

WHAT TO DO NOW

- Choose a quarterly or semiannual review rhythm.
- Document findings and unresolved issues.
- Assign owners and due dates to action items.
- Track completion before the next review.

Trusted Support Resources Identified

Know who to contact before a technology or security problem occurs.



**Asking for help is
responsible
stewardship.**

WHAT THIS MEANS

Identify trusted technology partners, denominational resources, security professionals, or managed service providers that can assist the ministry.

WHY IT MATTERS

No organization is expected to solve every technology challenge alone. A known support path improves response when suspicious activity or difficult changes occur.

WHAT TO DO NOW

- Record trusted contacts and how to reach them.
- Ask for help when implementing new systems.
- Seek assistance when responding to suspicious activity.
- Document an Incident Response Plan.

Protect Yourself

Practical steps for pastors, treasurers, office staff and volunteers. No technical background needed.



**The threats
churches
face**



**How AI
changes the
scams**



**Protecting
church
money**



**Protecting
confidential
information**



**Everyday
habits and
responding**

WHY IT MATTERS

Churches are trusting places. Scammers count on that.

WHAT MAKES CONGREGATIONS ATTRACTIVE TARGETS



A culture of trust and wanting to help



Small staff and volunteers wearing many hats



Names, roles and emails posted on websites and in bulletins



Money moving every week: offerings, payroll, vendors, online giving



Shared passwords and older computers

What attacks on churches look like



Phishing email

Looks like it's from the bank, Microsoft or the conference, asking you to click a link and "verify" your login.



Pastor, Conference staff impersonation

"Are you available? I need a quick favor." Then a request for gift cards or a wire transfer, from a look-alike address.



Check & payment fraud

Stolen checks get altered or copied. Fake "vendor" emails ask you to change where payments are sent.



Ransomware

Malicious software locks church files, records and membership data until a ransom is paid.

Six red flags in any message



Mismatched sender

The name says "Pastor," but the address is a stranger's.



Urgency or secrecy

"Today," "right away," "keep this between us."



Unusual payment

Gift cards, wire transfers, or new bank details.



Suspicious links

Hover before you click: does it go where it claims?



Unexpected attachments

Invoices or "documents" you weren't expecting.



Asks for a password or code

No legitimate organization needs these from you.

The gift card scam, step by step

1 · THE HOOK

"Are you available? I need a quick favor."

2 · THE EXCUSE

"I'm in a meeting and can't talk. Just reply here."

3 · THE ASK

"Buy gift cards for a family in need and send me the codes."

4 · THE LOSS

Once the codes are shared, the money is almost impossible to recover.



Make it policy: no request for gift cards or payments will ever come by text or email alone.

The "we've changed banks" scam



A familiar email

It appears to come from your contractor, utility, or a staff member, sometimes from their real, hacked account.



New account details

"Please update our banking information for future payments" or "change my direct deposit."



Found out too late

Nobody notices until the real vendor or employee asks why they weren't paid.



Defense: call the vendor or employee at a number already on file, and have two people approve any banking change.

AI makes old scams far more convincing



Voice cloning

Sermon audio posted online can be used to imitate the pastor's voice on a phone call.



Polished phishing

No more typos to tip you off. Emails can mimic how your pastor or treasurer actually writes.



Tailored stories

Your website, bulletins and social posts give AI the details to build a believable request.



Fake video

Video calls and photos can be faked. Seeing someone is no longer proof it's them.

The Monday morning call



The treasurer's phone rings. It sounds exactly like the pastor:

"I'm at the hospital with a family and my phone's about to die. The roofer needs \$8,500 today or we lose our spot. I'm texting you the account number. Please just send it."

ASK

What red flags do you hear?

ASK

What should the treasurer do next?

Positive Pay: let the bank check your checks



STEP 1

You report

Each time you write checks, send the bank the list: check number, date, amount and payee.



STEP 2

Bank compares

Every check that comes in for payment is matched against your list.



STEP 3

You decide

Anything that doesn't match is flagged. You approve it or have it returned, before the bank's deadline.



Also ask about: payee-name matching and ACH Positive Pay / ACH debit blocks, which stop unauthorized electronic withdrawals.

Paper checks are still a target



How it happens

- Checks are stolen from mailboxes
- Ink is "washed" and the payee or amount rewritten
- Account numbers are copied onto counterfeit checks
- A check in the offering plate exposes the giver's account number too



How to protect the church

- Use Positive Pay
- Mail checks inside the post office
- Write checks with gel ink, which resists washing
- Pay vendors electronically when you can
- Reconcile statements promptly every month

More safeguards to ask your bank about

SAFEGUARD	WHAT IT DOES
Dual approval	A second person must approve any wire or online payment
ACH block or filter	Only approved companies can pull money from the account
Account alerts	Text or email for large withdrawals and new payees
Separate accounts	Keep online giving and operating funds apart to limit exposure
Daily review	Look at activity online every day, not just at month-end
Callback on changes	Never change vendor or payroll bank details from an email alone

Keeping online giving safe



Use a reputable processor

Let an established giving platform handle card data, with two-step login on the admin account.



Never store card numbers

No card numbers on paper forms, spreadsheets or email. If someone sends one, delete it.



Watch for "card testing"

A burst of tiny gifts from strangers means criminals are testing stolen cards. Ask your provider to turn on fraud filters.



Review reports regularly

Check refunds, disputes and changes to where deposits go.

Never read or send it over the phone or email



What counts as confidential

- Bank account and routing numbers
- Passwords and one-time login codes
- Social Security and tax ID numbers
- Giving records and pledge amounts
- Pastoral care and prayer concerns
- Personnel and payroll details



Why not?

- Caller ID and email addresses are easy to fake
- Email can be forwarded, hacked or misaddressed
- Your bank will not call asking for your password or a login code
- Once it's read aloud or sent, you can't take it back

What to say: simple scripts



SOMEONE ASKS FOR ACCOUNT INFO

"I'm not able to share that over the phone. I'll call you back at the number we have on file."



"THE BANK" CALLS YOU

"Thanks. I'll hang up and call the number on the back of our card."



A REQUEST FEELS OFF

"Church policy says I have to confirm this with a second person first."

The callback rule

1

Pause

Urgency is the scammer's tool. Real needs can wait ten minutes.

2

Don't reply

Hang up, or don't answer the email or text. Don't click its links.

3

Call a known number

Use the church directory, the back of your bank card, or the official website, never the number in the message.

4

Bring in a second person

Any new payment or banking change gets a second set of eyes.



Tip: agree on a staff code word for urgent requests by phone. An AI-cloned voice won't know it.

Caring for members' information



Directories

Keep online directories behind a login, and ask before publishing anyone's details.



Giving records

Limit access to the people who need it, such as the financial secretary.



Paper files

Lock cabinets, shred what you don't need, and keep desks clear.



Prayer lists

Share only what the person agreed to, and keep health details off public lists and websites.

Six basics that stop most attacks



Two-step login

Turn on multi-factor authentication for email and banking.



Password manager

A unique, strong password for every account.



No shared logins

Each person gets their own account; remove access when people leave.



Keep updated

Install updates on computers, phones and routers promptly.



Back up

Keep a copy of church records off-site, and test restoring it.



Guest Wi-Fi

Keep visitors on a separate network from the office.

Using AI tools wisely at church



Good uses

- Drafting newsletters and announcements
- Brainstorming events and program ideas
- Summarizing public documents
- Always fact-check before anything goes out



Don't put in

- Member names with giving or contact details
- Pastoral care notes or prayer concerns
- Financial statements, payroll or bank records
- Anything you wouldn't post publicly



Next step: adopt a short written AI policy for staff and volunteers.

What a church AI policy should cover

TOPIC	QUESTIONS TO ANSWER
Approved tools	Which AI tools may staff and volunteers use?
Off-limits data	What may never be entered: names, giving, care notes, finances
Human review	Who checks AI-drafted content before it's published or sent?
Transparency	When do we say AI helped create something?
Decisions	AI never makes final decisions about money or people
Point person	Who answers questions and keeps the policy current?

Act fast, and don't be embarrassed

1 Stop

Don't send more money.
Disconnect an infected computer
from the network.

2 Call the bank now

The sooner they know, the better
the chance of stopping or
recovering a payment.

3 Secure accounts

Change passwords and turn on
two-step login.

4 Tell leadership

Pastor, finance chair, trustees, and
the district or conference office.

5 Call your insurer

Ask whether the church has crime
or cyber coverage.

6 Report it

FBI: ic3.gov
FTC: reportfraud.ftc.gov

Your 30-day checklist



Ask the bank about Positive Pay and ACH blocks



Turn on two-step login for email and banking



Require dual approval for all payments



Put the callback rule in writing



Review who has access to every account



Back up church files and test a restore

Questions?

*Be wise as serpents and innocent as doves.
Matthew 10:16*



HELPFUL RESOURCES

CISA cyber guidance

cisa.gov

FBI scam reporting

ic3.gov

FTC fraud reporting

reportfraud.ftc.gov

Your bank's fraud line