FINANCE & ADMINISTRATION
General Council on Finance and Administration
THE UNITED METHODIST CHURCH

UMC SUPPORT INFORMATION TECHNOLOGY

SECURITY CONSIDERATIONS WHEN USING TECHNOLOGY

Sharon **Asmus**

Chief Information Officer

☎ Phone: 615-916-2729

✉ Email: sasmus@gcfa.org

1908 Grand Ave. Nashville, TN 37212

www.UMCSupport.org

The Omaha Christmas Blizzard - 2009

A little bit about me:

- I’m from Nebraska (#GBR)
- I moved to Nashville in 2010
- This is my 31st year in technology
- I’m a generalist – I know a little about a lot of things
- My expertise is with cyber security and data
- My superpower is translating tech speak into English
- I ♥ Excel
- Zero pets, 1 husband, 2 daughters, 3 plants
- My SEC team is Auburn (#wareagle)

Technology Leadership Team

Josh Wallin, IT Operations Director

Josh joined GCFA in October of 2022. He resides Idaho and has 15 years of IT management experience supporting domestic and international teams. Josh and his team at GCFA support our customers’ IT projects, onboarding, and infrastructure needs, such as your managed servers and networks. When not leading his team and supporting our IT customers, Josh enjoys spending time outdoors and all things sports.

Rob Jett, Technology Services Director

Rob Jett, joined GCFA April 2024. He is responsible for customer relationship management, IT service management and endpoint equipment sales & support. Rob is an Ole Miss graduate with a passion for technology and problem-solving. He brings a wealth of experience from his previous technology leadership roles. Outside of work, Rob enjoys golfing, fishing, and attending live music concerts.

Adam Fahey, Enterprise Applications Manager

Adam is not a new name to many of our IT Support customers. He has been with GCFA since 2012. Before officially joining GCFA, Adam worked as a GP consultant with Tribridge serving GCFA. He supports our ERP systems and integrations such as Microsoft Great Plains, Donor Direct, and Jet Reports. When not working, Adam enjoys walking his dog, watching sports, and hiking/camping.

Introduction

As a Technology Managed Service Provider (MSP), we are like the tech-savvy guardian angel for organizations of the United Methodist Church. We swoop in, armed with keyboards and coffee, to keep your digital kingdom running smoothly. Here's the lowdown:

What's an MSP Anyway?

- We're the ones who handle all things tech so that our customers, UMC organizations including GCFA, can focus on what really matters: the mission of the United Methodist Church.

Our Ministry

We focus on technology administration so

YOU can focus on ministry

UMC INFORMATION TECHNOLOGY SUPPORT

FINANCE & ADMINISTRATION
General Council on Finance and Administration
THE UNITED METHODIST CHURCH

- ***Area Conference Office Manager:*** *“We have had a wonderful experience using GCFA for our IT service needs. First, we save almost 70% a month in billing. Second, we get quick response, and the team has gone above and beyond in onboarding us and getting us acclimated to the new environment.*

- ***Area Conference IT Specialist:*** *"As I've come to usually expect, I had a great experience working with the GCFA Support Team. They were quick to respond when our server crashed…. The Team worked with me in a collaborative fashion … and we were operational again within a relatively short time."*

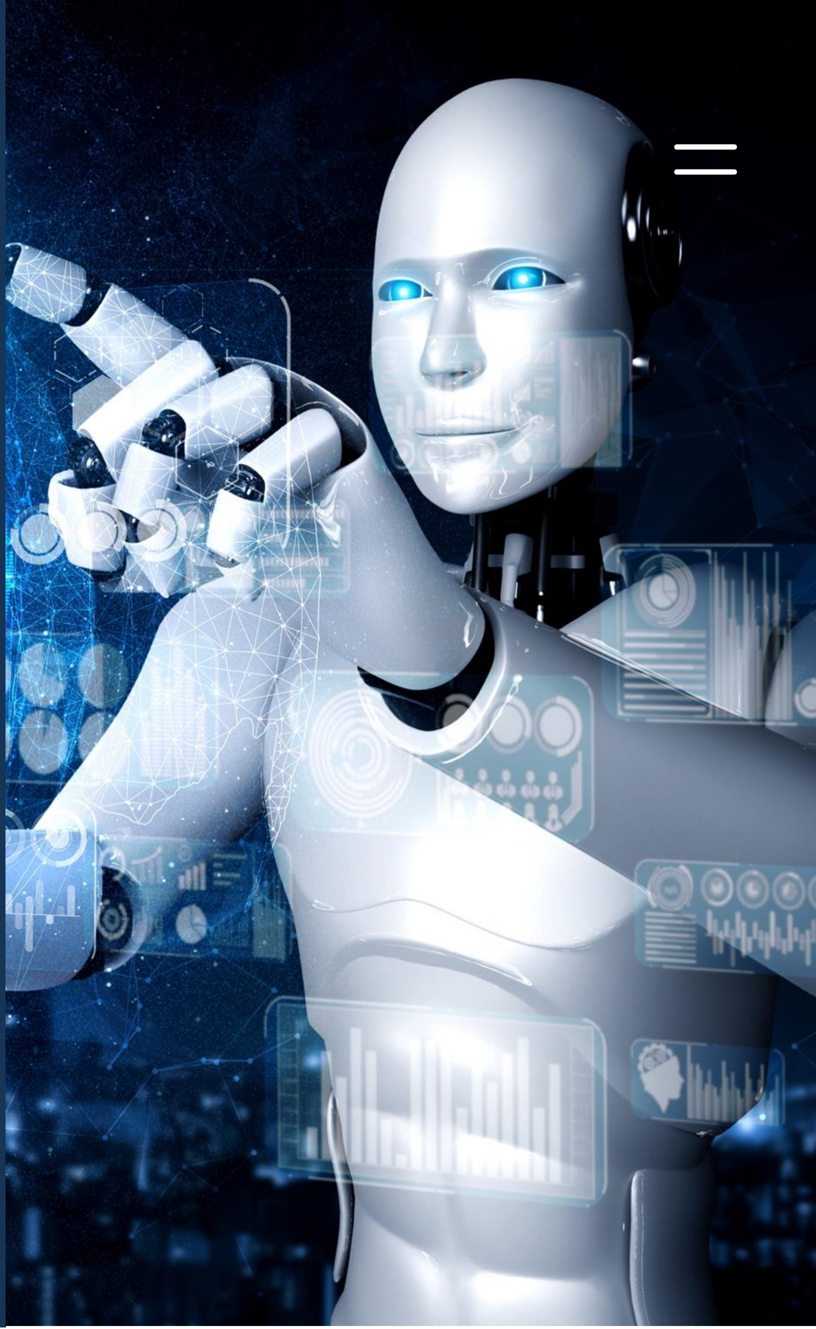
Agenda

- Module 1: AI Safety (30 minutes)
- Technology Security Considerations
  - Module 2: Internet Access & Safety (10 minutes)
  - Module 3: Computer Safety (10 minutes)
  - Module 4: Email & File Security (10 minutes)
  - Module 5: Cloud Apps & Third-Parties (10 minutes)
  - Module 6: Privacy & Data Security (10 minutes)
  - BONUS: Security Awareness Training (10 minutes)

We ALL must protect UMC
from data loss due to misuse,
disclosure, fraud or destruction

Module 1: AI Safety

Who Uses AI Today?

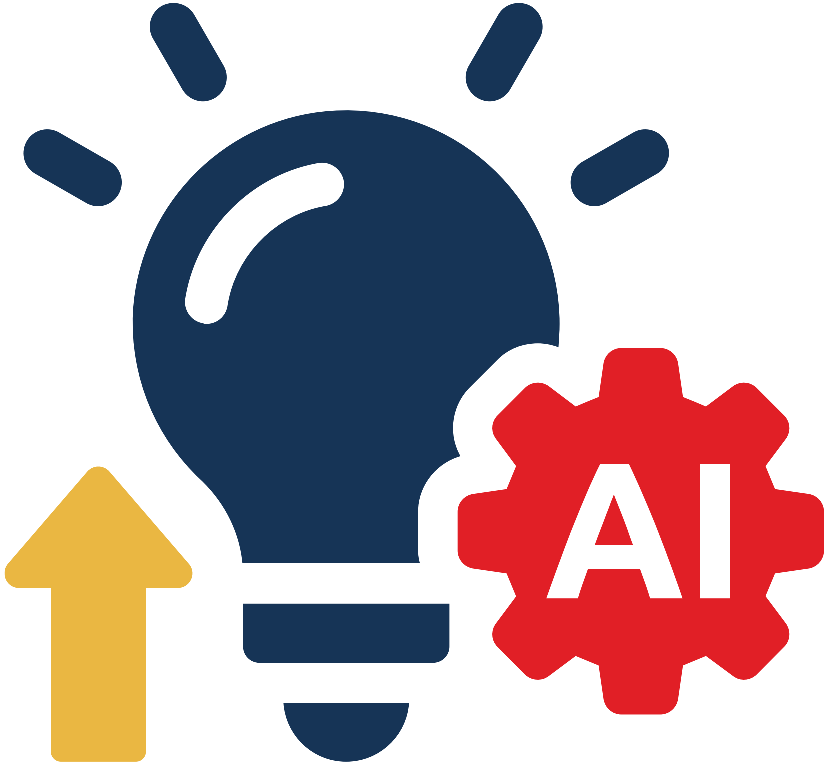


Overview Of AI

AI refers to the simulation of human intelligence in machines that are programmed to think and learn.

Examples Of AI

In Everyday Life



Virtual Assistance

- Siri & Alexa

Recommendations Systems

- Netflix & Amazon

AI In Healthcare

- Diagnostic Tool & Personalized Treatment Plans

AI In Finance

- Fraud Detection & Credit Scoring

Virtual Meeting Assistants

- Zoom & MS Teams

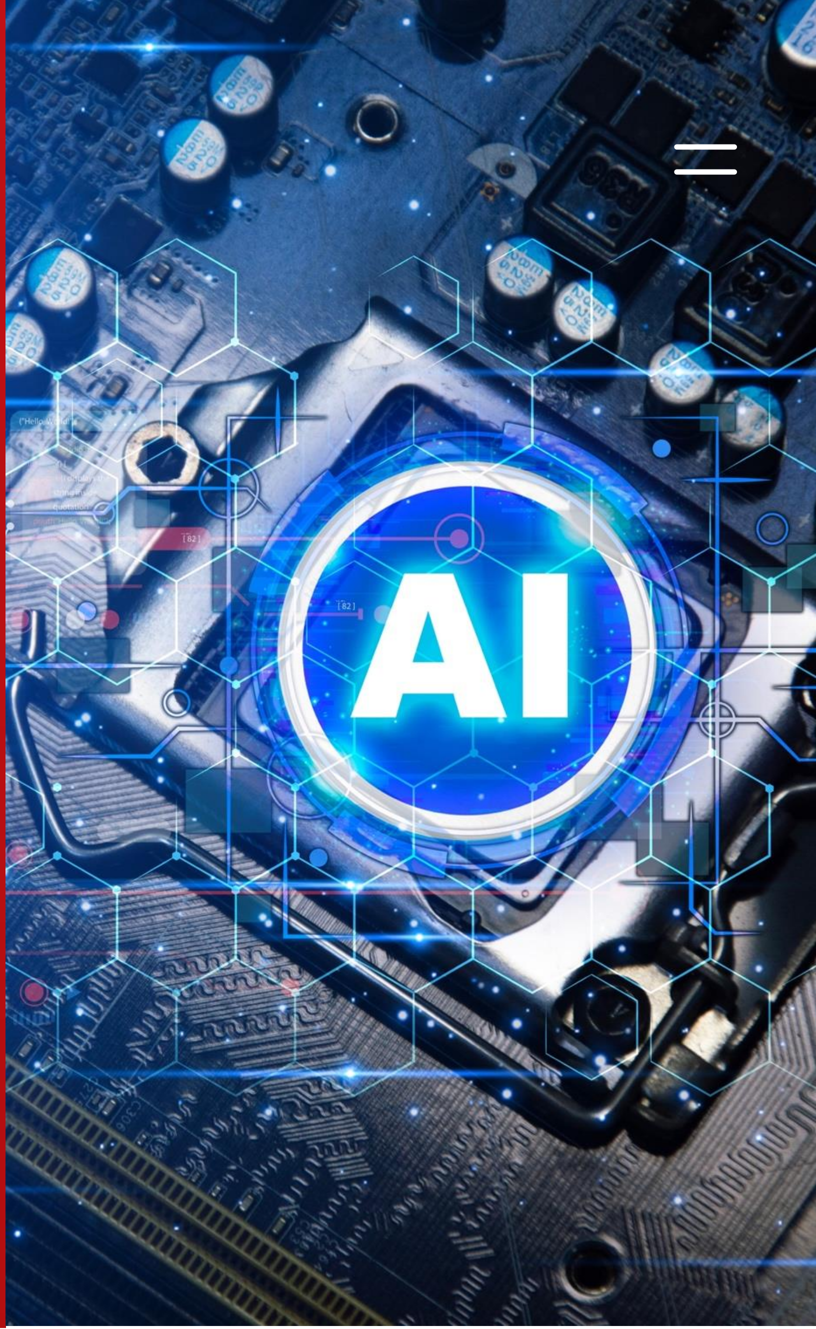
Other Acronyms

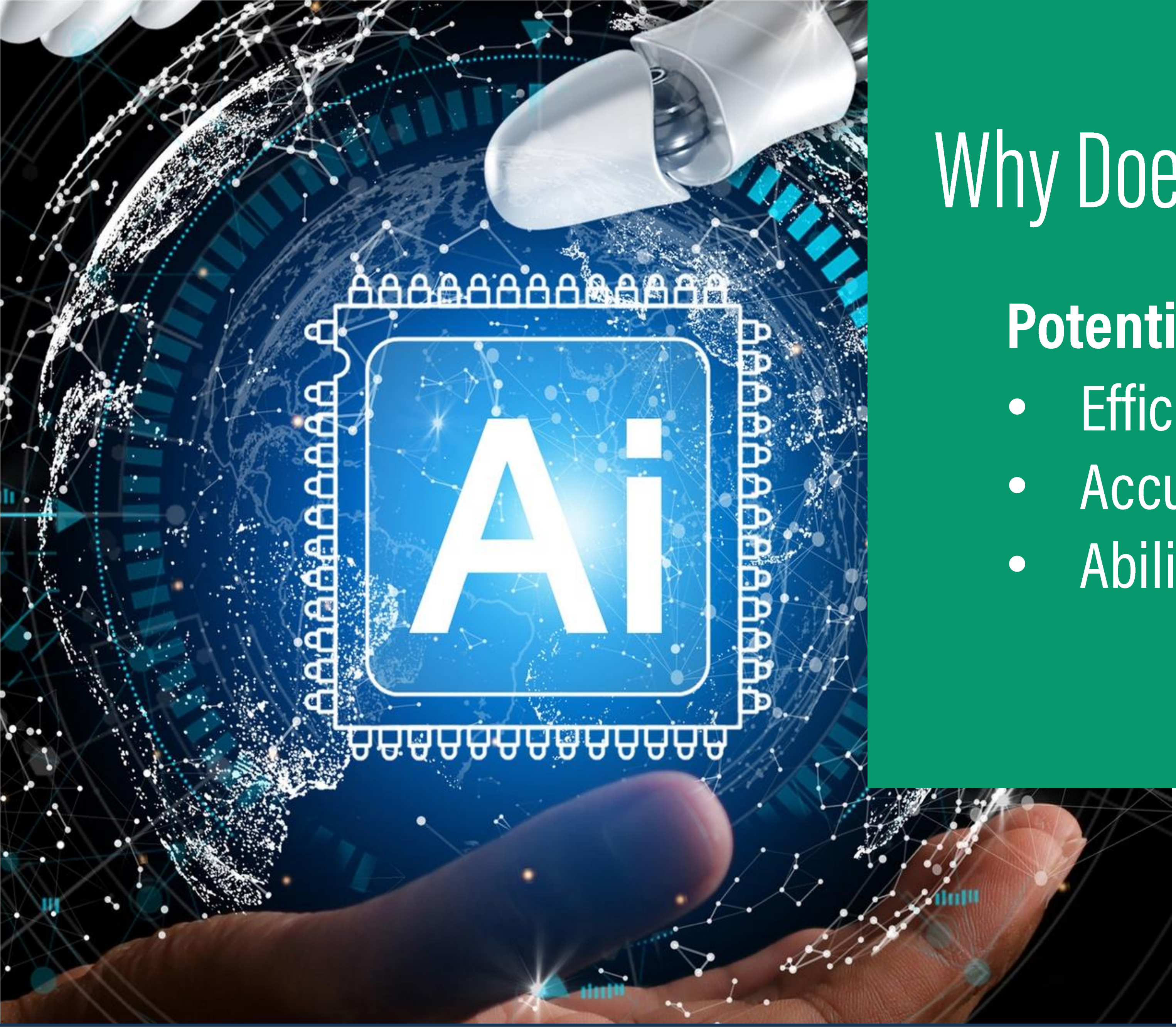
Larger Language Models

Natural Language Processing

Generative AI

Understanding AI Safety





Why Does AI **Safety Matter**

Potential benefits of AI:

- Efficiency
- Accuracy
- Ability to handle large datasets

Considerations

Importance of ethical AI:
Ensuring AI benefits all and does not harm

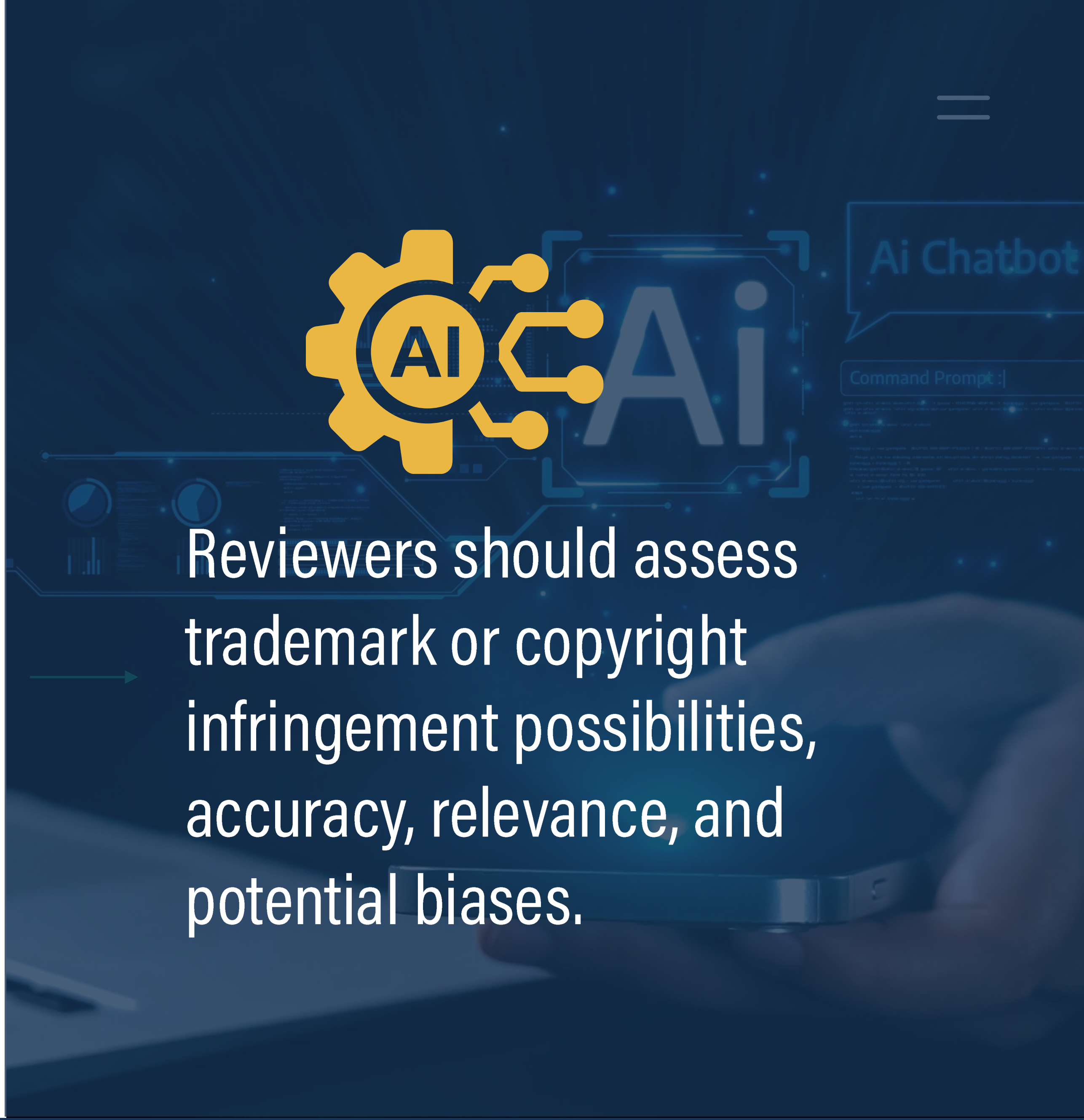
Examples

- ✓ Bias in AI algorithms affecting hiring processes
- ✓ Privacy issues with facial recognition technology

Key Safety Guidelines for Employees

Content **Generation**

As an AI user, you are required to review all AI-generated content before dissemination.



Reviewers should assess trademark or copyright infringement possibilities, accuracy, relevance, and potential biases.

Data Privacy & Security

You can only input publicly available data into AI tools.

The organization's confidential or sensitive data should NEVER be input into AI tools.

→

Educate yourself on safe data sharing practices & reach out to your IT or UMC Support for help.

→

As needed, implement encryption, access controls, and anonymization techniques.

Bias & Fairness

As an AI user

You need to ensure that the AI models you are using are trained on diverse and representative data.

You will regularly monitor and address any biases that emerge during AI

You will educate yourself about potential biases and limitations

Transparency & Accountability

Ensuring accountability in AI decision-making:

- Clear documentation of AI processes
- Users should understand how AI decisions are made
- Mechanisms for users to challenge AI decisions

Transparency & Accountability Cont.

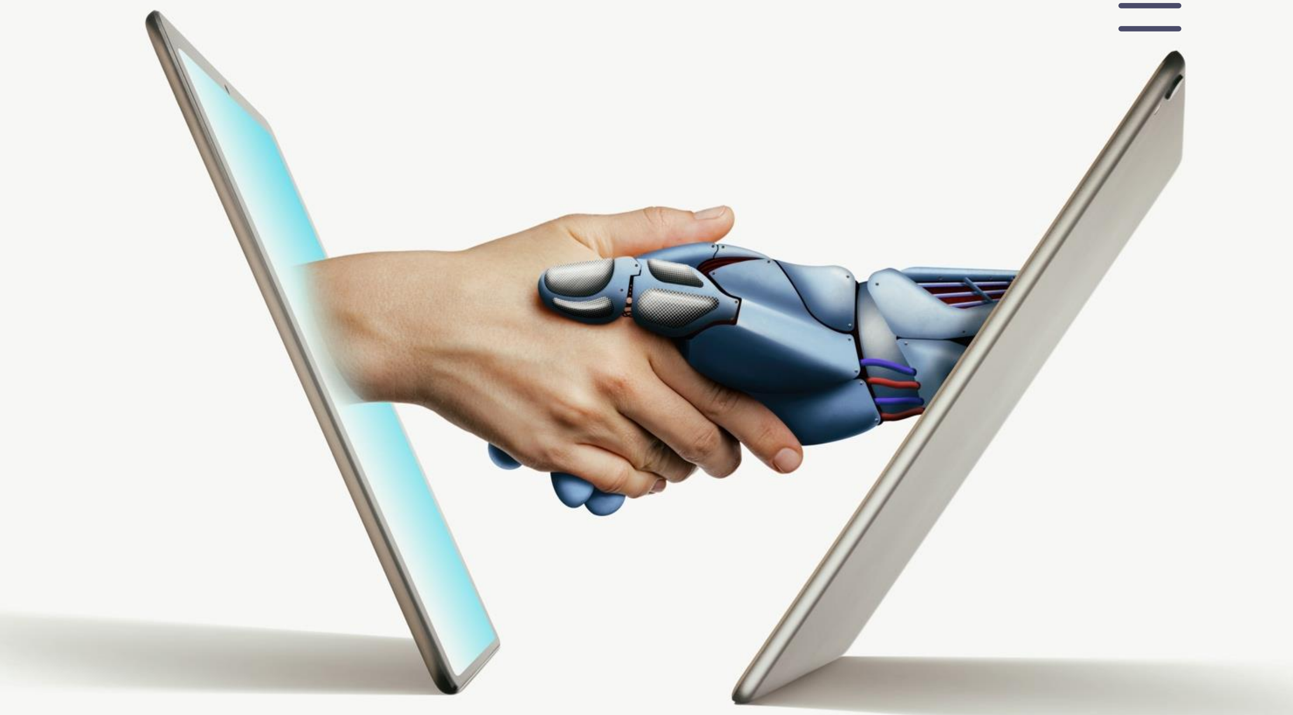
As an AI user, you are responsible for:

Clearly communicating when AI systems are in use.

Provide explanations for AI-generated decisions where feasible.

Maintaining an audit trail of your AI activities.

Implementing Safe **AI Practices**



Guidelines for safe AI implementation

- Leverage GCFA Artificial Intelligence Usage Rules Template
- Adherence to ethical guidelines
- Regular monitoring and evaluation of AI systems

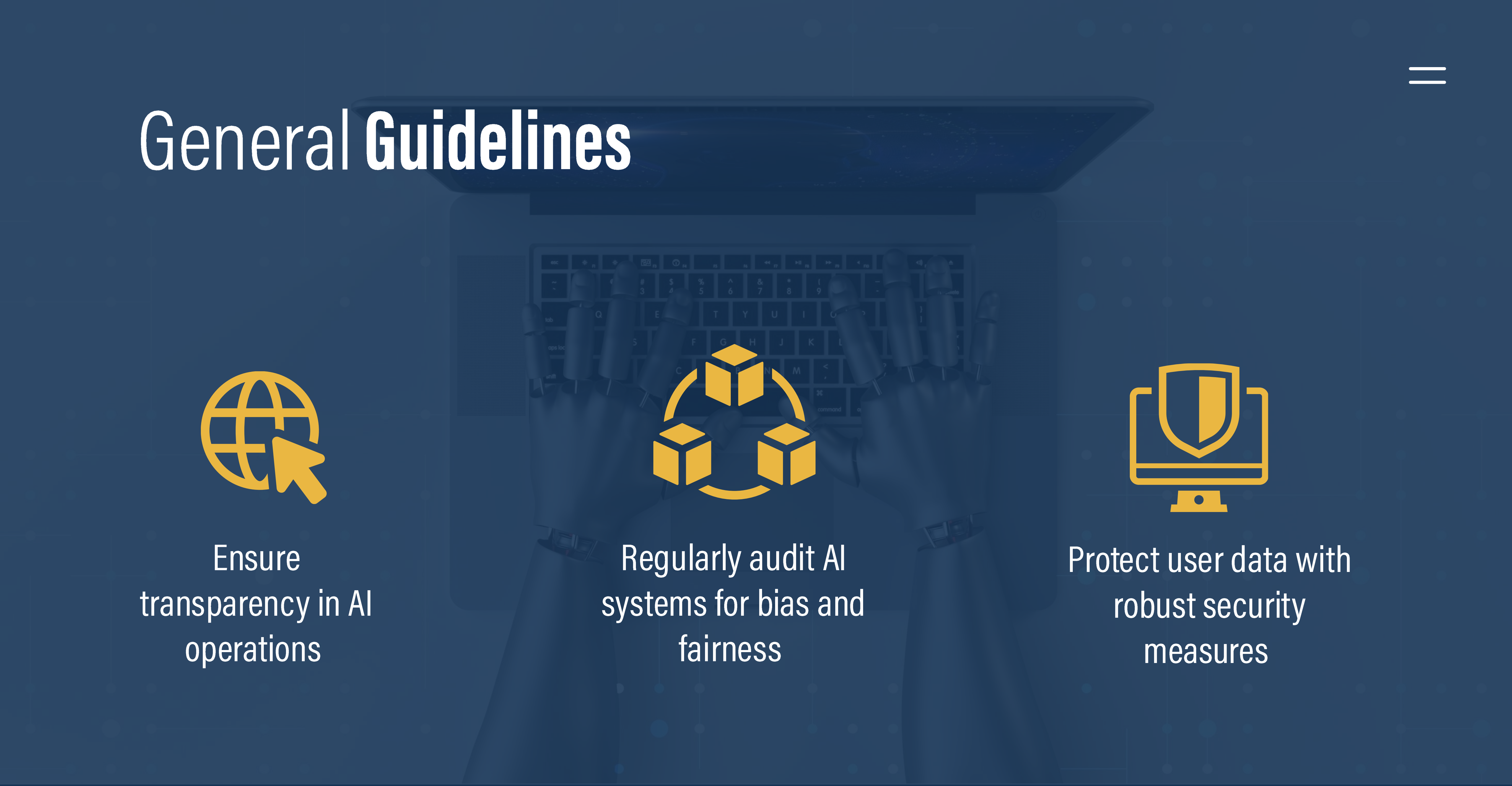
Role of administrators in ensuring AI safety:

Contract reviews of AI tools/products to understand how data is used

Setting policies for AI use

- Providing training and resources for staff

Best Practices For Ethical AI Use



General **Guidelines**

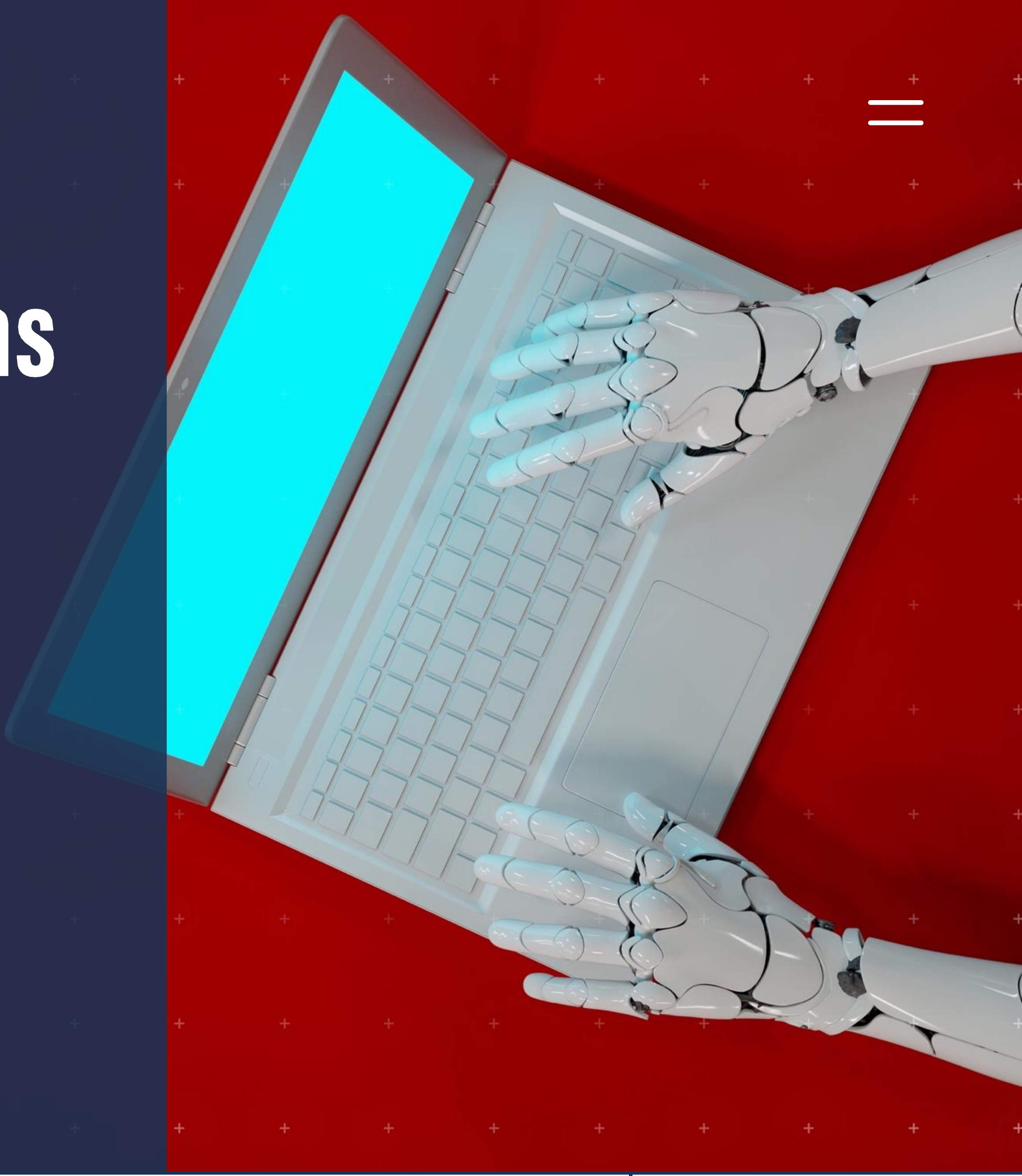
Ensure transparency in AI operations

Regularly audit AI systems for bias and fairness

Protect user data with robust security measures

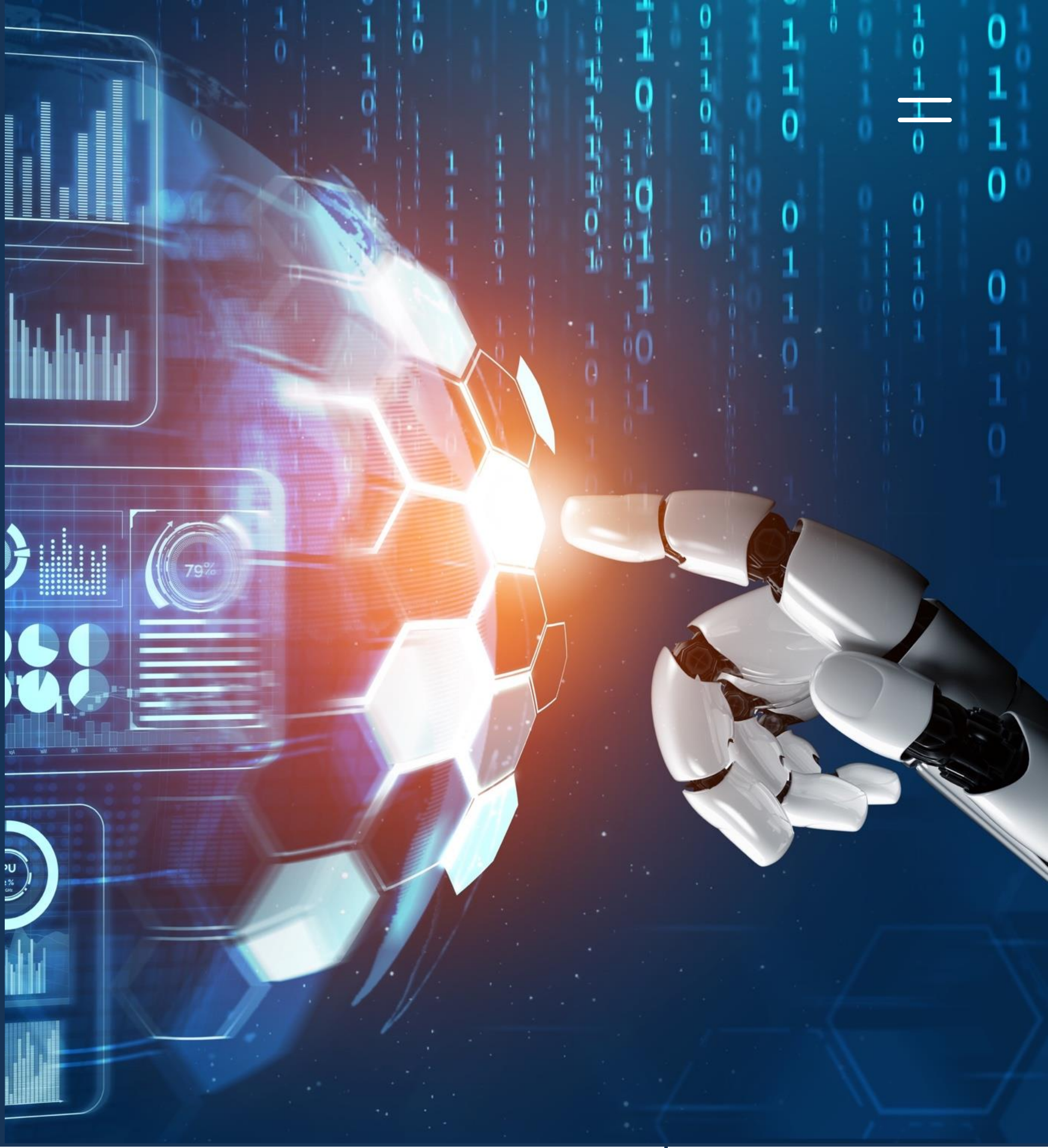
Specific Rules **For Organizations**

- ✓ **Develop and enforce an AI ethics policy**
- ✓ **Provide training on AI safety for all employees**
    - Establish a clear process for reporting and addressing AI-related issues



Promote **Inclusivity**

- ✓ Involve diverse teams in AI development
- ✓ Ensure AI systems are accessible to all users



Continuous **Improvement**

- ✓ Regularly update AI systems based on feedback and new research
- ✓ Stay informed about the latest developments in AI ethics and safety

Protecting Personal Data With Meeting Recording AI Tools

Best Practices **For Data Protection**

- Select Secure AI Tools
- Limit Access
- Educate Participants
- Monitor Activity
- Update Software

Questions?

Agenda

- AI Safety (30 minutes)
- Technology Security Considerations
  - Module 2: Internet Access & Safety (10 minutes)
  - Module 3: Computer Safety (10 minutes)
  - Module 4: Email & File Security (10 minutes)
  - Module 5: Cloud Apps & Third-Parties (10 minutes)
  - Module 6: Privacy & Data Security (10 minutes)
  - BONUS: Security Awareness Training (10 minutes)

We ALL must protect UMC from data loss due to misuse, disclosure, fraud or destruction

What's at **Risk?**

Data Breach & Data Loss

Diminished Ministry Services

Negative Financial Impact

Consulting Services

Cybersecurity Assessment

01 Identify and assess vulnerabilities in the organization’s data and information assets.

02 Provide actionable recommendations to mitigate identified risks.

03 Develop and implement cybersecurity policies and procedures.

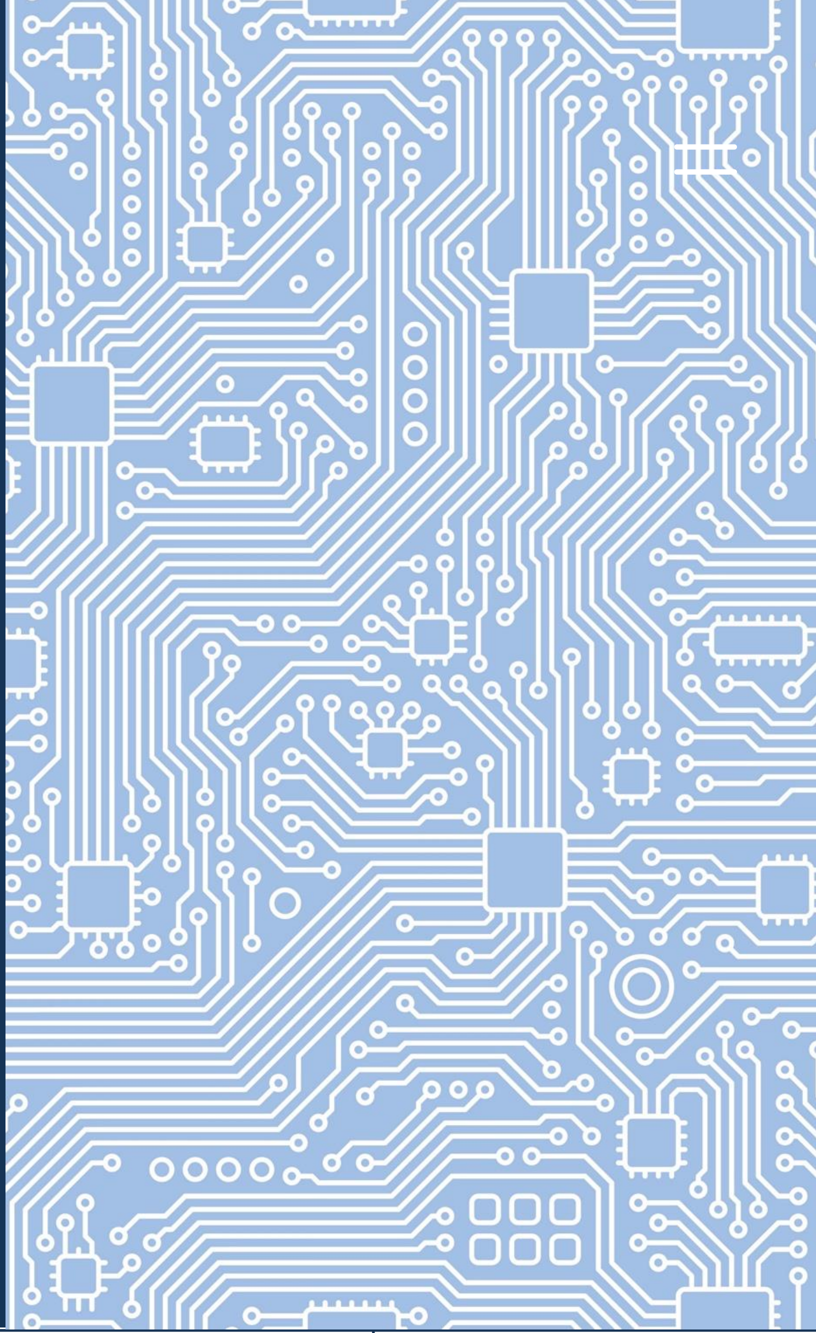
04 Enhance the organization’s ability to identify, protect, detect, respond to, and recover from cybersecurity incidents.

UMC SUPPORT INFORMATION TECHNOLOGY

Technology Policy Manual:

- Technology Acceptable Use
- Artificial Intelligence
- Access Control
- Incident Response
- Awareness and Training
- Data Retention
- Others TBD

Module 2: Internet Access & Safety



How do you **Connect?**

From Office

From Home

Public Wi-Fi / Hot Spot

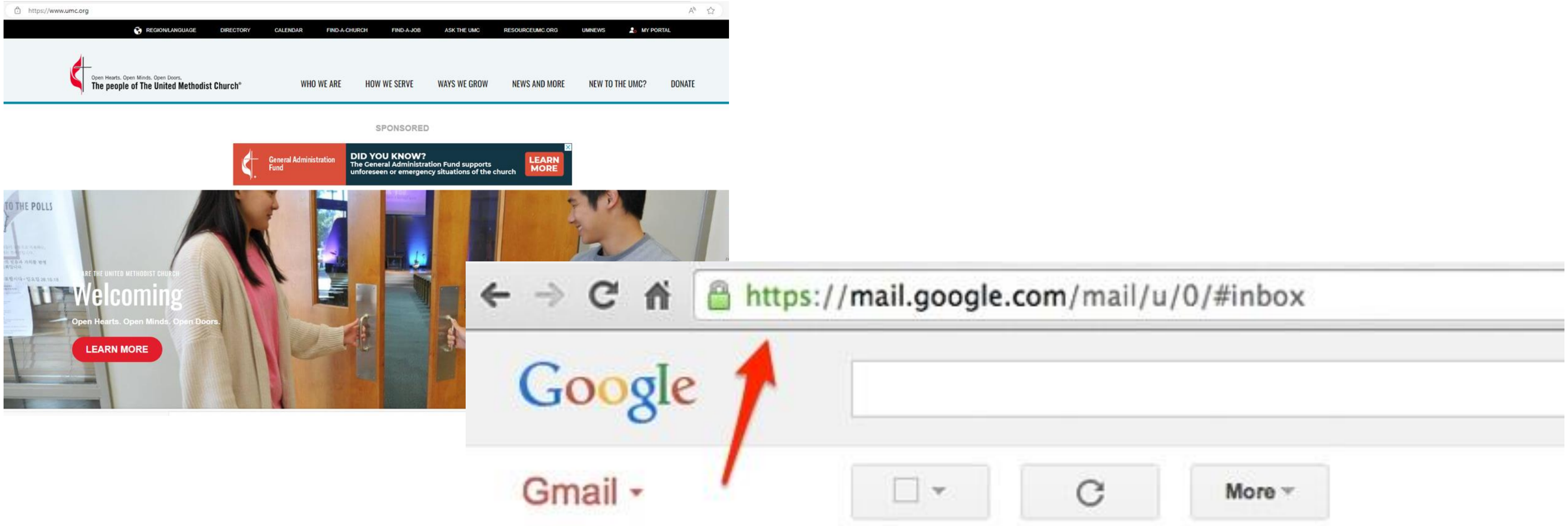
Safety Step 1: Use Encryption

What is Encryption?

Encryption protects data transmitted over the internet by converting it into a secure format that can only be read by authorized users.

Data & Info - Encryption

What is Encryption? https://www.youtube.com/watch?v=ySP-dvcOgas



https://www.umc.org

Open Hearts. Open Minds. Open Doors.
The people of The United Methodist Church®

SPONSORED

General Administration Fund

DID YOU KNOW?
The General Administration Fund supports unforeseen or emergency situations of the church

ARE THE UNITED METHODIST CHURCH
Welcoming
Open Hearts. Open Minds. Open Doors.

https://mail.google.com/mail/u/0/#inbox

Secure Wi-Fi

Best Practices

Private / Secured Networks

Wired (Blue Wire)

Authenticate via certificate (GCFA)

Authenticate via password – WPA2 (Admin)

Private Home Network

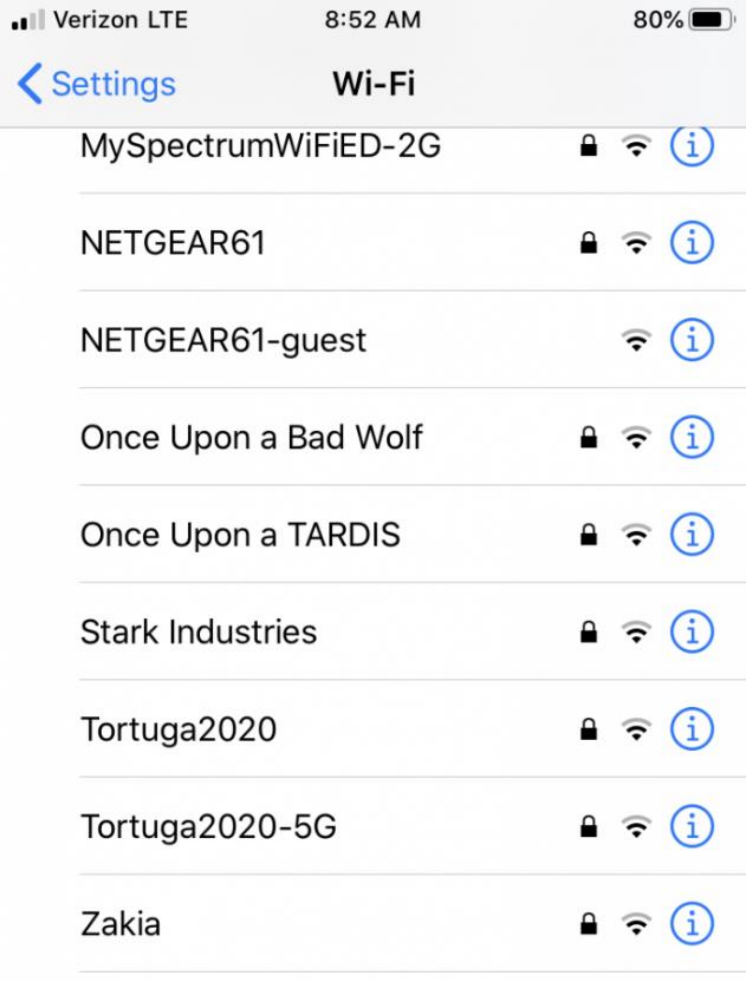
Use WPA2

Use a strong password for your encryption key, such as a combination of letters and numbers of 14 characters or more. Change the default network name and password on your router

Hot Spot

Enable strong encryption on your hotspot: WPA2 w/password

- Change Default Network Name
- Enable Network Encryption
- Create a Strong Password
- Disable WPS
- Set Up a Guest Network
- Regularly Update Passwords



Verizon LTE 8:52 AM 80%

Settings Wi-Fi

MySpectrumWiFiED-2G 🔒

NETGEAR61 🔒

NETGEAR61-guest

Once Upon a Bad Wolf 🔒

Once Upon a TARDIS 🔒

Stark Industries 🔒

Tortuga2020 🔒

Tortuga2020-5G 🔒

Zakia 🔒

Public / Unsecured Networks

- Public Wi-Fi is inherently insecure – so be cautious.
- Treat all Wi-Fi links with suspicion - Don’t connect to an unknown or unrecognized SSIDs
- Consider using your cellular service instead of public Wi-Fi

Recommendations:

- Protect your device against cyberattacks - anti-malware, updates, patches
- Turn off sharing – Control Panel>Network and Internet>Network and Sharing Center – Change Advanced Sharing Settings
- Enable a firewall – Windows Firewall for non-UMC devices

Use a VPN (virtual private network) - Creates a ‘private tunnel’ that encrypts your data

Upgrade Firmware

What is Firmware?

Firmware is the software that is embedded in your router, switch, firewall, access point, gateway, etc. controlling its functions and operations.

Think of it as the operating system for the equipment used to connect to the Internet, like how Windows or macOS operates on your computer.

Why Update Firmware?

- Firmware updates provide security patches, performance improvements, and new features.
- Many routers provided by Internet Service Providers automatically perform updates.

UMC SUPPORT INFORMATION TECHNOLOGY

Network Services

Enterprise Grade Equipment:

- Utilizes enterprise-grade networking equipment
- Reduces downtime
- Minimizes network congestion

Offer equipment at discounted rates due to bulk buying power

Financing Available

cisco Meraki

UniFi

Hewlett Packard Enterprise

FORTINET

paloalto NETWORKS

Services:

- Perform a Network Assessment to determine security enhancements and/or equipment upgrades ($250)
- Established on-call technical a support channel for staff to ask questions and get help.
- Offers proactive advanced monitoring.

Questions?

Module 3: Computer Safety

Computer Question:

What kinds of computers do you use?

Mac / iOS

Windows

Other

Computer Equipment Types

Keep Safe from Theft/Loss
Erase / Wipe Prior to Disposal

Windows
Mac

USB Stick

SD Cards

iPhone
iPad

Multi-Function Printers

Recommended Equipment Link

No Windows Home
Be careful w/Amazon
More than 250 GB storage

Android
Floppy Disk

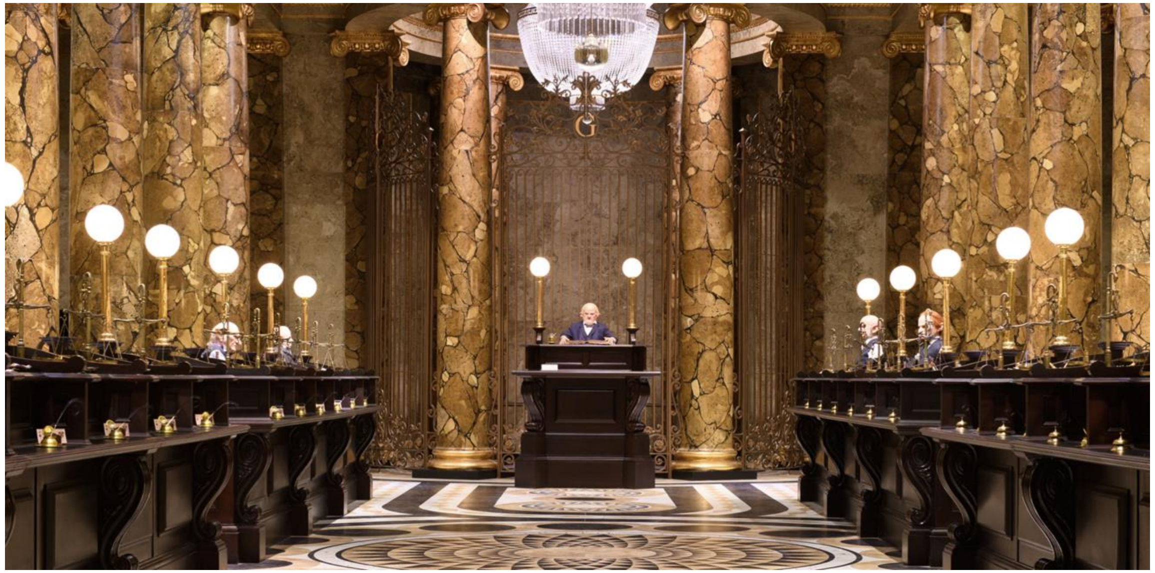
Using personal equipment
is highly discouraged

Understanding Disk Encryption

Ensuring that sensitive data on computers remains secure and protected

- **What is Disk Encryption?**
    - Protects the data on your computer by converting it into a code that cannot be easily read by unauthorized people.
    - Even if someone steals your computer, they won't be able to access your files without the encryption key or password.
- **Why is Disk Encryption Important?**
    - Protects Sensitive Information
    - Prevents Unauthorized Access
    - Compliance
- **Enable Disk Encryption on Windows (Using BitLocker)**
- **Enable Disk Encryption on Mac (Using FileVault)**

- **Best Practices for Disk Encryption**
    - Use Strong Passwords
    - Keep Recovery Keys Safe
    - Regular Backups
    - Stay Updated

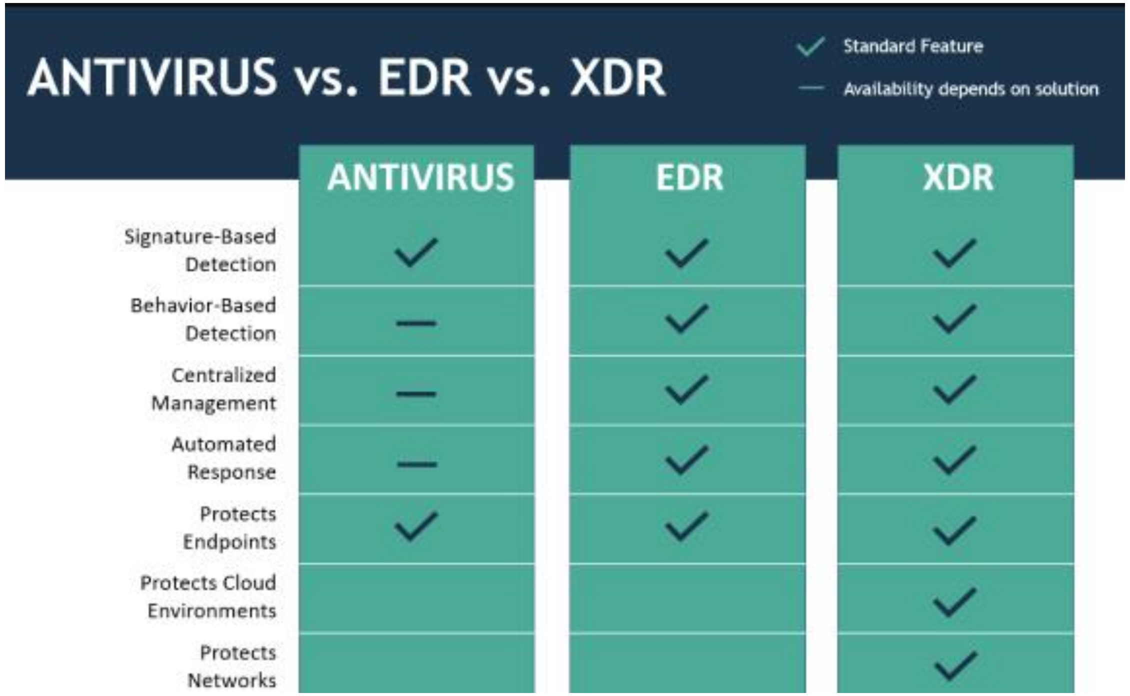


Anti-Virus Software

Windows & Mac Computers

What is Anti-Virus Software?

Anti-virus software helps protect your computer from viruses, malware, and other cyber threats.



ANTIVIRUS vs. EDR vs. XDR

✓ Standard Feature

— Availability depends on solution

	ANTIVIRUS	EDR	XDR
Signature-Based Detection	✓	✓	✓
Behavior-Based Detection	—	✓	✓
Centralized Management	—	✓	✓
Automated Response	—	✓	✓
Protects Endpoints	✓	✓	✓
Protects Cloud Environments			✓
Protects Networks			✓

What is Endpoint Detection and Response (EDR)

Also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

What is Advanced Malware Protection (XDR)?

Extended Detection and Response (XDR) is an advanced security solution that provides comprehensive protection against sophisticated cyber threats.

Benefits of XDR

- Detects and responds to threats across multiple endpoints.
- Provides advanced threat intelligence and analytics.
- Enhances overall security posture.

Steps to Implement XDR

- Choose a Reputable XDR Solution
- Consult with IT Professionals
- Monitor and Respond

Automatic Updates

Windows Computers

Enable Automatic Updates for Windows:

- Open Settings: Click on the Start menu and select Settings (the gear icon).
- Go to Update & Security: In the Settings window, click on Update & Security.
- Windows Update: Select Windows Update from the left-hand menu.
- Advanced Options: Click on Advanced options.
- Automatic Updates: Under Choose how updates are installed, select **Automatic (recommended).** This ensures that updates are downloaded and installed automatically.

Enable Automatic Updates for Applications:

- Microsoft Store Apps:
- Open the Microsoft Store.
- Click on the three dots in the upper-right corner and select Settings.
- Toggle the switch under Update apps automatically to On.

Say Goodbye to Windows 10

Automatic Updates

Mac Computers

Enable Automatic Updates for macOS:

- Open System Settings: Click on the Apple menu in the top-left corner and select System Settings.
- Go to Software Update: Click on General in the sidebar, then select Software Update.
- Automatic Updates: Click the i button next to Automatic Updates.
- Turn on the options you want:
    - Download new updates when available
    - Install macOS updates
    - Install application updates from the App Store
    - Install Security Responses and system files

Enable Automatic Updates for Applications:

- Open the App Store.
- Click on App Store in the menu bar and select Preferences.
- Check the box for Automatic Updates to ensure apps are updated automatically.

Resources

Managed Workstation Service:

- Anti-virus Software
- Advanced Malware Protection (XDR)
- Automated Operating System & Application Patching (Windows & Mac)
- Remote Access for Support Troubleshooting

$4.99 / device / month

UMC INFORMATION TECHNOLOGY SUPPORT

Equipment Sales and Configuration:

Save money by leveraging our discounts on computer equipment, benefiting from economies of scale.

- Assist with initial set up and configuration.

Service Desk:

Established US-based support channel for staff and volunteers to ask questions and get help.

New User Setup and Terminations

Hours: 7:30 AM - 5:30 PM CST, Monday to Friday

24/7 on-call support available

Questions?

Module 4:
Cloud Applications
& Third-Party Safety

Apps Question:

What kinds of apps do you use?

Operations Management

Billing / Accounting & Finance

Productivity

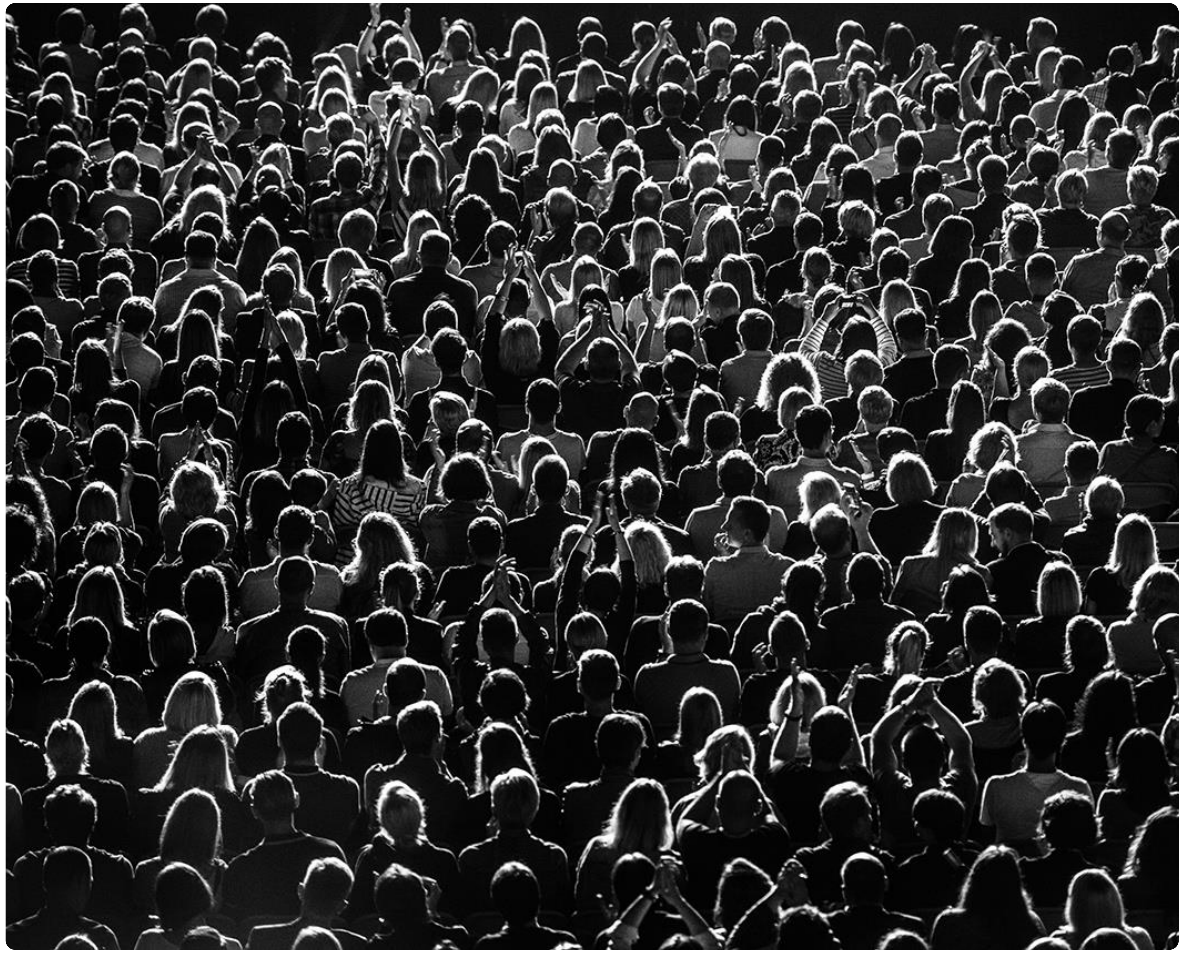
Cloud Services & 3rd Parties

Microsoft 365
churchtrac
realm
CHROMERIVER
planning center
aplos
breeze
Microsoft Dynamics™ GP
INTUIT quickbooks
shelbysystems®
Church Management Software

Safety Steps:

- Verify Security (via SOC-2)
- Breach Notification Terms
- Ensure Data is Encrypted
- Actively Manage Access
- Use MFA (multi-factor authentication)

UMC Support Resources



Buying Power:

Ministry Partner Program | General Council on Finance and Administration

Module 5:
Email & File Security

Email / File Question:

What do you use for email & file storage?

Microsoft 365

Google

Other

Email Security: Best Practices

All conference-related email communication is conducted via a “named” organizational email address.

Only use:
John.Wesley@campallen.org
jwesley@campallen.org
john@campallen.org

Don’t use:
office@campallen.org
officecampallen@hotmail.com
johnny1735@gmail.com

Multi-Factor Authentication

What is Multi-Factor Authentication (MFA)?

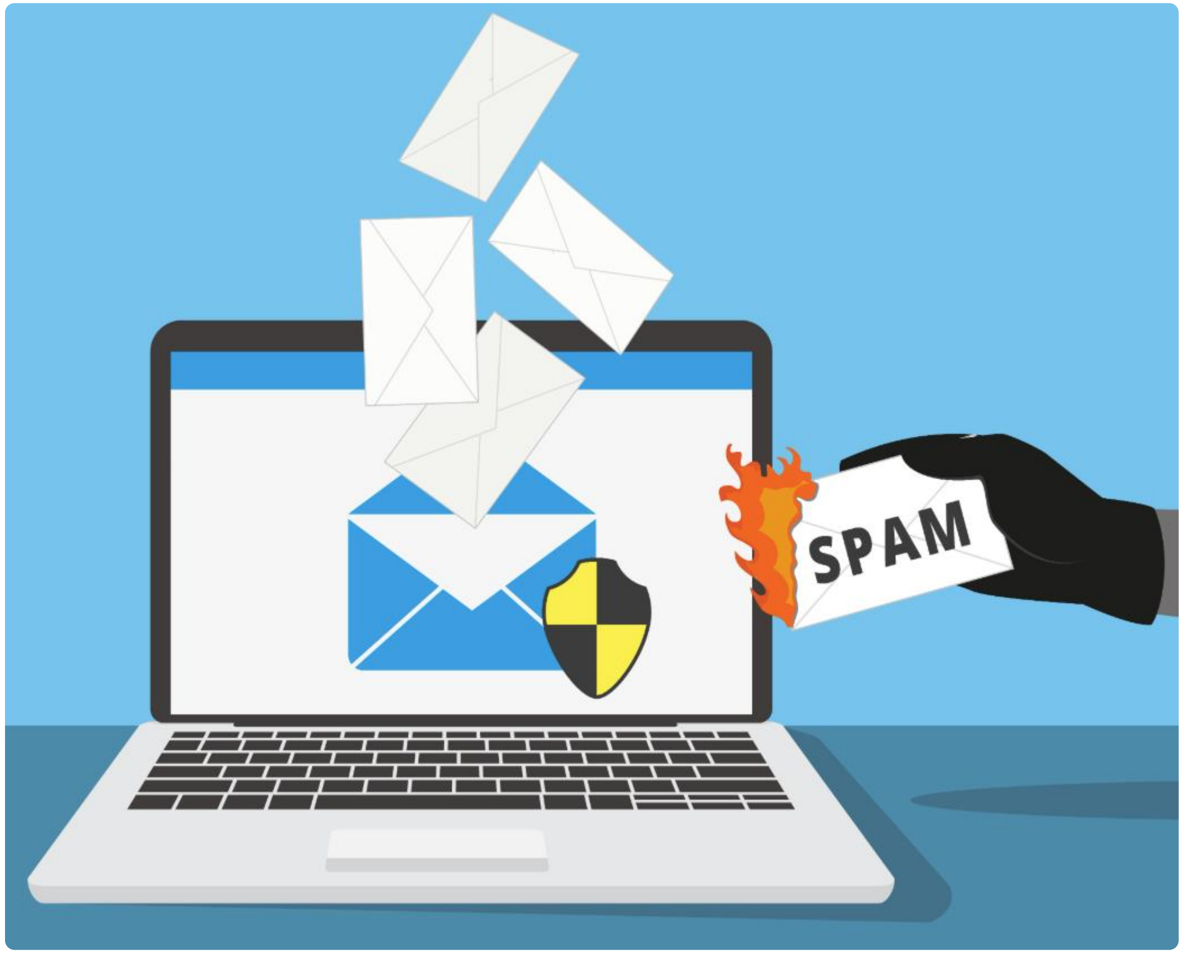
- Multi-Factor Authentication (MFA) is a security system that requires more than one method of verification to access an account. This adds an extra layer of protection beyond just a password.

Why is MFA Important?

- Enhanced Security: Even if someone gets your password, they can’t access your account without the second verification method.
- Protection Against Cyber Threats: Reduces the risk of unauthorized access and data breaches.

Email Security

More Best Practices



• Quarterly Account Review

- ALL email accounts use multi-factor authentication
- Electronic communication should be written assuming it will become a company record.
- Always correctly identify the sender's identity as email addresses are easily spoofed.
- Email queries for personally identifiable information should always be verified via another means prior to responding.
- Use extreme caution when communicating confidential or sensitive information. Keep in mind that all electronic and voice messages sent outside of the organization become the property of the receiver. Consider not communicating anything that you wouldn't feel comfortable being made public.
- Treat email attachments or links that have been sent unsolicited with extreme caution, especially if the sender is unknown. Viruses are often sent this way.
- Do regular phishing tests and security awareness training.

File Access & Passwords

- All access to information systems is granted/revoked TIMELY on a prescribed basis via a formal procedure.
- Restrict access to least privilege
- Protect the confidentiality of account and password information.
- Reset your password immediately if you have reason to believe that any unauthorized person has learned your password.
- Consider using a password manager
- **Use Multi-factor authentication**

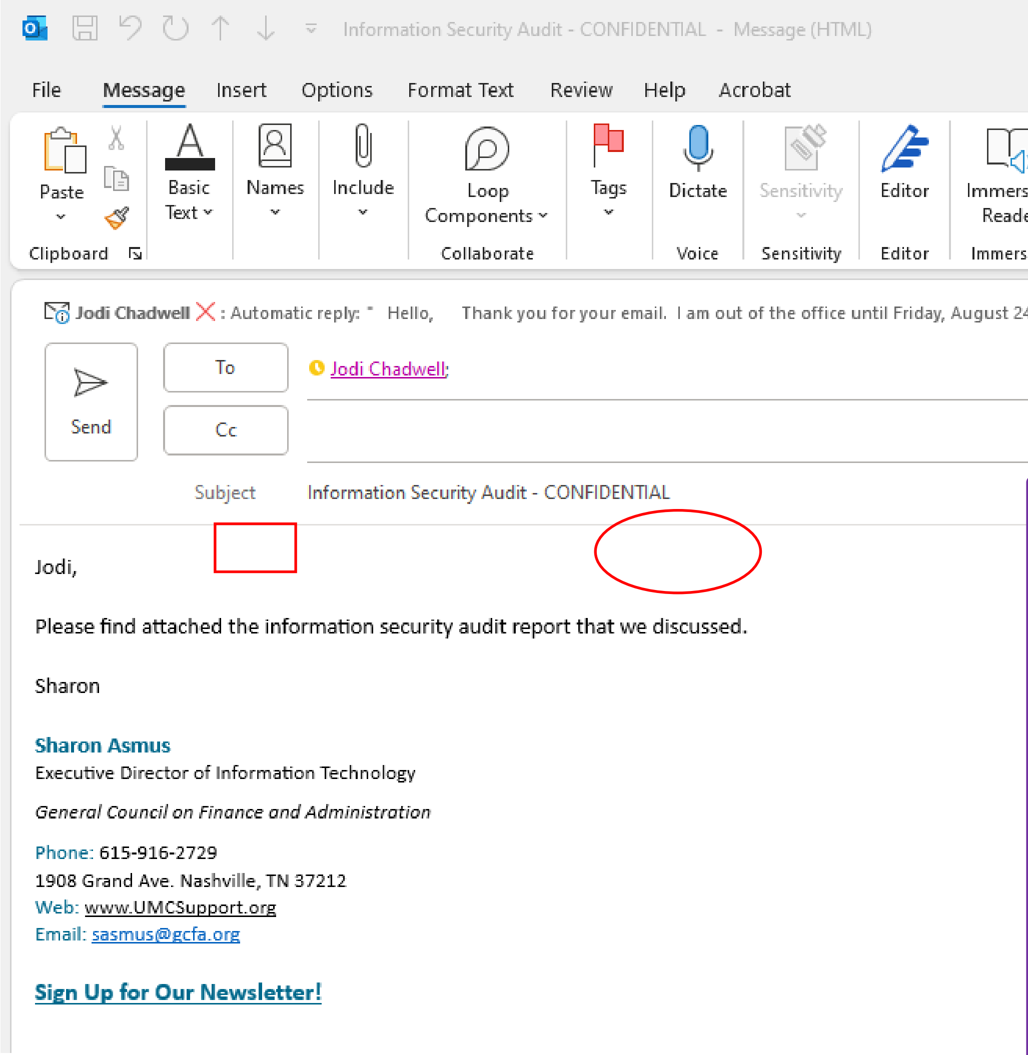
https://youtu.be/opRMrEfAliI

Data & Info – Email

<u>NOT</u> all email is secure.

Least secure email providers:

- Yahoo Mail
- AOL Mail
- Gmail
- Outlook
- Apple Mail



Jodi Chadwell ✕ : Automatic reply: " Hello, Thank you for your email. I am out of the office until Friday, August 24 assisting with the meeting logist...

To: Jodi Chadwell;

Subject: Information Security Audit - CONFIDENTIAL

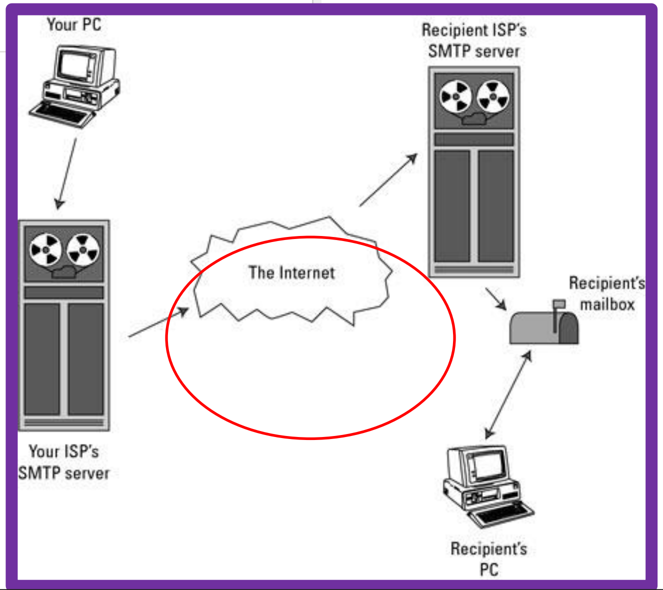
Jodi,

Please find attached the information security audit report that we discussed.

Sharon

Sharon Asmus
Executive Director of Information Technology
General Council on Finance and Administration
Phone: 615-916-2729
1908 Grand Ave. Nashville, TN 37212
Web: www.UMCSupport.org
Email: sasmus@gcfa.org

Sign Up for Our Newsletter!



Cloud File Storage

√

256-bit AES (Advanced Encryption Standard)= uncrackable

Name	Encryption At Rest
Local Drives (C)	?
Microsoft OneDrive	√
DropBox	√
Google Drive	√
iCloud	√
iCloud KeyChain	√

Tips & Tricks:

Enable two-step verification or multi-factor authentication

Double-check file sharing settings (are all folders public?)

Ensure timely user access controls (e.g., new hire access, promotions, terminations).

File Organization

Consistent Naming Conventions

- Use clear and consistent naming conventions for files and folders.
- Include dates and descriptive titles to make files easy to identify.

Folder Structure

- Create a logical folder structure that mirrors your church's organizational hierarchy.
- Use subfolders to further categorize files by project, event, or department.

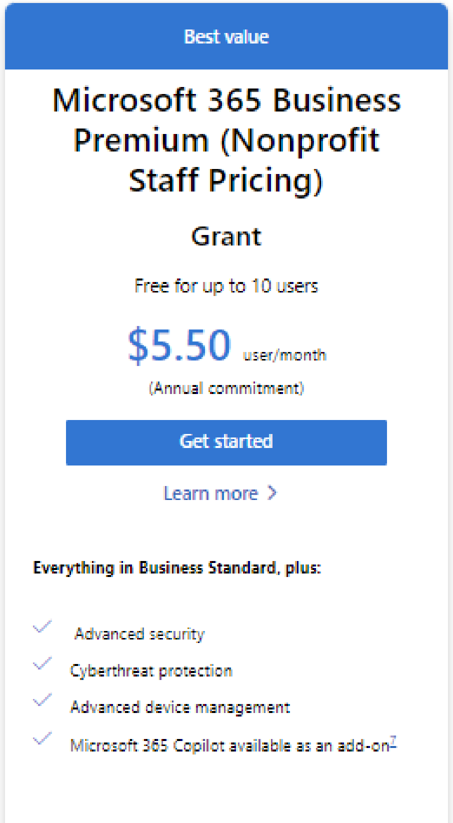
Version Control

- Enable version control in SharePoint to keep track of changes to documents.
- Restore previous versions if needed.

Organize your files in OneDrive - Microsoft Support

Email Security: Microsoft Email

10 FREE Microsoft 365 Business Premium licenses (Nonprofit Staff Pricing)



Best value

Microsoft 365 Business Premium (Nonprofit Staff Pricing)

Grant

Free for up to 10 users

$5.50 user/month

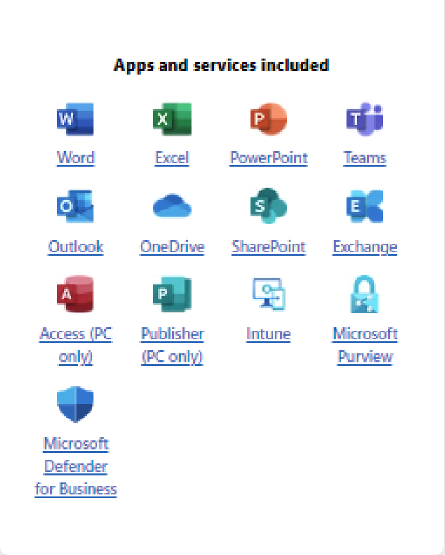
(Annual commitment)

Get started

Learn more >

Everything in Business Standard, plus:

- ✓ Advanced security
- ✓ Cyberthreat protection
- ✓ Advanced device management
- ✓ Microsoft 365 Copilot available as an add-on[2]



Apps and services included

Word, Excel, PowerPoint, Teams, Outlook, OneDrive, SharePoint, Exchange, Access (PC only), Publisher (PC only), Intune, Microsoft Purview, Microsoft Defender for Business

Consider using Non-Profit Microsoft 365

https://nonprofit.microsoft.com/en-us/getting-started#

Options for set up & config:

- UMC Technology Support is a Microsoft partner

  -1x1 “Phone a Friend” Support Services*

  -Training class with detailed instructions

- On your own leveraging online tools:

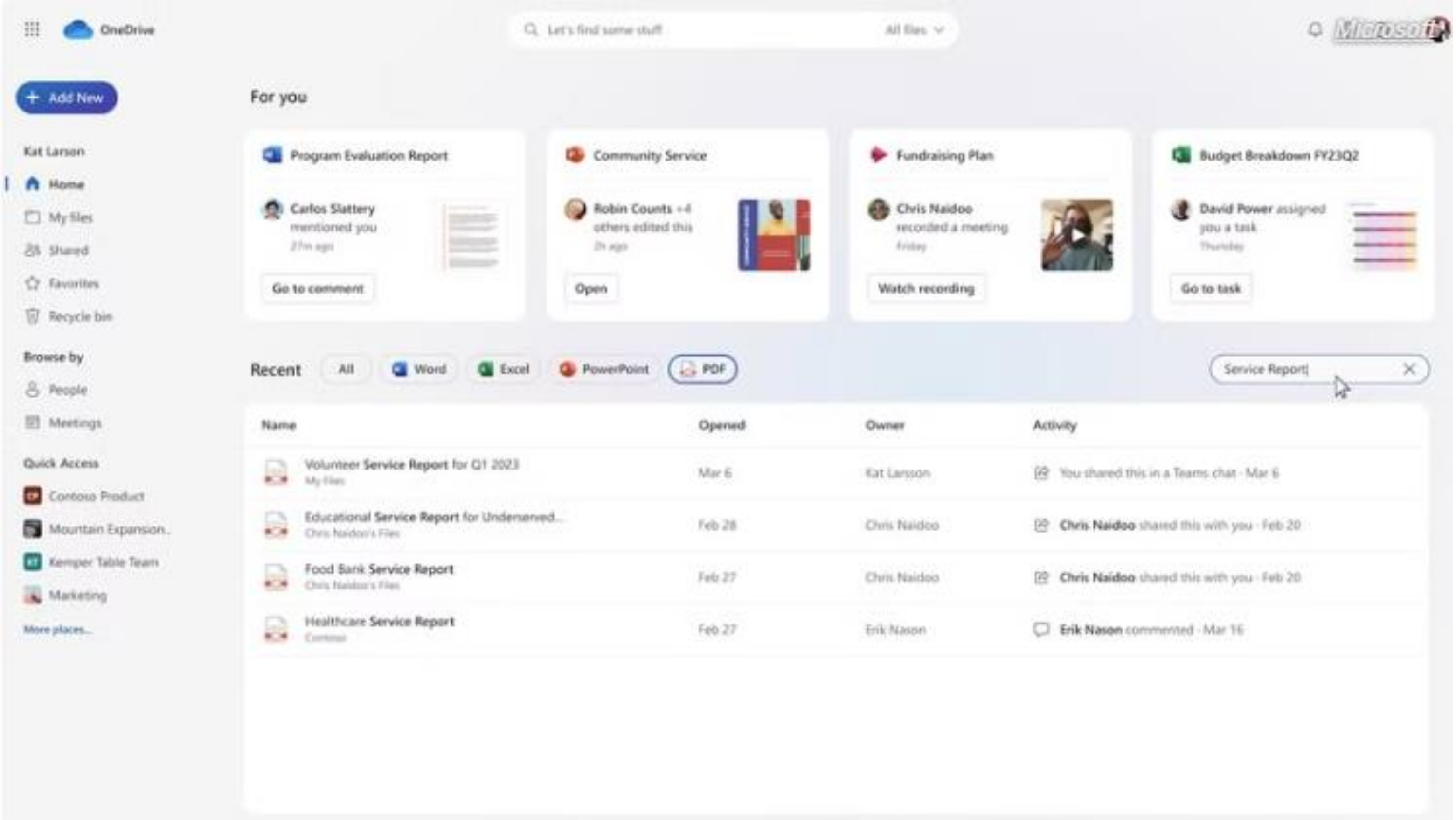
  https://www.microsoft.com/en-us/nonprofits

*Requires no-obligation support services contract

Microsoft OneDrive

Used for each person to store their individual staff files

- Access OneDrive through your Microsoft 365 account.
- Create folders for different departments or projects.
- Upload files by dragging and dropping them into the appropriate folders.
- Share files with specific individuals or groups by using the "Share" feature.

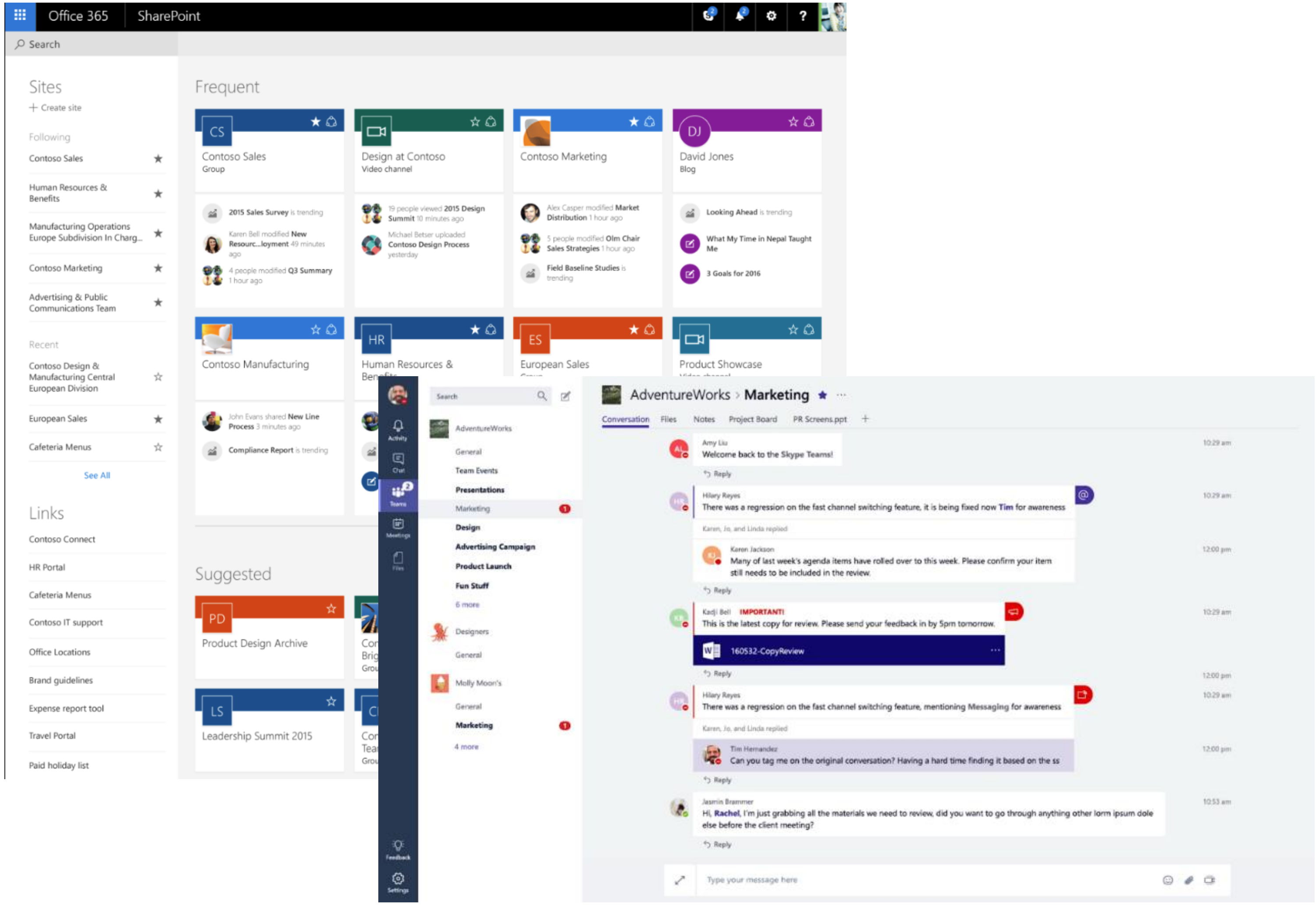


Name	Opened	Owner	Activity
Volunteer Service Report for Q1 2023 My Files	Mar 6	Kat Larsson	You shared this in a Teams chat · Mar 6
Educational Service Report for Underserved... Chris Naidoo's Files	Feb 28	Chris Naidoo	Chris Naidoo shared this with you · Feb 20
Food Bank Service Report Chris Naidoo's Files	Feb 27	Chris Naidoo	Chris Naidoo shared this with you · Feb 20
Healthcare Service Report Contoso	Feb 27	Erik Nason	Erik Nason commented · Mar 16

Microsoft SharePoint & Teams

Used to store shared files

- Access SharePoint & Teams through your Microsoft 365 account.
- Create a new site for your church or specific area (e.g., preschool).
- Set up document libraries within the site to organize files.
- Upload files and set permissions to control who can view or edit them.



Amy Liu 10:29 am
Welcome back to the Skype Teams!

Hilary Reyes 10:29 am
There was a regression on the fast channel switching feature, it is being fixed now Tim for awareness

Karen, Jo, and Linda replied

Karen Jackson 12:00 pm
Many of last week's agenda items have rolled over to this week. Please confirm your item still needs to be included in the review.

Kadji Bell IMPORTANT! 10:29 am
This is the latest copy for review. Please send your feedback in by 5pm tomorrow.

160532-CopyReview

12:00 pm

Hilary Reyes 10:29 am
There was a regression on the fast channel switching feature, mentioning Messaging for awareness

Karen, Jo, and Linda replied

Tim Hernandez 12:00 pm
Can you tag me on the original conversation? Having a hard time finding it based on the ss

Jasmin Brammer 10:53 am
Hi, Rachel, I'm just grabbing all the materials we need to review, did you want to go through anything other lorm ipsum dole else before the client meeting?

Staff Transitions

Transferring Files

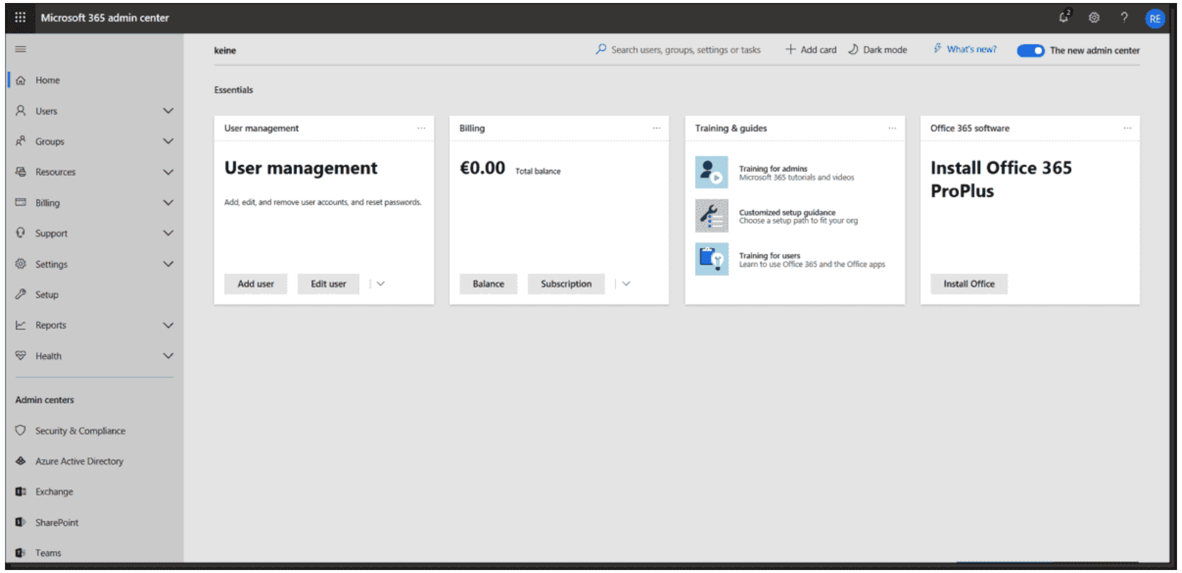
- Before a staff leaves, ensure all relevant files are transferred to the centralized OneDrive or SharePoint location.
- Use the "Move to" or "Copy to" features to transfer files between OneDrive and SharePoint.

Access Management

- Update permissions to remove access for departing staff or volunteers.
- Grant access to new staff or volunteers as needed.

Archiving

- Archive old files that are no longer actively used but need to be retained for record-keeping.
- Delete files no longer needed.



User management

User management

Add, edit, and remove user accounts, and reset passwords.

Billing

€0.00 Total balance

Training & guides

Training for admins
Microsoft 365 tutorials and videos

Customized setup guidance
Choose a setup path to fit your org

Training for users
Learn to use Office 365 and the Office apps

Office 365 software

Install Office 365 ProPlus

Office 365 management tasks - video training - Microsoft Support

Resources

Online Training

- Microsoft Learn: Introduction to SharePoint and OneDrive
- Microsoft Learn: Training and Change Management for SharePoint and OneDrive
- Microsoft Learn: OneDrive Documentation
- Microsoft 365 for business security best practices - Microsoft 365 Business Premium | Microsoft Learn

UMC INFORMATION TECHNOLOGY SUPPORT

- Assist with initial set up and configuration.
- Establish a support channel for staff and volunteers to ask questions and get help with OneDrive and SharePoint.
- Offers service desk hours for personalized assistance.

Questions?

Module 5: Data Privacy

Data & Info Security

Data is typically comprised of four classifications of information:

- Public/Unclassified
  - generally available to anyone within or outside of the organization

- Private
  - info. kept within the org, can’t be distributed outside of the org.

- **Confidential**
  - **potentially damaging if released (e.g., HR or payroll data, SSN)**

- **Secret/Restricted**
  - **harmful to UMC if leaked (e.g., legal documents, financial reports)**

Data Privacy

Best Practices

Key Principles of Data Privacy

Minimization: Collect only what’s necessary.

Consent: Always get permission before collecting or sharing data.

Security: Use strong passwords, encryption, and secure storage.

Access Control: Limit access to authorized personnel only.

UMC Support Resources

Sample UMC Privacy Policies

- Privacy Policy | GCFA
- United Methodist Partners Privacy Policy | UMC.org
- East Ohio Conference of The United Methodist Church
- Policies and Practices - Don Lee Camp and Retreat Center

UMC INFORMATION TECHNOLOGY SUPPORT

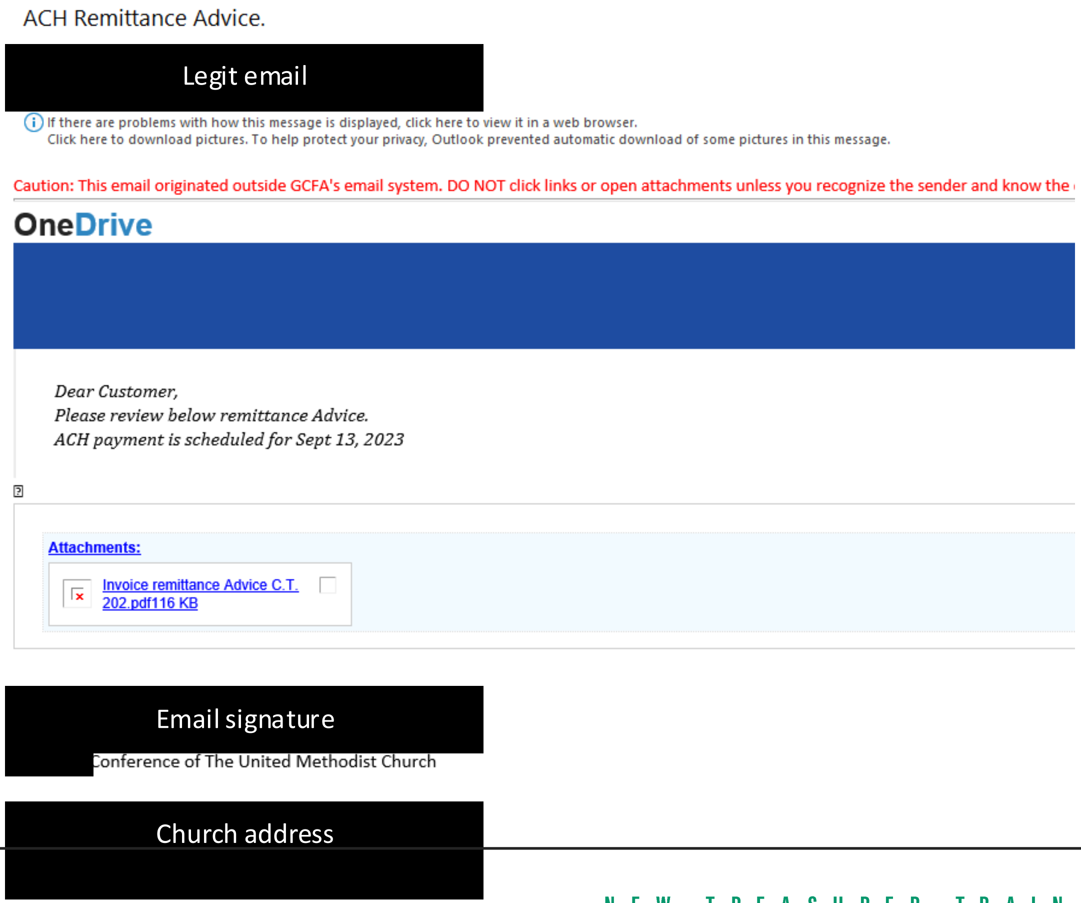
Consulting Services

- Assist with privacy policy creation.
- Assist staff with drafting & implementing procedures to support the privacy policy.

Bonus: Security Awareness Training

Security Awareness Training

Did you know that *91%* of successful data breaches started with an email?



ACH Remittance Advice.

Legit email [redacted]

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Caution: This email originated outside GCFA's email system. DO NOT click links or open attachments unless you recognize the sender and know the

OneDrive

Dear Customer,
Please review below remittance Advice.
ACH payment is scheduled for Sept 13, 2023

Attachments:

Invoice remittance Advice C.T. 202.pdf116 KB

Email signature [redacted]

[redacted] Conference of The United Methodist Church

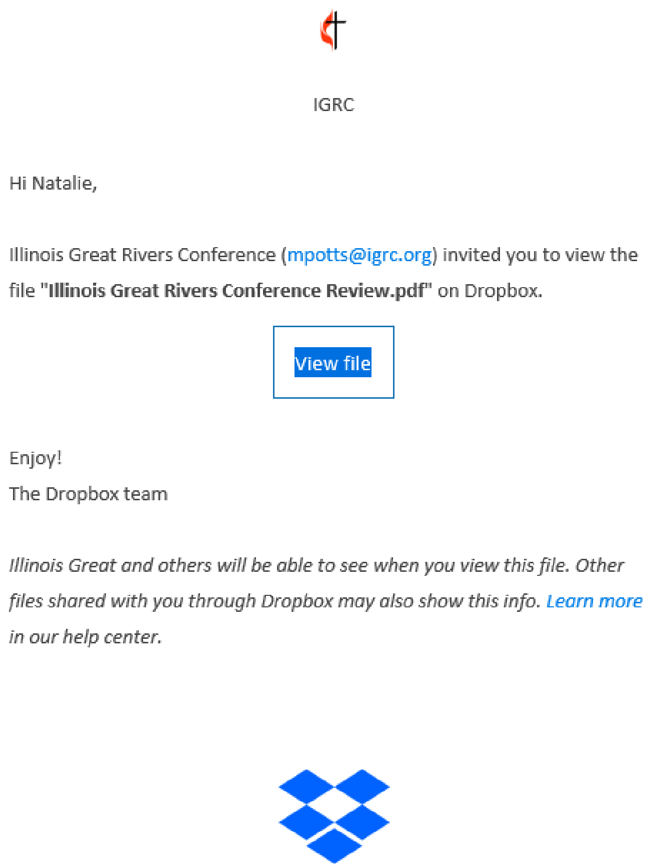
Church address [redacted]

- What is phishing?
  - Sophisticated impersonation via email or text
    - Impersonation from legitimate contacts who have had their accounts hacked.
    - How hacked?

- The example phishing email to the left came from a known UMC conference employee including the legitimate email address, signature and conference address.

Security Awareness Training

Expecting this file?



IGRC

Hi Natalie,

Illinois Great Rivers Conference (mpotts@igrc.org) invited you to view the file **"Illinois Great Rivers Conference Review.pdf"** on Dropbox.

View file

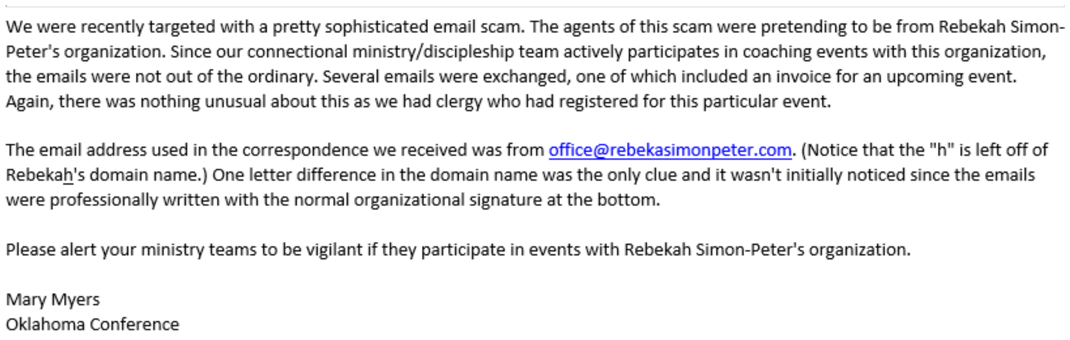
Enjoy!
The Dropbox team

Illinois Great and others will be able to see when you view this file. Other files shared with you through Dropbox may also show this info. Learn more in our help center.

Copycat email domain?

office@rebeka***h***simonpeter.com

office@rebekasimonpeter.com



We were recently targeted with a pretty sophisticated email scam. The agents of this scam were pretending to be from Rebekah Simon-Peter's organization. Since our connectional ministry/discipleship team actively participates in coaching events with this organization, the emails were not out of the ordinary. Several emails were exchanged, one of which included an invoice for an upcoming event. Again, there was nothing unusual about this as we had clergy who had registered for this particular event.

The email address used in the correspondence we received was from office@rebekasimonpeter.com. (Notice that the "h" is left off of Rebekah's domain name.) One letter difference in the domain name was the only clue and it wasn't initially noticed since the emails were professionally written with the normal organizational signature at the bottom.

Please alert your ministry teams to be vigilant if they participate in events with Rebekah Simon-Peter's organization.

Mary Myers
Oklahoma Conference

Security Awareness Training Policy

- Training should be conducted with those who have an organizational email, domain/network access account or those who process, transmit and/or store sensitive data. This includes all employees, (full time or part time), contractors, consultants, partners, interns, volunteers or other third parties.
  - Training should be administered to all new-hires or role changes
  - Completion of regular computer-based training
  - Mock anti-spear phishing and social engineering tests and follow-up training as deemed necessary by the organization.
- Upon completion of each security awareness training module, all computer users will be required to complete and pass a test.
- Upon hire and annually, provide specialized training for individual job roles that manage high risk and sensitive information (e.g., credit card data, personally identifiable information (PII, PHI), etc.).
- Upon hire and annually, provide specialized training for any employees that have administrator system access or hold other positions with significant and relevant information and/or application security operations responsibilities.

UMC Support Resources

Quarterly Security Awareness Training Webinar

Mar. 18, 2 pm EST

Webinar Registration - Zoom

UMC INFORMATION TECHNOLOGY SUPPORT

Security Awareness Training Services

- Quarterly training campaigns
- Monthly phishing tests
- Role-specific training (e.g., new hire, system admins, sensitive data handling)

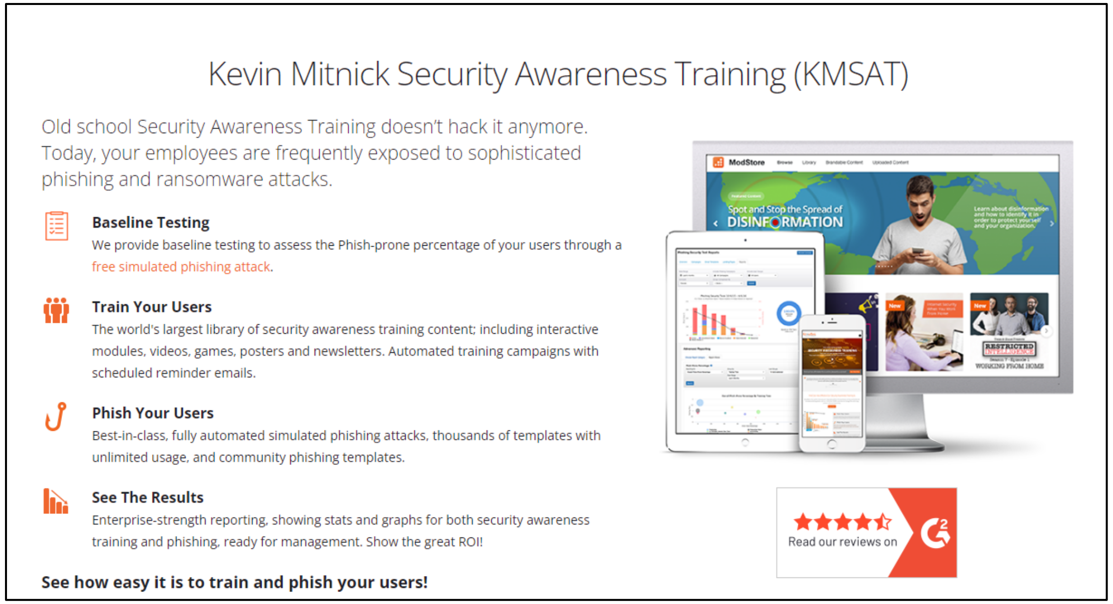
Resources

UMC INFORMATION TECHNOLOGY SUPPORT

- Get Enhanced Cybersecurity
- Common Scams
- Protect Your Ministry
- Protect Against Ransomware
- Elevate Your Digital Defense
- UMC Support Technology Services

Resources

- Training Campaigns



Kevin Mitnick Security Awareness Training (KMSAT)

Old school Security Awareness Training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

Baseline Testing
We provide baseline testing to assess the Phish-prone percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

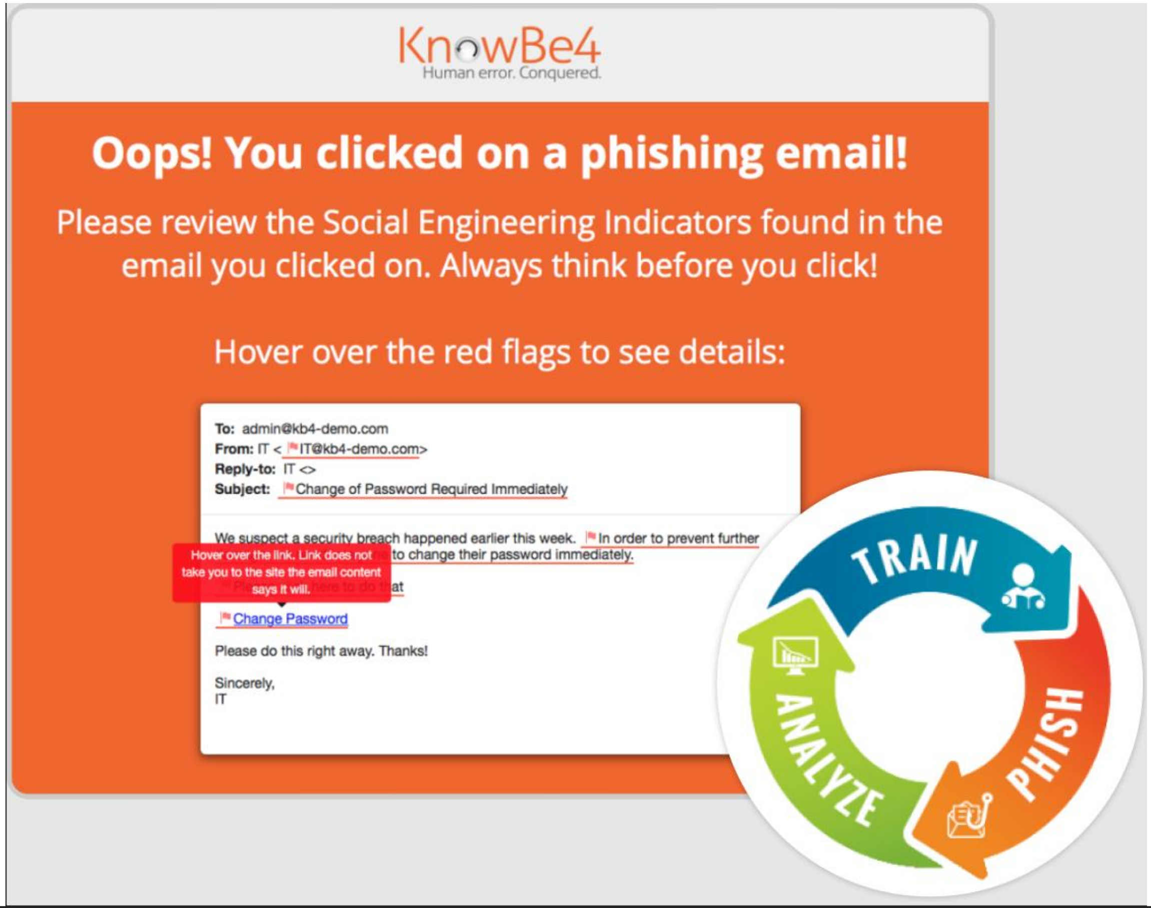
See The Results
Enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management. Show the great ROI!

See how easy it is to train and phish your users!

$1.91 / user / month

- Simulation

KnowBe4
Human error. Conquered.



KnowBe4
Human error. Conquered.

Oops! You clicked on a phishing email!

Please review the Social Engineering Indicators found in the email you clicked on. Always think before you click!

Hover over the red flags to see details:

To: admin@kb4-demo.com
From: IT < IT@kb4-demo.com>
Reply-to: IT <>
Subject: Change of Password Required Immediately

We suspect a security breach happened earlier this week. In order to prevent further … to change their password immediately.

Hover over the link. Link does not take you to the site the email content says it will.

… at

Change Password

Please do this right away. Thanks!

Sincerely,
IT

Conclusion

- UMC Technology Support is your trusty sidekick in the digital realm. We’re here to keep your bits and bytes in harmony, your servers singing sweetly, and your Wi-Fi password a well-guarded secret.
- Remember: When in doubt, reboot. And when in serious doubt, call your friendly neighborhood UMC Support.

Thank You!

☎ Phone: 615-916-2729

✉ Email: sasmus@gcfa.org

1908 Grand Ave. Nashville, TN 37212

www.UMCSupport.org

UMC SUPPORT INFORMATION TECHNOLOGY

FINANCE & ADMINISTRATION
General Council on Finance and Administration
THE UNITED METHODIST CHURCH

Appendix A:
GCFA – UMC Support Computing Standards 2026

Summary of Recommended Devices

FINANCE & ADMINISTRATION
General Council on Finance and Administration
THE UNITED METHODIST CHURCH

UMC INFORMATION TECHNOLOGY
SUPPORT

Desktops – Value / Standard / High-End

Value: Dell Pro Slim Plus – i5, 16GB RAM, 256GB – $953

- **Standard:** OptiPlex SFF Plus 7020 – Ultra 7, 32GB, 512GB – $1396
- **High-End:** Precision 3680 – i9, 32GB, 512GB – $2400

All-in-One Desktop

- Dell Pro 24 AIO – Ultra 5, 16GB, 256GB – $1,659

Laptops – Value level

- Dell Pro 14 – Core 5, 16GB, 256GB – $960.45
- Dell Pro 14 Plus – Ultra 7, 16GB, 512GB – $1416.26

Laptops – Standard / High-End

- Dell Pro 16 – Core 5, 16GB, 256GB – $970.92
- Dell Pro 16 Plus – Ultra 7, 16GB, 512GB – $1,477.81
- Pro 16 Plus PB16250 – Ultra 7, 32GB, 512GB – $1,711.10

Printers – Color / B&W

Canon LBP633Cdw Color Laser – $450

Canon LBP246dw B&W Laser – $375

Scanner & Webcam

- Canon R50 Office Scanner – $529

- NexiGo StreamCam N930E – $54

All-in-One Printer/Scanner/Fax

- Canon MF269dw II – B&W AIO – $380