IN OBSCURA LLC
THREAT INTELLIGENCE – SECURITY COUNTERMEASURES-INVESTIGATIONS
ALEXANDRIA, VIRGINIA
https://inobscura.org/

Judges 6:12 ESV And the angel of the Lord appeared to him and said to him, "The Lord is with you, O mighty man of valor."

CYBER THREAT NOTE– 9 JAN 2026

TLP-C CYBER THREAT NOTE Troublesome Tithes Scammers Use Deepfakes 6 January 2026

CAVEAT: THIS INTELLIGENCE PRODUCT RELIES ON OPEN-SOURCE MEDIA OR GOVERNMENT RELEASED UNCLASIFIED INFORMATION. RECOMMENDED ACTIONS ARE INCLUDED FOR CLIENTS FOR INFORMATION AND ACTIONS DEEMED APPROPRIATE.

CHURCH THREAT LEVEL – URGENT

Troublesome Tithes: Scammers Use Deepfakes to Trick Churchgoers
ASIS Security Management Journal, Sara Mosqueda, 6 January 2026
https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/january/scammers-ai-vs-churches/

A growing number of pastors and ministers are warning their congregations about scams using artificial intelligence (AI) to impersonate them through online messages, calls, and deepfakes. Throughout the United States—including **Alabama**, **Florida**, **Missouri**, **Nebraska**, and **New York**—and even beyond, such as a **megachurch in the Philippines**, faith leaders have been warning their followers about these scams.

Confusing the issue for churchgoers is the fact that a lot of real pastors and ministers with large online followings are asking for donations or selling items on their platforms. But what they are selling is different from their AI mimics, and the funds go to a different account, of course.

"With the help of social media, religious authority figures have been able to reach believers far beyond their neighborhoods, but the proliferation of content featuring their likenesses and voices has also provided the perfect opportunity for scammers wielding generative AI tools," *WIRED* recently reported.

With so much video and audio content online posted by religious leaders, scammers are able to sample that information and feed it into an AI tool. Along with targeting members of a church, these captured and manipulated voices can be used in increasingly sophisticated **phishing attempts** to try to get religious institutions themselves to transfer funds to scammers.

Beyond targeting people's bank accounts, AI featuring or targeting a minister, pastor, or notable church figure has also been used to spread disinformation.
In July 2025, TD Jakes, an author and pastor from Texas, had to deal with rumors that he attended sex parties hosted by Sean "Diddy" Combs, who at the time was facing federal charges of sex crimes. Jakes said that an investigation into the online rumors found that **44,000 of the accounts spreading the claims were bots**.

Deepfakes of Pope Leo XIV have also surfaced on social media, including ones where he delivers a message to the president of Burkina Faso, delivering false sermons, and attacking U.S. Vice President JD Vance.

On other occasions, the motive for a deepfake video or other AI-generated product is unclear, such as short-form videos with unknown (and likely fictional) pastors delivering a viral sermon. WIRED pointed to one TikTok account, **Guided in Grace**, that notes in its bio it is using AI "to show a parallel universe," but the captions on its videos, which were all posted in October 2025, do not indicate that they are AI-generated. The account has more than 10,000 followers.

Spotting deepfakes is getting harder and harder. Take the extra moment to try and determine if what you're watching is real or just more AI slop. One method is the **SIFT model**:

- **S**top—don't make snap decisions or actions.

- **I**nvestigate the source.
- **F**ind better coverage by looking for a trusted source reporting on the event or verification.
- **T**race the original context.

Threats Growing Beyond Financial Information

Because of this, the number of churches seeing cyber attacks is growing. Financial information isn't the only target for cybercriminals. Your website and Wi-Fi are also prime targets. The types of cyber attacks have become more complex and continue to evolve – malware, phishing, Trojan horse viruses, and ransomware attacks. In many cases, the threats are evolving so quickly it's hard for your IT team to stay on top of them.

Think about your personal email account. The number of questionable emails that get through the spam filter is alarming. Who wouldn't think about clicking on an email regarding issues with your bank account or credit card? Now consider your church staff. Not all are tech-savvy enough to identify a phishing email, and even those who are, aren't always vigilant.

Your church literally can't afford to incur a cyber attack. If your member's or financial data is compromised, it will immediately impact your giving and your church's reputation. The willingness to share personal and financial information will evaporate. Trust will be lost. Leadership's abilities will be questioned. And, inevitably, the impact of the cyber breach will spread throughout your community. A security breach will be tough, if not impossible, to recover from.

Church Security Vulnerability Prevention

There are ways your church can reduce the odds of an attack. And resources are available to help you eliminate the vulnerabilities of your church's cybersecurity.

Security Assessment

- Knowing how vulnerable your people and systems are is a critical initial step for your cyber security.
- Set up procedures and policies to prevent an attack. And to address a cyber security event should one occur.

- Take your free Information Security Assessment now.

Training

- Keeping staff updated on potential cyber threats is a must. Sharing tips on types of phishing will demonstrate how simple or sophisticated they can be.
- Requiring strong passwords is essential. Set a minimum of total characters, numbers, and special characters. Also, require passwords to be updated regularly

IT

- Invest in tools that will enable your IT staff to stay on top of cyber security issues.
- Investing in IT staff training and certifications is also advisable.

Managed Service Provider (MSP)

- MSPs can partner with your organization to provide peace of mind that your IT devices, users, and data are secure and operating efficiently.
- They'll improve security, give you immediate access to expertise, and expand your IT staff without the extra benefits expense or HR forms.
- They will provide a proactive plan and help implement it to ensure IT problems don't occur.
- An MSP offers affordable subscription-based pricing models that give you immediate security and cover IT services from security and risk mitigation to network infrastructure to software licensing.

  Cyber threats are real. You must ensure your data and systems are safe if a cyber attack occurs. The time to take action is before an event occurs. Contact us today to find out if we can mitigate your security risks.

MINISTRY THREAT LANDSCAPE

The following examples are ways churches and other ministries have been victims of cybercriminal activity in the real world: An Ohio ministry was scammed out of $1.75 million in a business email compromise (BEC) attack while the ministry's facilities were undergoing a $4 million renovation. Hackers gained access to two employee email accounts and used the accounts to convince other employees to wire funds to a fraudulent bank account.iv

A church in Iowa had seven years' worth of files encrypted in a ransomware attack after an employee clicked on an email titled "job application – please see attached CV." Churches in Bristol, England, were victims of a similar attack.v A church's online giving system was hacked, and someone gained access to their usernames and passwords.

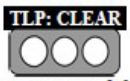
The first day, $17,000 was taken. Each day after, approximately $3,000 more was stolen, until the thefts were discovered by the ministry. The grand total stolen was $181,709. A hacker was able to gain access to and place malicious computer code on a church's shopping site.

This allowed the hacker access to any new credit card information entered in the system. The church had to spend $15,000 to research the damage. In addition, it was required, by law, to offer its 1,800 customers professional ID protection. A church bookkeeper received a message on her screen that she had been the victim of a computer breach. As a result, she was locked out of the system.

The message prompted her to call an unknown phone number to restore access to the computer. She allowed access to the hackers and immediately saw SSNs show up on the screen. At that point, she knew something was wrong. Experts were hired to monitor credit for those affected. A church received a notice that its records were frozen and held for ransom. The church did not pay the ransom, lost access to the records (which were not physically backed up) and was forced to rebuild all its records from scratch. A church had its website hijacked by ISIS/ISIL.

The terror group posted graphic images and videos of shootings and beheadings. These examples are just a glimpse into the threats facing ministries and churches. In fact, over 20% of churches have experienced a successful cyberattack.vi Furthermore, that number may be higher considering many churches may not even be aware they have been compromised.**///END OF ARTICLE///**

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 For the eyes and ears of individual recipients only, no further disclosure.	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
 Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.
 Limited disclosure, recipients can spread this within their community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
 Recipients can spread this to the world, there is no limit on disclosure.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

///END OF REPORT///