In Obscura
Vincent M. Nasti, Founder, Chief Executive Officer, Consultant
In Obscura, LLC | Threat Intelligence | Security Countermeasures | Investigations
https://inobscura.org/

(TLP-C) CYBER ATTACKS AND AI AGAINST CHRISTIAN CHURCHES MISSIONARIES 11 JUN 2026

KNOW THE TARGET – WATCH THE TARGET – LOOK DEEPER -EXPECT THE UNEXPECTED

IN OBSCURA THEAT LEVEL – IMMINENT

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.

IN OBSCURA COMMENT

Open Source Intelligence collection has established cyber intrusions of U.S. church computer systems with exfiltration of personally identifiable information on the clergy and congregation. Considering the escalation of the threat environment in Europe and the United States targeting churches, related equities, clergy and congregations, most remain exceptionally soft targets.

Why Are Churches Being Targeted[1]?
Churches may not have million-dollar bank accounts, but they possess something just as valuable: data and trust. Here's why they're attractive to cybercriminals:

- Sensitive Information: Churches store detailed records about their congregants—names, addresses, phone numbers, donations, even counseling notes.

- Online Donations: With the rise of digital tithing and giving platforms, churches process financial transactions that can be intercepted or manipulated.

[1] Why Are Churches Being Targeted, 15 Apr 1016, Bawn Crush Cyber Risk, https://bawn.com/risk-resilience-bawns-guide-to-cybersecurity-and-beyond/why-churches-are-becoming-a-growing-target-for-cyberattacks

- Low Cybersecurity Readiness: Many churches rely on volunteer-run IT systems or outdated technology, making them easier targets.

- Public Leadership: Pastors and staff are publicly known, making it easier for criminals to impersonate them in email or text scams.

- Fast Payment Pressure: Ransomware attackers know that churches may pay quickly to restore critical systems, especially around holidays or major events.

- Churches may not have million-dollar bank accounts, but they possess something just as valuable: data and trust. Here's why they're attractive to cybercriminals:

- Sensitive Information: Churches store detailed records about their congregants—names, addresses, phone numbers, donations, even counseling notes.

- Online Donations: With the rise of digital tithing and giving platforms, churches process financial transactions that can be intercepted or manipulated.

- Low Cybersecurity Readiness: Many churches rely on volunteer-run IT systems or outdated technology, making them easier targets.

- Public Leadership: Pastors and staff are publicly known, making it easier for criminals to impersonate them in email or text scams.

- Fast Payment Pressure: Ransomware attackers know that churches may pay quickly to restore critical systems, especially around holidays or major events.

Recent Cyber Incidents Involving Churches

Here are just a few recent examples that illustrate how real—and growing—this threat is:

- The World Council of Churches (WCC) communications systems have been hacked by a ransomware group. https://www.oikoumene.org/news/wcc-hit-by-ransomware-attack

- Greater Mt Calvary Holy Church (DC) – Aug 2024: Ransom Hub ransomware disrupted operations and may have exfiltrated personal data bawn.com.

- River Valley Church (April 2024): Hacktivists leaked sensitive data in a politically motivated campaign bawn.com.

- World Council of Churches Ransomware Attack (Dec 2023) The global Christian inter-church organization was hit by a ransomware attack from the Rhysida group, who demanded nearly $280,000 in Bitcoin and threatened to leak data.

- Greater Mt Calvary Holy Church (Aug 2024)RansomHub, a known ransomware gang, targeted this prominent Washington, D.C. church, disrupting operations and possibly compromising personal data.

- Blue Grass Church Email Scam (Sept 2024) Scammers created a fake Gmail account impersonating the church's pastor and reached out to members for "urgent help"—a classic Business Email Compromise (BEC) tactic.

- SiegedSec Attack on River Valley Church (April 2024) As part of a politically motivated campaign, hacktivists leaked sensitive data from River Valley Church, showing that ideological motivations are also in play.

- Saint Cecilia's Church of England School (Easter 2024)Ransomware disrupted this church-affiliated school's servers during Easter, impacting access to administrative systems and school operations.

Open Source Collection June 2026:
Church website hacked by group claiming to 'love ISIS'
January 26, 2015, Layman Presbyterian News and Analysis1Comment
By Allie Hinds, News Channel 11, (Tennessee)
https://layman.org/church-website-hacked-group-claiming-love-isis/

On Thursday if you logged onto Westminster Presbyterian Church's website you'd see the words "I love ISIS and Jihad", a violent video, and vulgar language.

The church's pastor Jim Richter said he woke up this morning to an email on his phone from a church member saying the website had been hacked by what appeared to be ISIS supporters. "I think it's terrifying, it's hostile no matter what you say about it," Marty Conley, who lives in Johnson City said.

A homepage to a church in East Tennessee, with about 200 members is not the first place you think would be vulnerable to a hack from ISIS. "I thought that was really strange. You don't think about that type of thing happening in our area, I mean little town Johnson City, Tennessee," Conley said.

New Beginnings Church (NC) – January 2026: Ransomware group Incransom claimed to have exfiltrated all sensitive data and threatened to leak it unless negotiations began www.dexpose.io.

Ransomware Group sinobi Hits: Ingomar Church
11 January 2026
https://www.hookphish.com/blog/ransomware-group-sinobi-hits-ingomar-church/

Incransom Targets St Ignatius of Loyola Catholic Community
Dexpose, January 9, 2026, Website listed as a victim of ransomware; attackers likely exfiltrated or threatened to publish sensitive data (netcrook.com).
https://www.dexpose.io/incransom-targets-st-ignatius-of-loyola-catholic-community/

Targeted by Tech: How Criminals and Governments Can Use AI and Cyber Attacks Against Christian Missionaries, Frontier Ventures, Issue #47-4, July 2025
https://connect.frontierventures.org/mission-frontiers/targeted-by-tech-how-criminals-and-governments-can-use-ai-and-cyber-attacks-against-christian-missionaries

As the global Church advances into digital frontiers, missionaries are facing not only spiritual and cultural opposition but the potential of an increasingly hostile cyber arena. Criminal syndicates, extremist groups, and authoritarian regimes are harnessing cutting-edge technologies and can target Christians spreading the gospel across restricted and persecuted regions. What once required human effort and espionage is now being amplified, automated, and accelerated through Artificial Intelligence (AI).

As the global Church advances into digital frontiers, missionaries are facing not only spiritual and cultural opposition but the potential of an increasingly hostile cyber arena. Criminal syndicates, extremist groups, and authoritarian regimes are harnessing cutting-edge technologies and can target Christians spreading the gospel across restricted and persecuted regions. What once required human effort and espionage is now being amplified, automated, and accelerated through Artificial Intelligence (AI).

This article explores how these cyber threats are evolving, why Christian workers are prime targets, and what ministry leaders can do to secure both their mission and their people.

Digitally Monitored Mission Field

Missionaries today are more connected than ever. Email, cloud-based file storage, messaging apps, and social media have revolutionized communication and coordination. But these same tools also expose missionaries to tracking, surveillance, and attack, both digitally and physically.

Hostile governments use AI to monitor internet activity, social media profiles, encrypted messaging apps, and even private emails. Sophisticated tools can intercept and analyze digital footprints in real time, identifying Christian workers based on keyword detection, behavioral analysis, voice analysis, or geolocation data.

An example of this danger includes fake QR codes impersonating secure messaging apps like Signal. These malicious links download spyware onto phones, giving attackers access to texts, contacts, locations, and call logs. This type of AI-enhanced social engineering transforms every "secure" message into a potential threat.

AI: Friend and Foe in Cybersecurity

AI is revolutionizing cybersecurity—but not only for the good guys. Adversaries are leveraging AI to supercharge attacks:

- **Automated phishing campaigns** that generate hyper-personalized emails based on scraped data. The goal is to get someone to click on a link and give an attacker an "in" to the ministry or missionary's digital world.
- **Deepfake audio and video** impersonations of missionary leaders or known contacts.
- **Behavioral mimicry**, where AI learns a user's communication style and replicates it to gain trust before launching an attack.
- **AI-powered malware** that mutates in real time to evade detection.

What's particularly dangerous is AI's ability to scale. With traditional phishing, an attacker could send a few hundred messages a day. AI can now generate thousands—each convincingly tailored to the victim's language, culture, and context.
As missionaries become more digitally active, their online personas become fertile ground for AI-driven reconnaissance and manipulation.

Real-World Impacts: Lives at Risk

Unlike corporate hacks that focus on stealing credit cards or financial data, cyberattacks on missionaries can be a matter of life and death. Leaked communications can expose ministry plans, endanger local believers, and compromise entire church networks.
In regions hostile to Christianity, governments use surveillance technologies to identify and intimidate local believers. Identity correlation (linking user-names, phone numbers, or social media accounts to real people) has led to interrogations, deportations, and in some cases, imprisonment.

It is important that missionaries balance usability with security. While Paul in the New Testament openly declared his travels and companions, John was more cautious, avoiding names and preferring face-to-face communication. Both models are biblical. The lesson: Missionaries must adapt their cybersecurity posture based on the risks of their environment.

Top Threats Facing Missionaries

Drawing from industry insights like Cisco's Identity Security and Splunk's Top 50 Cyber Threats, here are some of the most pressing digital dangers Christian workers face:

- **Credential Stuffing & Account Takeovers:** Attackers use stolen passwords from other breaches to access ministry systems.
- **Phishing & Spear Phishing:** Highly targeted attacks pretending to be from partners or field teams.
- **Surveillance Malware:** AI-enhanced spyware embedded in fake Bible apps, messaging platforms, or shared files
- **DNS Hijacking:** Redirecting missionary traffic to fake sites to harvest credentials or deliver malware.
- **Fake Wi-Fi Networks:** Rogue access points near conferences or cafes where missionaries gather
- **Social Media Profiling:** Mining missionary posts to determine location, travel plans, or team members.
- **Supply-Chain Attacks:** Compromising third-party tools used by ministries (email platforms, CRMs, etc.).

- **Mobile-Device Exploits:** Insecure or jailbroken phones serve as easy entry points into field operations.

Digital Discipleship Demands Digital Stewardship

Many ministries invest in prayer, partnerships, and preaching but overlook cybersecurity as part of their missional stewardship. That must change.
The digital world is a mission field—and a battlefield.

Some clear steps ministries can take:

- Use multi-factor authentication (MFA) across all systems.
- Encrypt all communications, especially on mobile.
- Regularly update devices and software to patch vulnerabilities.
- Employ VPNs and encrypted DNS services (like Cloudflare or DNSWatch).
- Use password managers and avoid password reuse.
- Secure physical devices with locks & access controls.
- Provide training on phishing, fake links, and deepfakes.
- Implement strict data-access and confidentiality policies.
  A missionary's identity is the new perimeter. Ministries must protect their people's digital identity with tools that verify not just a password but the device, location, and behavior of each login.

AI-Powered Defense for AI-Powered Threats

AI isn't just a threat—it's a tool Christians can use for defense.
AI-driven cybersecurity platforms can detect anomalies, flag suspicious logins, and stop malware in real time. Machine learning can analyze login behavior and block access if something seems off. Even backup tools now use AI to detect ransomware and automatically roll back to safe versions.

Emerging tools allow for:

- Real-time threat detection and automated response.
- Predictive analytics to forecast where attacks may occur.
- Identity intelligence to detect impersonation or deepfakes.
- Behavioral biometrics for access control.

Faith & Firewalls: A Biblical Approach

Security isn't about paranoia. It's about preparation. In Scripture, Nehemiah didn't stop building the wall to fight every enemy, but he did set guards and made sure the builders had swords. Jesus told his followers to be "wise as serpents and innocent as doves." And Paul warned believers not to be unaware of Satan's schemes.

Cybersecurity is a matter of wise stewardship—of lives, resources, and the gospel itself. As AI-driven threats grow, Christian organizations must evolve. Not with fear but with faith-infused strategy. With the right tools, training, and trust in the Lord, missionaries can continue to bring the hope of Christ into the darkest—and most digitally dangerous—places on earth.

Next Steps for Ministry Leaders

1. Conduct a cybersecurity audit for your team.
2. Mandate MFA and encrypted messaging.
3. Train every staff member and volunteer on basic digital hygiene.
4. Use AI-driven security tools that adapt to emerging threats.
5. Build partnerships with Christian tech ministries for ongoing support.

The message of Jesus will never be stopped by code or cables.
But those who carry it must walk wisely in a world that is watching, listening, and attacking. Let's equip our missionaries—not only with prayer and resources but with digital armor for the modern mission field.

Author

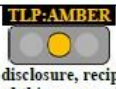
JON RALLS

Jon Ralls is the Executive Director of a nonprofit Business As Mission endeavor working with Christian mission teams in over 100 countries from multiple organizations. He can be contacted at jralls@kavanahmedia.com

///END///

==========

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///