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 WARNING
FREE WI FI EXPLOITATION (FORBES NEWS)
2 DECEMBER 2025
CHURCH THREAT LEVEL - HIGH

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.

SUBJECT: Cyber exploitation of Smart phones, based on Forbes reporting and analysis via TSA Cyber and additional information from cyber security firms. Although focused on the holidays and travel risks, this is passed as threat warning fir Christians in transit.

But a much deeper concern for In Obscura is the larger context of cyber espionage and targeting threat risks. Churches have been targets cyber espionage in the past, the successful exfiltration of Personally Identifiable Information on congregations, clergy, staff and as well the security force. Live services also provide further intelligence value to enemy elements based on the interior facial captures. If you have camera and audio surveillance interior and exterior this is in play for exploitation as well. Why? Target surveillance and intelligence collection for exploitation during any chose attack vector.

One suggested resource is the FBI Internet Crime Compliant Center (IC3) at ic3.gov
There you will can see the depth and breadth complete with public and industry alerts.

TSA Warning—Do Not Use These Networks On Your Smartphone
ByZak Doffman, Forbes News, Dec 02, 2025, 06:57am EST
https://www.forbes.com/sites/zakdoffman/2025/12/02/tsa-warning-do-not-use-these-networks-on-your-smartphone/
TSA warning comes to life as man jailed for attack.

Almost all smartphone users are at risk, Google says, flagging messaging attacks and "unencrypted" networks that are "easily exploited" by hackers. This stark alert echoes a warning from America's Transportation Security Administration (TSA).
TSA tells the traveling public: "Don't use free public WiFi." And now, with the holiday season underway, this will be front of mind. TSA has faced some criticism for its alert, not least indirectly from the FTC, but Google has now said exactly the same.
There may be some wry smiles within TSA's cyber team this week, given the news that a man "who created 'evil twin' Wi-Fi networks to capture personal data and hacked into women's online accounts to steal intimate material" has been jailed.

ForbesSamsung Updates All Galaxy Phones—Google Warns Attacks UnderwayBy Zak Doffman

That update comes from the Australian Federal Police (AFP). The attacks took place onboard a flight — in midair. Airline employees "identified a suspicious WiFi network – which mimicked a legitimate access point – during a domestic flight."

Public Wi-Fi warnings rile cyber experts because most data traffic to and from devices is now encrypted. But that focuses on interception of the data itself. An evil-twin attack is different. This fakes an access point, using a similar Wi-Fi name to a real service, "hoping that users will connect to it instead of a legitimate one."

Per Kaspersky, "when users connect to this access point, all the data they share with the network passes through a server controlled by the attacker. An attacker can create an evil twin with a smartphone or other internet-capable device and some readily available software. Evil twin attacks are more common on public Wi-Fi networks."
None of this is new. I reported on the in-flight Wi-Fi threat in 2020. "Public Wi-fi will always have risk," Cyjax CISO Ian Thornton-Trump told me. "I once saw a Starbucks and a Subway Wi-Fi access point, flying from Newark to Vegas at 35,000 feet."

At an airport or a mall or a resort, it's all too easy to scroll through the countless Wi-Fi networks looking for one absent a private padlock and with an option to connect. "Free Airport Wi-Fi" or "Free Flight Wi-Fi" are easy to create and hard to police.

Zimperium warns that "during travel, these risks multiply. Airports, hotels, rideshare hubs, and cafés all offer rich hunting grounds for attackers leveraging man-in-the-middle attacks or malicious public Wi-Fi. And employees, often multitasking or in a hurry, are far more likely to click, install, or connect without thinking twice."

With the holiday season, TSA's travel advice will now come back around.

Just be careful before you click to connect. **///END///**

==========DISSEMINATION==========

IN OBSCURA HAS ADOPTED THE OSINT CLASSIFICATION SYSTEM OF DHS DEPARTMENT OF HOMELAND SECURITY CLASSIFICATION: TLP CLEAR, TLP Clear: when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. HOWEVER IN OBSCURA RELEASE PROHIBITION MARKINGS APPLY https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usagg

==========

REQUEST WRITTEN PERMISSION, EMAIL, PRIOR TO DISSEMINATING ANY IN OBSCURA PRODUCTS OR INFORMATION.

TRAFFIC LIGHT PROTOCOL REQUIREMENTS FOR DISSEMINATION

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///