How to Prevent Wireless Microphone Eavesdropping

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Jack was concerned about his job so he eavesdropped on the Board meetings. Joan makes money selling her exceptionally high quality, but unauthorized, recordings of concerts. Jared is a star reporter at a business media outlet due to his almost pre-cognizant scoops. What's their secret?

Wireless microphone eavesdropping; the easiest and safest way to listen in. It negates needing an invitation or having to pay for admission. It overcomes the doors being closed to prevent sound leakage. It is a classic espionage trick used for financial gain.

Targets of wireless microphone eavesdropping range from espionage at corporate off-site meetings to bootlegging concerts, to media news gathering.

Here you will learn how to prevent wireless microphone eavesdropping.

Step 1 – Know Your Microphone

Basically, a wireless microphone is a miniature radio station worn by a public speaker, presenter, or musician. The sound of the person's voice and/or musical instrument is transmitted to a nearby radio receiver, amplified and played through loudspeakers so the audience can hear more easily. In some cases the audio is also used to make a recording or is transmitted to a select remote audience.

Unfortunately, radio transmissions do not stop at the receiver. Wireless microphones can transmit for distances of 100 feet to a mile depending upon the type of microphone and terrain. Any receiver tuned to the same frequency can receive the signal, if it is an FM analog signal.

FM analog modulation is used by all older wireless microphones. Inexpensive wireless microphones currently being sold are also FM analog types.

Eavesdropping on a specific meeting is only one danger. Presenters often don't know, or forget, lavaliere microphones continue to broadcast when they are off stage.[1] Only the receiver may be turned off. This means that side comments, hallway and bathroom conversations will still be intercepted. Even when they remove the microphone, it may not be turned off. So beware, commercial wireless microphones are designed to be sensitive, and they will broadcast crystal clear audio.

When targeting off-site meetings, for example, the opposition will set up radio receivers and recorders in one of the hotel's rooms, or in an unoccupied car parked nearby, as demonstrated in this 2-minute video.[2] (You may also use the QR code to access it.)

These outsiders are betting you will use wireless microphones, and that you will make a variety of other simple security mistakes. You will never see them.

There are three basic types of wireless microphone transmissions: FM Analog, Digital, and Digital Encrypted.

[1] https://youtu.be/pdE83FX-Mto?t=28

[2] https://counterespionage.com/wireless-microphone/

How to Prevent Wireless Microphone Eavesdropping

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

• FM Analog Microphones

FM analog transmissions are the easiest to intercept. All that is required is a radio receiver tuned to the same frequency.

FM analog wireless microphones look similar to other types of wireless microphones. Clues that you may be using an FM analog microphone include: it's an older and/or less expensive model.

A quick internet search of the model number can confirm the type. Many FM analog microphone specification sheets do not mention their transmission type as being FM analog, no surprise there. They also don't mention encryption. Price is another good indicator of security. If it is inexpensive, it is probably an FM analog model.

• Digital Microphones

Eavesdropping on digital transmissions is difficult, but not impossible. When intercepted, the signal sounds like static instead of a clear voice. This is because the transmitter is communicating with the receiver digitally. This eliminates random eavesdropping. The receiver then converts the digital signal back to analog so it is intelligible.

If a determined eavesdropper is aware of the make and model number of the system being used they can simply purchase a like receiver for interception and demodulation.

Identifying this type of wireless microphone can be tricky…

Digital Doesn't Always Mean Secure

A *digital* wireless microphone can mean several things…

Some manufacturers label their FM analog wireless microphones as being *digital*, without further explanation. When pressed, they admit *digital* only refers to the circuitry, not the transmission; this is a very deceptive marketing practice.

Honest manufacturers use the *digital* label to mean the transmission is *digital*. While this increases security due to the steps needed to demodulate the transmission, absolute privacy cannot be fully assured.

• Digital Encrypted

This type of system will prevent wireless microphone eavesdropping, but only if programmed properly.

Encryption is an option, not a default, in many systems. It has to be turned on and programmed to pair with a specific receiver. Venue audio-visual crews, *if* they use digital encrypted systems, usually don't take the time to encrypt unless specifically asked to do so. Be sure to ask.

If they are not familiar with the process, here are the instructions for the most ubiquitous systems in use today. Other systems have a similar set-up process. Their instruction manuals are available on-line.

How to Prevent Wireless Microphone Eavesdropping

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Step 2 – Programming Your Microphone

Use the information here as a general orientation. Read your system's manual for specific instructions.

The Shure QLX-D, ULX-D, Axient Digital (AD), and Microflex (MX) systems offer digital transmission *and* encryption capabilities. Employing full security, however, is a two-step process.

If the system is simply operating in digital mode the transmitter can also be paired—given a moment at close range—to any similar rogue receiver. If the digital transmission is *also* encrypted the microphone will only pair with its legitimate receiver. It is then the transmissions are considered to be business-level secure.

Double Check the Settings

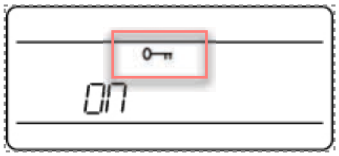
Shure wireless microphone systems feature Advanced Encryption Standard (AES-256) to protect the audio signal. When encryption is enabled, the receiver generates a unique encryption key which is shared with a transmitter during an IR sync. An IR sync is accomplished by holding the transmitter near the receiver when programming. An infrared beam (similar to a TV remote control) transmits the encryption key between the units, thus completing the encryption process.

Transmitters and receivers that share an encryption key, form a protected audio path, preventing unauthorized access by other receivers. To maintain security, components remain encrypted when turned off and on.

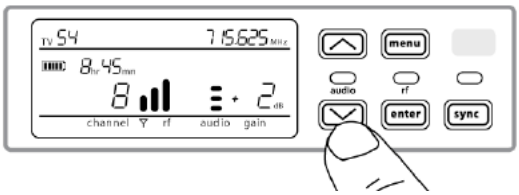
Creating an Encrypted Audio Channel[3]

1. Press the menu button to navigate to the encryption menu, indicated by the key icon.

2. Use the arrow buttons to select an encryption option:
   - ○ ON = encryption enabled
   - ○ OFF = encryption disabled



3. Press enter to save. The key icon will be shown on the receiver display.



4. Press the sync button and align the IR sync windows of the transmitter and receiver. The encryption key icon will appear on the transmitter screen when the IR sync is complete and the encryption key has been transferred from the receiver.

Additional transmitters can share the same encryption key with a single receiver. Perform an IR sync to encrypt each additional transmitter.

Notes:

- The audio-visual staff might install the same encryption key on all mics and receivers, once, and never update them. Then, if a spare receiver goes missing, every event they stage

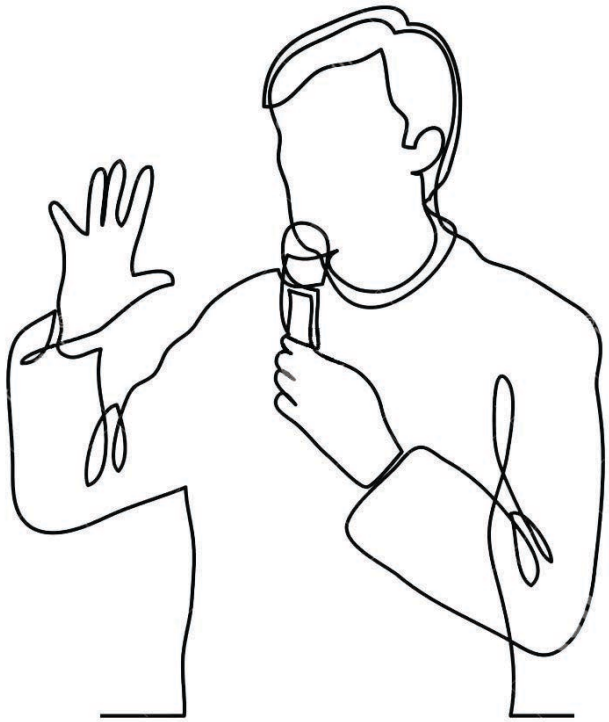
[3] https://pubs.shure.com/guide/QLXD/en-US

How to Prevent Wireless Microphone Eavesdropping

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

would be in jeopardy. Always ask the audio-visual staff to refresh the encryption keys.

- When OFF is selected to disable encryption, perform an IR sync to clear the encryption key from the transmitter and prevent an encryption mismatch error or FAIL message.
- If mixing system components encryption will not be available.
- If the encryption setting is not turned ON some types of digital wireless microphones will still need to be paired with rogue receivers. Doing this would *briefly* require bringing the mic and receiver within IR visual contact.



Resources to Combat Wireless Microphone Eavesdropping

Beyerdynamic TG-1000 / MCW-D[4]
2.4 GHz, Direct Sequence Spread Spectrum [DSSS] digital, proprietary encryption scheme based upon a 16 bit pattern.

Yamaha / Revolabs[5]
DECT, 1.92 GHz
128-bit encryption

Lectrosonics[6]
D² System
256-bit encryption - AES 256-CTR

Shure[7]
Shure QLX-D, ULX-D, Axient Digital (AD), and Microflex (MX) systems
AES-256 encryption

Kevin D. Murray CPP, CISM, CFE, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[8] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

[4] https://north-america.beyerdynamic.com/tg-1000-product-family-1.html

[5] https://uc.yamaha.com/products/microphone-systems/wireless-audio-conference-room-kit/

[6] https://www.lectrosonics.com/d2-system.html

[7] https://www.shure.com/en-US/products/wireless-systems

[8] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/