Privacy and SIP on the Public Internet.

It's no secret that Internet telephony is much more vulnerable to eavesdroppers than conventional phone calls. That's because IP phones aren't part of the public phone network, where tapping requires a specific, physical wire connection. Unprotected calls transmitted via a LAN, a WAN, or the Internet can be easily intercepted by anyone with a protocol analyzer, simply by capturing and analyzing the voice packets. This means that just about anyone can snoop on your business and personal calls, including employees, business partners, competitors, law-enforcement authorities, and government officials.

Since you probably don't like the idea of everybody and anybody listening to your conversations, you'll want to take action to ensure your VoIP privacy. The best way to accomplish this is with encryption.

As you probably already know, VoIP voice traffic is data that is transmitted over networks. This means, like any type of computer data, VoIP can be protected by encryption. Unfortunately, while VoIP encryption tools are widely available, not many people have taken the time and effort required to use the technology. That's a shame, because encryption can make it make it nearly impossible for someone to snoop on IP telephony calls. Here's a look at four different VoIP encryption approaches.

Internal Encryption: Many VoIP clients have responded to customer security concerns by incorporating encryption into their software. Skype Ltd., for example, has installed encryption support into its proprietary software. Check your client's provider to see if any encryption services are available.

TLS (Transport Layer Security) and IPsec (IP Security): TLS and IPsec are handy ways of encrypting VoIP calls. TLS encrypts VoIP data traveling between two applications, while IPsec encrypts information for two devices and all the applications running on them. Both protocols aim to keep unauthorized parties from interfering with or listening to calls, and they are almost impossible to manipulate externally. Both approaches are well worth considering.

SRTP (Secure Real-Time Transfer Protocol): SRTP is ideal for protecting VoIP traffic because it has a minimal effect on call quality. For each call you make, a unique encryption key is created, which makes eavesdropping almost impossible. This attribute alone makes SRTP a good choice for day-to-day calls, as well as highly confidential conversations.

VPN (Virtual Private Network): If your business has a VPN, you can leverage its built-in encryption feature to protect your IP telephony calls. Best of all, this protection is extended to all users — even traveling employees who log in to the VPN from a laptop. Remember, however, that a VPN can only secure the data from gateway to gateway. Once calls are on your LAN, you'll need additional protection.

People expect their phone calls to be as private as when they're speaking to someone in their own office or home. VoIP technology by itself can't guarantee this level of protection, so it's up to you to insist on the the safeguard — encryption — that will keep your conversations confidential.