

CYBEREXPERTS.com

We bring you...

"The Greatest Minds
in Cybersecurity"

[Home](#)[Cybersecurity](#)[Cybersecurity Guides](#)[Cybersecurity Careers](#)[Cybersecurity Encyclopedia](#)[Our Mission / Contact Us](#)

How to Encrypt Phone Calls




CYBEREXPERTS.com

How to Encrypt Phone Calls

by [George Mutune](#)

Best Practices for Encrypting your Phone Communications

 **ezoic** [report this ad](#)

Search




Phone communication through voice calls and text messages in the workplace is critical to ensuring continued productivity. In the post-COVID-19 era, a significant number of organizations have permitted employees to continue working remotely. As a result, mobile devices will remain critical to sharing sensitive information through various communication channels: SMS messages, VoIP calls, regular phone calls, video calls, group chats, instant messaging, and conference calls.

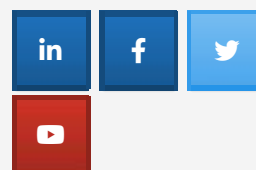
However, malicious cyber actors often target mobile phones or android devices that lack end-to-end **encryption** protection. According to **Checkpoint's Mobile Security Report 2021**, nearly every company experienced **cyberattacks** targeting cell phones, mobile apps, mobile calls, mobile communications, and communications done over a mobile network. Particularly, the report revealed the following statistics, which underscore the essence of making secure calls by adopting practices that enable encrypted calls:

1. At least 46% of companies have an employee that uses mobile devices to download harmful applications. Attackers use such apps to spy on unencrypted phone video or audio calls.
2. More than 40% of the mobile devices with internet access, including android and IOS devices, contain inherent vulnerabilities in their operating systems.
3. 97% of organizations worldwide face numerous threats that compromise secure phones. Additionally, dependence on mobile devices and wireless networks results in an expanded attack surface in the current digital age, potentially exposing users to multiple attacks.

Importance of Secure Voice Calls in the Workplace

 **ezoic** [report this ad](#)

Follow us to learn
great things



Cybersecurity Encyclopedia

**Advanced Persistent
Threat**

Adware

Antimalware

Banner Grabbing

Cloud Security

Cross-Site Scripting

Cyberattack

Cybersecurity

Defense in Depth

Denial of Service

Eavesdropping

Encryption

Secure communications are essential to protecting data and user privacy. Call encryption can provide peace of mind since an organization can be certain that nefarious cyber actors cannot intercept or exfiltrate sensitive information shared through a mostly insecure internet connection. Besides, the value of encrypting phone calls extends beyond a proactive approach to **cybersecurity** since numerous regulations require businesses to ensure the complete privacy of all stakeholders.

More importantly, encrypting cell phone calls guarantees secure messaging, secure file transfers, and total security of a caller ID, which is necessary to achieve complete user privacy. Besides, mobile phone encryption is necessary to address the privacy concerns of mobile users as most security experts agree that hackers are constantly using middle attacks to steal unencrypted personal information.

Espionage
Firewall
Insider Threat
Malware
Man-in-the-middle Attack
Network Security
Phishing
Ransomware

Common Phone Communication Methods

1. Voice over Internet Protocol (VoIP)

VoIP is a leading call communication standard that enables users to make voice and video calls. VoIP providers, such as zoom and Skype, have become essential in the post-pandemic era since VoIP calls are done via an internet connection. However, sufficient **network security** and call encryption measures are essential components required to ensure secure communication. Attackers can intercept unencrypted VoIP communications, especially if they are done over insecure wireless networks.

Besides, since VoIP integrates CRM systems and analytics platforms, unencrypted VoIP has heightened security risks to a company. Therefore, organizations should only use VoIP providers that implement end-to-end encryption, deploy secure wireless networks with TLS security and enabled Secure Real-time Transport Protocol (SRTP), and implement two-factor authentication to prevent unauthorized use.

2. Landlines

Landlines are largely unutilized today due to increased mobility and access to internet services. Nevertheless, landlines are often secure since a single line connects callers on each end of the line. Although wiretapping attacks are possible threats, they are usually difficult to execute for individuals lacking access to law enforcement resources. Still, security threats impacting landlines are a reality, and enterprises should implement sufficient protection measures. A common method of enhancing the security of landline calls is only using secure phones that implement measures for implementing voice calls. In addition, callers on both ends of the line must use encrypted phones to protect sensitive

3. Cell Phones

Cell phones have taken over communication in every sphere worldwide. Factors like reasonable security measures, convenience, and cheap costs have increased cell phone communications uptake. However, cell phones communicate through network signals, and individuals with the requisite knowledge can intercept them. Fortunately, an array of encryption techniques makes it possible to transmit confidential data without worrying that the communications may fall into the wrong hands. However, the overall security of cell phone communications largely depends on implemented encryption techniques. The following section discusses the different ways cell phone users can encrypt different types of phone communications.

Recommended Practices for Encrypting Phone Communications

1. How to Encrypt Voice and Video Calls

The Signal app, a desktop and smartphone encryption app, is a widely used method for ensuring user privacy. Numerous security researchers have audited the open-source application, with academic cryptographers and renowned security analysts like Edward Snowden recommending it for its encryption capabilities. Therefore, Signal users can use it to make encrypted Signal voice and video calls. Alternatively, WhatsApp, the leading messenger platform, uses Signal's encryption protocols for video and voice calls and is suitable for secure communication. Also, organizations can use the Wire encryption app to make encrypted group calls, an essential attribute for protecting details of a highly sensitive conference call.

2. Encrypting Email Communications

Email communication is a widely-used method for sharing sensitive data due to its convenience and reliance over the years. However, attackers have devised various methods through which they can intercept email communications. Luckily, multiple email applications contain built-in encryption protocols designed to safeguard secret chats. For example, users can integrate Enigmail with Mozilla's Thunderbird email client to send encrypted email messages. Mailvelope is also a browser plugin that users can install to encrypt Gmail messages. Also, Protonmail email provides an end-to-end encrypted email service but requires all users to create Protonmail email accounts to send email messages securely.

3. Encrypting Data at Rest in Cell Phones

Android and iPhone users account for the lion's share of mobile device users worldwide. As a result, they store terabytes of sensitive information that can attract malicious individuals, such as hackers and disgruntled friends or family members. Encrypting data at rest is a critical measure for protecting against unwanted access to personal information. Luckily, smartphone storage encryption is fairly effortless. Smartphones enable full-disk encryption, where setting a strong passcode can provide the necessary protection. Biometrics like fingerprints also enables users to encrypt and secure stored information.

4. Encrypting Text Messages

Modern messaging platforms provide end-to-end encryption protocols to prevent cybercriminals from intercepting communicated messages. WhatsApp and Signal are among the most popular messaging services renowned for their message encryption standards. Also, Facebook's Secret Conversations encrypt data communicated through Facebook's Instant Messaging app. However, other messaging services permit users to sign up without providing a phone number. The apps are recommended for phone users seeking some level of autonomy. However, downloading communication applications from third parties rather than the official vendors may introduce security risks like inadequate encryption and backdoors used for data exfiltration.

George Mutune

I am a cyber security professional with a passion for delivering proactive strategies for day to day operational challenges. I am excited to be working with leading cyber security teams and professionals on projects that involve machine learning & AI solutions to solve the cyberspace menace and cut through inefficiency that plague today's business environments.

📁 Cybersecurity

< [Which Industries Are Most at Risk for Cyberattacks?](#)

Sponsored Content

**Eerie Discoveries Still Discussed
Decades Later**
History Daily

**Bra and Panty Sets Adored by
Top Indie Designers.**
brasbuyusanet.com

**[Photos] Historic Wild West - It's
Unbelievable How Much We
Have Progressed Since Then**
The Primary Market

[Gallery] Wonderful Female Athletes Around The World
BetterBe

[Gallery] This Is What She Actually Looks Like In Real Life
DailyForest

Quickly Claim 4 Free Bathroom Remodel Price Quotes Online
BathandShowerPros.com

Recommended by | 

Leave a Comment

Name *

Email *

Website

Post Comment



[report this ad](#)