CALLBRIDGE
by iotum

How To Keep Your Online Meetings Private And Secure

Feel confident knowing your information is private and your connection is secure while video conferencing with Callbridge.

TABLE OF CONTENTS

INTRODUCTION

Thank you for downloading.

Now more than ever we rely on the Internet and technology for our everyday needs, on every level between home and office.

From smart refrigerators to online banking; depositing checks with a click of your camera phone to connecting to hundreds of people through a teleseminar or virtual party or conference call – our information is transferred, and exchanged, sent, and received. Our data travels far and wide.

But just how safe is our information on this interconnected web we have access to? What do you need to know about this ever-changing landscape, and how it affects the way in which you communicate; how your privacy stays private, and security stays secure?

The following ebook is for you if you use video conferencing technology for any reason including running a business and staying connected to friends and family. For these reasons and more, it's critical to be aware of the implications of transferring data online, and knowing which precautions can secure how you send and receive information.

If you're looking to get a more in depth understanding about what privacy and security is and how it impacts the way in which you use technology, the following ebook is loaded with tips, ideas, and tools you can put into action now.

CHAPTER 1

PRIVACY VS. SECURITY

PRIVACY VS. SECURITY

For any type of online meeting, both privacy and security play major roles in the quality and peace of mind of your virtual experience. Together, they safeguard your presence online. Apart, they establish and maintain your cyber safety. You need both in order to engage online safely.

Privacy refers to the rights you have to your own personal information. It's about protecting user identity from being exposed and shared. It means taking the precautions to keep your data away from the reach of unwelcome or unauthorized entities and individuals. Privacy is about keeping your identity locked and protected.

Privacy can offshoot to include:

Personal

Anything that has to do with "private" information in regards to your livelihood and identification, where if the information was known, it could compromise your well-being and negatively impact the quality of your life:

- Social security number
- Credit card details
- Online banking information
- Email accounts and password

PRIVACY VS. SECURITY

Public

This is in reference to the way in which you are responsible for handling other people's personal information as part of your profession. If you are required to handle data that belongs to other individuals, it's up to you to protect it from illegal access.

Corporate

This comprises customer data, intellectual property, patents, NDAs and other sensitive and confidential documents, all of which must remain locked down and unaccessible to unauthorized individuals.

PRIVACY VS. SECURITY

Security refers to the actual access of the data you're exchanging. Where is this sending and receiving of information happening and how accessible is it to unauthorized, unwanted individuals? Security is about maintaining the confidentiality and integrity of the data between point A and point B. It is the barrier put in place so your data cannot be leaked, stolen, or broken into.

Some primary online threats include:

Malware

One of the most common forms of cyberattacks, malware (a portmanteau for malicious software) is a tool that has been designed to infiltrate and penetrate a system or device by way of a weak spot or vulnerability in the security system. Malware attempts to locate and zone in on the system, then attach itself to damage, modify or deteriorate it, and steal and delete data.

Ransomware

Referred to as high-grade malware, ransomware acts as a block, effectively stopping a user from accessing their own personal information. The victim's files are encrypted, and in exchange for their rightful access, the victim must pay the ransom to regain access through a decryption key. Ransomware is most commonly used by way of phishing attacks through an "email" that unleashes a corrupt file that attacks the user's info.

Phishing

You know those calls or emails that claim you have won an all-expenses-paid trip or a prize? This is the oldest trick in the book, but remains as a very popular one. Not only does phishing exist in the form of fake emails, websites and text messages, these attacks are designed to steal personal information, and can be quite costly and detrimental.

Privacy requires taking the precautions to keep your information and data hidden or out of reach of attackers, while security refers to keeping that data locked and inaccessible from attackers. Together, they are a unified force that protects you whenever you're engaged online – and most importantly, one that needs to be implemented while using video conferencing.

CHAPTER 2

PRIVACY CONCERNS

PRIVACY CONCERNS

Your personal information should be just that – personal. Although it's an umbrella term, personal data refers to any information that is uniquely yours. The obvious includes the previously mentioned information (ex. credit card details). The sort-of-obvious includes social media posts, location data, what you type into Google, etc. And then the really not-so-obvious data includes how you uniquely use technology, the patterns of keystrokes on your personal computer, etc.

Where does my personal data go?

Consider how when you download an app, you are prompted with an "Allow Location" message or how when you go from one website to the next, there are retargeting banners that follow you based on your search history.

Any and all of these scenarios and more scrape up your info and can be sold to third parties. This can even happen when you willingly sign up for a new trial or enter your information with the intention of only signing over your info to one company. Unbeknownst to you that information is sold to a third party without your consent. Without strict privacy laws in place, this is how info gets leaked.

PRIVACY CONCERNS

Who has access to it?

Consumers are aware of the information they are signing over – sometimes. They are happy and consenting individuals who want to give out info in exchange for a product or service. It's when personal data is taken, stolen and given away for a company's own profit or benefit to data brokers, however, that it becomes a problem. Anything from medical records, social media connections, online visits and purchases are bought by firms for research purposes or for ways to figure out how to sell to consumers better and more directly.

How is data protected from third parties?

You can't always be certain whether or not companies are selling to third parties. A good indication that they aren't is if they're compliant with General Data Protection Regulation (GDPR), considered the tightest privacy and security law in the world. Companies cannot collect or share your data without explicit consent.

In fact, any video conferencing service that isn't GDPR compliant should be reconsidered. Why take the risk? Keep your data protected with regulations put in place specifically to be out of reach of third parties.

PRIVACY CONCERNS

Considered the tightest privacy and security law in the world, the GDPR was created and regulated as a set of obligations for organizations to adhere to when it comes to targeting people and collecting their data in the European Union. Even if you aren't in the EU but you still have clients or offer goods and services or process the data of EU citizens or residents, the GDPR still applies. Key regulatory points include:

- Data protection principles
- Proving GDPR compliance
- Data security and organizational measures
- Data protection principles
- When you're allowed to process data
- Consent to process information
- Appointing data protection officers
- The privacy rights of people

Mitigate any potential for risks when considering how video conferencing software transmits information by ensuring the conferencing company provides:

- Privacy commitments in place for the user which means no ads, no selling to third parties and no external info scraping.
- Immediate termination of private info and data upon subscription completion.
- Access to your own customer data for any time or reason.
- Encrypted data storage on a secure network of protected servers.
- Technology that meets international standards like HIPAA, GDPR and more.

CHAPTER 3

SECURITY CONCERNS

SECURITY CONCERNS

Creating a safe space for information to be sent and received is a must for companies, organizations and even households. No one wants to be engaged in an online meeting only to realize that their information was broken into and tampered with. Fortunately, there are plenty of security measures that can be put into place to protect your information.

Breaking Down Video Conferencing Security

Whether it is for for personal use or for financial institutions, medical practitioners, law firms, military and most other forms of business, video conferencing won't be successful without security measures.

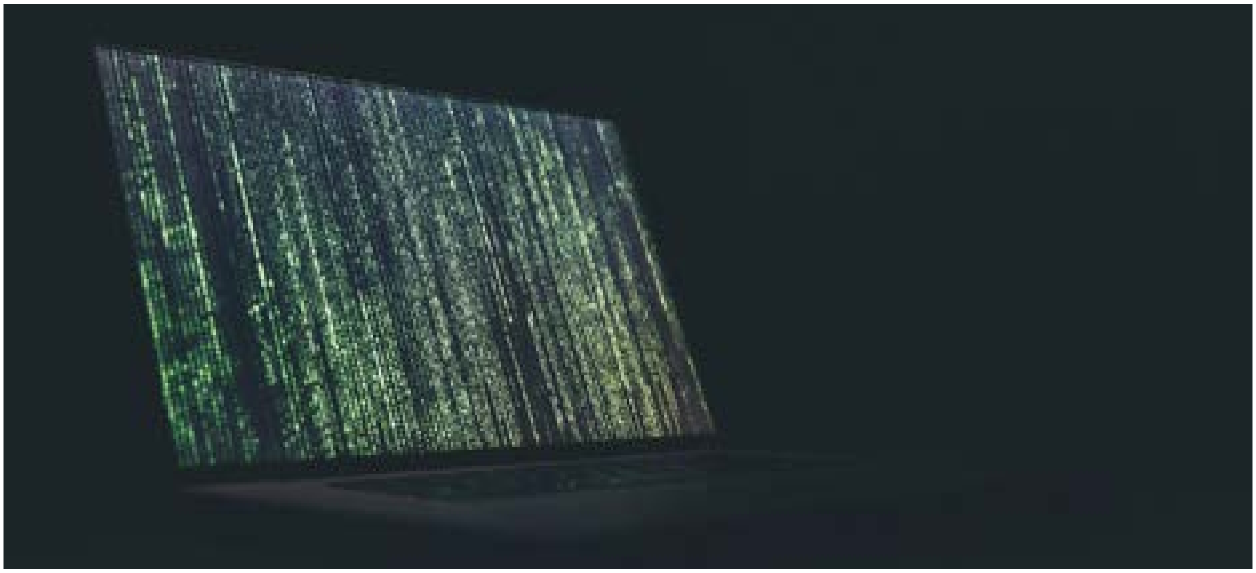
A video conferencing platform that is secure must have data storage and data transmission strategies.

Data Storage:

Most often, video conferences are saved and revisited later. Attendees can record, and capture the conference, and save on their own device or save to storage (cloud). Any information shared, discussed and transmitted through these video conferences can be sensitive or not meant for anyone else other than the attendees, therefore when it comes to storage, data needs to be locked down – physically.

Video conferencing services that operate using a subscription-based model typically store all video-conferencing data in facilities that are offsite, locked down and protected by 24/7 surveillance. Access is highly restricted and those who do have accessibility must go through additional levels of security that include scanners, key cards and more.

SECURITY CONCERNS



Data transmission:

The more vulnerable aspect of the two, video conferencing security must work to protect the integrity of the information being sent and received. This is where the data gets bounced around multiple times amongst public and private networks between the sender and receiver.

Security comes down to two basic components:

- Implementing a firewall or filtering device that protects the video conferencing system
- Using encryption to protect video streaming

Depending on the classification of information being transmitted, commercial-grade encryption is utilized by many companies at every endpoint and bridge location. Video conferencing that uses encryption and certificate-based authentication is extremely critical to the success of transmitting sensitive data (or any data) over networks.

With Callbridge's 2-person encryption and added security features like Security Code, you can feel confident knowing you're preventing hackers from stealing your data. Adding an extra layer of protection with a Security Code grants access to participants with the code, and keeps unwanted individuals out.

SECURITY CONCERNS

Encryption, one of the most important security features, strives to keep sensitive data safe from leaking by scrambling discernable text that can only be "unlocked" with a decryption key. Digital eavesdropping ("being spied on") happens when data gets stuck in between storage and transit, making it vulnerable to theft. Therefore, security depends on the devices that are hosting your information. Callbridge's 2-person encryption ensures safe transit between machines. When you hit send, your data is converted into scrambled code at the beginning point then unscrambled and deciphered at the endpoint. This is especially necessary when info is transmitted through the Internet. Before the information is sent and available to be read by the receiver, the scrambled data is reassembled back into its original, readable form.

Encryption prevents third parties like law enforcement or malicious government from spying on your calls. Hacking is a thriving global business and with encryption, you can rest assured knowing the transmission of your information is safe.

CHAPTER 4

VIDEO CONFERENCING PRIVACY AND SECURITY NEEDS MET

VIDEO CONFERENCING PRIVACY AND SECURITY NEEDS MET

Choosing video conferencing technology for your work and or home life doesn't have to be an overwhelming process, nor do you have to be extremely savvy when it comes to understanding how it all comes together. **Callbridge covers your privacy and security.**

Callbridge's robust software does the heavy lifting for you, and comes with all the features required to communicate safely and privately. Instead of having to seek out the details regarding protocols, encryption technology and beyond, choose software that comes outfitted with the tools and features of the trade to give you peace of mind and confidence knowing you made the right decision.

Security and Moderator Controls:

This gives the moderator full control of how a meeting is set up, from sending links in an email to organizing attendees and sending out automatic invites and reminders. With Callbridge, moderators can add another layer of protection by asking attendees to enter access codes and pin numbers and implement high grade security features like One-time Access Code, and Meeting Lock, to name a few.

Moderators have the ability to secure the conference room. Everyone in the room is visible in the participant list – there are no hidden individuals. It's easy to remove or block unwanted participants by simply hitting "block." Use the "lock" button in the online meeting room to ensure your meeting is sealed off.

Plus, conferences can be organized to include an online meeting room before they start, giving mods the opportunity to kick out unauthorized people and only admit invited participants. In webinars for example, moderators can set it up so attendees are restricted from distributing content to each other or elsewhere.

VIDEO CONFERENCING PRIVACY AND SECURITY NEEDS MET

Consent and Secure Retention:

Participants must be notified if the meeting is being recorded. When video conferences are automatically set to record or the moderator starts recording without permission, this raises questions of privacy and security, and could cause legal trouble if not looked after.

Meeting organizers need to communicate whether or not a session is being recorded and need to make it understood that no one can record it with any outside devices. Participants must consent or be aware of the policies in place.

Furthermore, storage must be secure. Where are the recordings going and what are the retention methods in place? With Callbridge, storage is cloud-based and able to store all encrypted recordings for easy access and locked down storage.

Consider the use of strong passwords, and multi-factor authentication when it comes to storing, and retrieving these recordings and files down the line.

Due Diligence and Agreements:

What privacy and security controls make sense for the information you are passing along online? Do your policies contradict or empower the purpose for your conferences? Callbridge's privacy and security information is available online for anyone to read and get better acquainted with. If you want to know more, visit here and don't hesitate to call support and learn about what can be done to provide you with the assurances you need to conduct business safely and securely.

CHAPTER 5

TIPS AND BEST PRACTICES

TIPS AND BEST PRACTICES

Audio and video conferencing software is designed to make communication fast, simple, and effective, and should come loaded with security features that keep you and your information safe. There are, however, precautions and measures you can take into consideration that reinforce how you communicate.

Here are a few generalized ways in which you can create safe privacy and security habits whenever you are present online, from surfing the web to engaging on social platforms:

- Limit what you share online via social media. With so many eyes on your wall, account, and page, it's easy for hackers to build a "file" about who you are to gain your trust. Keep your profile sparse and adjust your privacy setting accordingly.
- Avoid any potential phishing scam – if you don't recognize an email address, don't click on it. Only open mail from recipients you know and trust.
- Keep devices protected with antivirus programs and always update software. Don't use old and outdated software that hasn't been upgraded. Old bugs, vulnerabilities and weak spots leave you open and susceptible to attacks and infiltration.
- When entering your credit card number to make purchases online or subscribe to a service and more, have a quick read over the company's Privacy Policy. Check how they collect and use information. A good rule of thumb is to keep an eye out for any mention of GDPR. Even though it's meant for EU citizens and residents, chances are the service has taken the necessary measures to be extra considerate of customer privacy in general.

TIPS AND BEST PRACTICES

Follow these tips and best practices for heightened privacy and security when you engage in online meetings and conferences:

Be Selective

Choose software that stands its ground when it comes to privacy and security. Before you buy, try a trial. Learn why they claim to be secure, and compare their product to other competitors to make sure you are getting the most value and quality for your specific needs.

Pro-tip: Free trials of 30 days and up are often a good sign that the company is interested in retaining you as a customer. Anything less isn't enough to really get the most out of exploring the layout. Use the free trial to poke around and get a good feel for how you can benefit from its use.

TIPS AND BEST PRACTICES

Rely on Secured WiFi

For sensitive information, rely on connecting your handheld device to a secure WiFi network rather than 4G. Information passed through a phone call or text message is convenient, but for confidential info, sharing it through a cell tower is far less secure. This also applies to publicly accessible networks found at libraries, airports and cafes.

Switch up Passwords

It's easy to want to use one password for everything, but it's common knowledge that frequently changing your password is the best way to keep your data protected. A strong password has a combination of letters, numbers, upper case, lowercase and special characters. Aim for 9 characters and over.

Pro-tip: Come up with your own personal algorithm that is easy to remember but is unique to every site you use. For example:

- Decide on a length (ex. 6 letters + 3 numbers)
- The first 6 is the brand's name, uppercase
- The following 3 is an animal that starts with the same first letter
- Use your favorite number
- End with your favorite punctuation mark, twice

For Callbridge, it would look like: CALLBRcat17!!
For Amazon, it would look like: AMAZONant19??

TIPS AND BEST PRACTICES

Consider the Info You're Sending

What information needs to get sent across and is it necessary? How sensitive is it and is it required? Do a sense check and consider other ways of getting the information across. Is there another or more creative way of communicating it or another option that bypasses the need for it to be sent?

Mandate Audio and Video Conferencing Policies

Discuss with your team or office about creating a conferencing policy that outlines best practices with everyone's best interests in mind. Highlight video conferencing etiquette, rules and procedures for a clear understanding of how to have a safe and private meeting everyone can be a part of securely.

TIPS AND BEST PRACTICES

Here are a few secure video conferencing policies to discuss and agree on. Put these in place for the safety of everyone involved, including their own personal information and company data:

1. Participants must receive permission from any everyone on the call before recording a video conference.
2. Only one person is allowed to record using the video conferencing software – no mobile phones allowed.
3. Remove confidential data from the camera's view and opt for a clean and clear space at a desk or conference room.
4. If possible, designate a room or space specifically for video conferencing so information cannot be overheard or seen.
5. When not in use, ensure cameras and microphones are shut off.
6. If you need to use a remote camera, only one person should be in control and it should be an authenticated user only.
7. Create a new PIN for every meeting.
8. Agree what kind of information can be discussed in a video conference and who can attend (ex. which clients, employees, etc.)

Stay on top of what's happening online with technology that is new and/or updated. Older versions do not age well with time, leaving your information open to security vulnerabilities, changing algorithms, outdated software and lack of sophisticated scanning systems. Plus, old data encryption methods won't do you, your clients, customers, employees, patients and reputation any favors if data is at risk.

Stick with conferencing software that comes loaded with security features and stays up to date for you, making sure all you have to worry about is your business while privacy and security is taken care of in the background.

CHAPTER 6

ABOUT CALLBRIDGE

ABOUT CALLBRIDGE

Privacy and security is of the utmost importance when running a business and protecting clients, intellectual property, personal information, trade secrets, and so much more. Video conferencing software that's able to safeguard exchanged information between sender and receiver builds your reputation as being reliable and forges trustworthy partnerships with clients and customers.

From account creation, to payment details and before, during and after conference calls, Callbridge's web conferencing two-way communication software takes both privacy and security seriously.

The 3 features that work hard to keep your privacy and security at the forefront:

1. Meeting Lock

   Start every meeting by locking the session to keep out unauthorized participants from intruding. Latecomers are still welcome but will be required to ask for permission.

2. Security Code

   When discussing confidential information, add a conference security code to the meeting for reservation-less and scheduled calls. Only those with the code are granted access to the meeting.

3. One Time Access Code

   Choose from using a default access code or a randomly generated one-time access code that is unique to the call. Encrypted and bespoke, it is only valid for a specific call and for its duration.

ABOUT CALLBRIDGE

Plus, Callbridge offers a highly secure and private platform:

- Point-to-point 128-bit encryption
- Fully encrypted via WebRTC
- Granular privacy controls
- Recognized by the Canadian Anti-Spam Legislation (CASL), HIPAA Seal of Compliance and GDPR compliant

Callbridge's guiding principles for safe and secure conferencing:

- Moderators Have the Ability to Secure the Conference Room

  Everyone in the room is visible as seen in the participant list. It's easy to block, remove or grant access to latecomers. For an extra layer of protection, add one-time access codes and security pins to your meetings, and lock the room to ensure the meeting is closed.

- Every Conference Comes With a Security Code

  Add a security code to the meeting that when enabled, all participants must punch in to join the call.

- Available Access Codes and Moderator Pins

  If there are previous participants who have the access code; or if there is a high turnover, company restructuring or if the details were shared with an unauthorized individual, the access code and moderator PIN can be changed at any time. Anyone with the old code will not be able to access future meetings once the code has been reset.

ABOUT CALLBRIDGE

- Personal Information is NOT Shared
  Your information is given to us and stays only with us. It doesn't go anywhere else and isn't sold to a third party.
- Encryption
  Media, links, documents – anything that is sent and received is encrypted to our server, and then decrypted so it can be processed and encrypted again before being sent to participants. All two-person point-to-point calls are encrypted.
- Safe and Secure Desktop App
  Installed and verified to be secure by VeraCode as part of the PenTest run in late 2019.
- Top-notch GDPR Compliance
  Known as the gold standard for privacy protection worldwide, the GDPR's principles and rules are closely adhered to.

Let Callbridge's world-class video conferencing technology meet your business' security needs, providing you with the peace of mind that your data and information is safe and sound. State-of-the-art features like Meeting Lock, Security Code and One-time Access Code are optimized to keep your meetings authorized and locked down.

With cutting edge technology that works behind the scenes to safeguard your data, you can focus on work and play while your information and privacy is taken care of in the background – no matter what you're working on with Callbridge as your web conferencing provider.

Start your 30-day complimentary trial here.

START FREE TRIAL