Data
22 de Junho de 2025

Benchmark and Multidimensional Analysis of Security in Video Calling Software

DeCast - GetBoarded

PCI · Creative Science Park – Aveiro Region
Via do Conhecimento
Edifício Central
3830-352 Ílhavo

Portugal

+351 234 243 750
(chamada para a rede fixa nacional)
pci@pci.pt
www.pci.pt

NIF 509 574 254

1. Description

This document aims to carry out a comprehensive analysis of security, not only from a technical perspective, but also considering emotional, symbolic, cultural and behavioral aspects. Through a benchmarking between the main video calling softwares — Zoom, Microsoft Teams, Google Meet and Discord — the security strategies adopted by each will be discussed, crossing them with theoretical concepts and elements of everyday life that influence the perception of security of users.

2. Context

Factors that contribute to the feeling of security

Emotional/Symbolic Safety	**Physical/Systemic Security**
Welcoming space Places with friendly or familiar people, adequate lighting and visual elements that convey comfort and protection.	**Controlled environments** Well-lit, organized, and monitored spaces — or digitally, waiting rooms, permissions, and sharing limits.
Rituals and routine Daily habits, such as drinking coffee in the morning or checking your phone before bed, create predictability, reinforcing the feeling of control.	**Visible signage and rules** Padlock icons, recording warnings, or clear visual feedback on connection status.
User-friendly technology Intuitive interfaces that allow easy control over audio, camera and screen sharing increase user confidence.	**Authority presence** Moderators, hosts, or administrators who can intervene in case of inappropriate behavior.
Personal privacy Ability to use pseudonyms, keep the camera off or personalize the digital environment.	**Control technology** Encryption systems, secure authentication, and action traceability (event log).
Trust Linked to the brand or the reputation of the platform, as well as its security certificates.	**Security automation** Facial recognition, sensors, artificial intelligence for automatic moderation, etc.

Empathy Non-violent language, respectful feedback, or experiences that demonstrate genuine concern for the well-being of users.	**Culture of responsibility** Rules of conduct, code of ethics, and the ability to report abusive users.
Mental health Access to tools that avoid cognitive overload, and virtual environments that do not cause stress or anxiety.	

Dimensions of Security in Software

To build a coherent structure for analysis, six key dimensions of security were defined:

1. Technical security	• Encryption; • Authentication; • Access control;
2. Emotional/symbolic security	• Interface clarity; • Language tone; • Predictability of system behavior;
3. User privacy	• Control over personal data; • Anonymity options;
4. **Mental health**	• Minimizing notifications; • Meaningless notifications; • Interface overload;
5. **Session moderation**	• Host control over participants; • Permissions;
6. **Culture and inclusiveness**	• Support for diverse languages; • Accessibility; • Backgrounds;

3. Benchmark of video calling software (user-centered security)

	Zoom	Microsoft Teams	Google Meet	Discord	Decast
End-to-end encryption	✔	X	X	X	?
Easily control of the microphone and camera	✔	✔	✔	✔	✔
There is a waiting room or a control over who enters	✔	✔	✔	✔	X
Allows to use fake names or remain anonymous	✔	X	X	✔	✔
Provides visual alerts when someone is recording	✔	✔	✔	-	✔
The organizer has control to mute and expel	✔	✔	✔	✔	✔
There is a button to report inappropriate behavior	✔	X	X	✔	X
Customizable name	✔	X	✔	✔	✔
Customize background in video call	✔	✔	✔	✔	✔
It has inclusive features like subtitles or translation	✔	✔	✔	X	✔
Notification of entry / exit of participants	✔	✔	✔	X	X
Sound/video on indicator	✔	✔	✔	✔	✔
Easy exit from call	✔	✔	✔	✔	✔
Request permission before sharing screen	✔	✔	✔	✔	✔
Visible call time	✔	✔	✔	X	X
Intuitive / Information clarity	✔	✔	✔	✔	X
The host has the control	✔	✔	✔	✔	X

4. Benchmark overview

Zoom	• It's a balanced platform. • It gives us the tools to control everything with clarity and security. • We feel in control of the call and protected. • Ideal for both work and personal use.
Microsoft Teams	• Ideal for companies. • It feels like a professional environment with well-defined rules. • It can seem too rigid and unwelcoming for informal or personal contexts.
Google Meet	• It's simple and reliable. • It's linked to your Google account and so provides security; • Doesn't allow you to be as anonymous or flexible. • It works well for those looking for something quick and straightforward.
Discord	• It's the most informal and social. • It gives us the freedom to be whoever we want, with avatars, names to choose from, and themed rooms. • It may not be ideal for work, but it makes us feel at home, especially in groups or communities.

5. DeCast testing overview

Issues	**Action required**	**Proposal solution**
The guest joins without needing authorization or notification; Anyone who gets the link can access the call; In configurations panel the options for blocking features are also not clear, as I tried to block the public chat and everyone was able to continue using it.	The host must be able to ensure that all configs and permissions are setup before call's starts;	Define a step-by-step config wizard when creating a chat session;
Anyone can take control of the meeting and the host can easily lose their position; We need to be always aware of the "users" tab to confirm who are in the call;	The host must keep control on entirely the call;	Define an easely accessed control panel for host view with all settings and options for during call actions;

There is no report button, meaning if we want to remove someone, there is only the "remove user" function and then select whether we want them to be expelled just once or permanently from that room. The person can easily re-enter in anonymous mode.		
Anyone who joins the call with mic and camera unable isn't noticed by others; The recording call is not well perceived by others;	All activity from others should be noticed by host and the others;	Define all the necessary notifications and alerts well visible for host and others;
When a participant is excluded, the message that appeared is unclair. In the bottom left appears a code text without context	All the technical messages should be avoided and replaced when needed by user-friendly messages;	Review all the message texts;
The button to end the call itself is not intuitive, it should at least be red. Muting the users on the call is also not intuitive. There is an icon but need to enter secondary menu;	All the relevant actions should be well noticed (ex: recoding; participants list);	Convert iconography and color scheme to standards and well recognized actions to take Minimize 'clicks' to take relevant actions;

6. Next steps

6.1. Redefine user flows;

6.2. Review text messages;

6.3. Review critical technical security issues;

6.4. Wireframe prototyping;