BUNKR Q&A

SPORTS®

Everything you need to know about BUNKR's mission to protect players and power the future of sport

How did BUNKR come to be?

BUNKR is founded by **successful information security entrepreneurs** who saw a broken system.

Everyday technology tools are built with fundamental **security and privacy vulnerabilities** that allow companies to collect and exploit your data

These business models prioritize data and growth over the financial, mental, and spiritual **well-being** of people

We knew we could do better—and we did. BUNKR is built to put **safety, security, and privacy** back in your control while maximizing productivity.

"Privacy is a human right."

BUNKR never sells or provides customer information to any third-party. **Ever.**

Our privacy policy is written in easy to understand terms. Find it here:

https://bunkr.life/privacy-policy/

BUNKR eliminates the top threat-vectors bad actors use to commit cybercrime and fraud, keeping people safe and secure.

What does BUNKR deliver?

Secure Messaging
Private invitation-only communication & document sharing with the people you trust

Password Management
Store and manage passwords securely and privately

Secure Cloud Storage
Organize and protect your files such as IDs, health records, & travel documents,

Notes
Capture your private thoughts, to-do lists, travel, business, prayers, ideas & health

"Privacy is a human right"
BUNKR never sells or otherwise provides customer information to any third-party

Secure Audio and Video (2026)
Later in 2026 we'll deliver secure audio and video calling

Our Mission

The BUNKR mission is to provide the **safest place on the Internet** for people to collaborate with those they trust, empowering them to reach their fullest potential and focus on what matters most to them in their lives.

The BUNKR founders and entire team **use their own product** throughout their lives and within our business.

You can find more about our vision & values at:

bunkr.life/vision-values

Q&A | Page 2

What specific risks in platforms like WhatsApp, Discord, and Snapchat are you solving for your clients?

The following risks are not edge cases - they are threats built into the foundation of modern communication platforms and fall into four primary categories:

1 Privacy, Personal Sovereignty, & PsyOps

- Modern platforms are built on the foundation of data collection & the exploitation of personal information
- Vague privacy policies allow them to collected, share, & sell personal information to third parties for "business purposes"
- Advertisers & third-parties manipulate and shape human behavior using established psychological techniques
- These PsyOps or "Psychological Operations" manifest as fear based algorithms which shape purchasing, voting, culture, & beliefs - often inviting domestic and foreign governments to manipulate people through fake ai-bots

Result: People unknowingly give up control of their personal sovereignty

2 Data Breaches & The Dark Web

- These modern communication platforms store massive amounts of personal data - making them prime targets for cybercriminals
- Personal information sold on the dark web is the fuel for cyberattacks & personal fraudulent attacks aimed at financial pay off
- Data breach reporting requirements in the industry are weak due to governmental lobbying
- These data breaches are only discovered when the platform's customer data is validated as for sale on the dark web by info security analysts

Result: Your most sensitive information becomes readily accessible to criminals

3 Cybercrime Exposure

- Compromised data enables large scale automated attacks (crime-as-a-service)
- Cybercriminals in countries without extradition treaties exploit built-in vulnerabilities in common technology platforms, leaving law enforcement with limited ability to act unless the attacker's location allows prosecution
- Cybercrime is now the world's third largest economy at around $ 12 Trillion, trailing only the GDP of the United States of America and China. It is difficult to fathom the financial, mental, and spiritual impact of this fact has on human beings.

Result: Individuals and families face constant financial, mental, & spiritual threat

4 Physical & Psychological Threats and Lawsuits

- Rapid rise in psychological and physical threats across common tech platforms—including grooming, bullying, human trafficking, fentanyl distribution, AI-generated exploitation, scams, and organized crime
- The availability of personal collected personal information on the dark web and vulnerabilities of common tech platforms facilitate these threats to be conducted at staggering scale.
- Ongoing wave of serious lawsuits against major platforms, citing deceptive practices, negligent design, inadequate monitoring, and harm to people

Result: Digital threats carry real-world harm & it's well documented

→

Q&A | Page 3

What evidence, research, and real-world cases shaped BUNKR's design decisions?

There are vast statistics and facts available which BUNKR's founders considered, we will provide just a few:

Global Scale

$12T

Cybercrime is now the World's third largest economy

at $12 Trillion and growing unabated

Child Safety

300M+

Children are victims of technology-facilitated sexual exploitation & abuse

Including non-consensual sexual images & video

Mental Health

46%

of minors experience online bullying

60 and 80 % of those having one or more **long-term effects including PTSD**

Delivering **Bank-Level Security** for Every Family on Earth

BUNKR removes the vulnerabilities these systems exploit. BUNKR delivers "bank-level" security at price point every family can afford. In the near future we will release a fully free version of BUNKR so that every person on Earth has access to bank level security.

What does "secure" mean in BUNKR in concrete terms? Is it end-to-end encryption, and who holds the keys??

Built on Proven Security Standards

For decades BUNKR founders **protected hundreds of millions of patient records around the world** in accordance with HIPAA and related regulations as well as trillions of wealth in accordance with FINRA, SEC, GDPR and other global regulations. Thus, BUNKR is built on the strictest privacy, security and compliance foundations including SOC 2 Type II.

1 End-to-End Encryption

Your data is encrypted at every stage - creation, storage, and transmission.

Using industry-leading encryption standards to keep your information secure and protected

2 You Control the Keys

Encyption keys are managed using Micosoft Azure Key Vault

BUNKR never sees or holds your keys. Ever.

Your data is secure and only you have the key.

3 Built on Proven Security Standards

BUNKR is founded and developed by security leaders who devoted their life to protecting:

- Hundreds of millions of patient records (HIPAA)
- Trillions in financial assets (FINRA, SEC)
- Global data systems (GDPR, SOC 2 Type II)

BUNKR Security: Protecting Your Rights

Can any third party (including BUNKR) access message content under any circumstances?

No. Only valid under a court order. Never otherwise.

Protecting U.S Citizens via The Bill of Rights

BUNKR is owned and operated in the United States which **enables legal protection of our customers' privacy through the U.S. Bill of Rights.**

Protecting non U.S. Citizens via MLAT

For non-citizens, our location in the United States **enables legal protections through the Malta Mutual Legal Assistance Treaty MLAT.**

Your messages are your business

To date, we have **never accessed a single customer message or data element, ever.** Nor have we been requested to access any customer content by any government.

Because BUNKR vets our users and we our platform does not lend itself to criminal use, we do not face government disclosure pressure that platforms with massive numbers of imposters, criminals and bots.

What are the risks of alternative approaches?

1. **Growing Regulation.** Businesses holding customer information and operating outside of the United States including the UK, Europe and others are **subject to growing local regulation** which requires cooperation with government authorities. Increasingly these governmental authorities require personal information collection without a firm due legal process.

2. **Undisclosed Data Collection.** Alternatively, if the country of operation has lax privacy laws, the business may **capture and use customer-athlete personal information** without notification for sale to third parties.

3. **Complex & indirect Privacy Policies.** Finally, the privacy policy of any solution should be easy to read and understand regardless as to the country of operation. If you **cannot understand the privacy policy** of the solution provider there is a very high probability, they are capturing sensitive information on their users and selling it without full disclosure.

Q&A | Page 5

How do you prevent unknown users or strangers from entering a client's communication environment?

By default, we have a **patent-pending design** that has been implemented and requires a formal invitation and acceptance process before any message can be sent. **Under no circumstances** can a BUNKR customer receive a message without going through our invitation & acceptance process. Further, under no circumstances can a customer be "discovered" on BUNKR.

Invite-Only System

A formal invitation and acceptance is required before any message can be sent

No Unsolicited Contact

Users cannot receive messages outside of this approval process

Zero Discoverability

Customers cannot be searched, found, or "discovered" on BUNKR

Protecting you from **Fake Accounts & Identity Spoofing**

BUNKR provides safeguards against impersonation, fake accounts, and identity spoofing through our patent-pending design. We provide a formal invitiation process where the user's identity is verified before they ever make contact.

"We don't use AI to replace parents."

What level of parental oversight does BUNKR enable?

View messages?	**Yes.**
See summaries or flagged risks?	**No. We do not use AI to replace parents.**
Set Permissions? (e.g. who can be contacted?)	**Yes.**
Stop conversations from being deleted?	**All conversations are archived if required for a legally authorized investigation.**
Can oversight be adjusted based on age maturity?	**At the parents discretion**

How are group chats structured differently from platforms like WhatsApp or Discord?

- BUNKR gives parents **100 % control** over who can join—only known and trusted people.
- BUNKR gives 100 % control and **visibility** on who joins a workspace.

Are There Limitations on:

Group size? No Technical Limitations. BUNKR groups contain only trusted people.

Forwarding Messages? No. There is no forwarding.

Viral Spread of Content? No. There is no concept of viral spread on BUNKR

What design choices do you make to reduce addictive usage patterns?

Giving Customers Time Back to **Focus on What Matters Most**

We do not attempt to manipulate our customers in any way whatsoever. "Addictive usage is not a concept for BUNKR. In fact, a fundamental BUNKR design goal is to always give our customers time back in their day to focus on what matters most to them.

Are there features like:

- Streaks. **No, and there isn't anything close to equivalent in BUNKR**
- Read receipts. **No, although we do have message delivered confirmation checkmarks**
- "Last seen". **No, there is no concept like this in BUNKR**
- Algorithmic amplification. **No. We have no algorithms observing our customers.**

We believe our customers have **personal sovereignty** to connect only with people they know and trust, then decide how they wish to collaborate with them.

How does a client join BUNKR?

Families, teams and individuals can join BUNKR through our web site at https://bunkr.life

Can they sign up independently, or must a parent initiate access?

Due to our registration requirements, BUNKR is a platform in which parents purchase a family plan account and add their minors. BUNKR has minor accounts which parents can activate which gives the parent total control over who is connected to their minor children.

How do you verify that users are:

Real People

BUNKR leverages a range of techniques to ensure all accounts are real people including the requirement to have valid Apple or Google registered accounts and a requirement to have payment on file. We also employ proprietary techniques.

Age Appropriate

Due to our registration requirements, BUNKR is a platform in which parents purchase a family plan account and add their minors. This helps keep you and your family safe with a birds eye view of access.

Trusted & Known

BUNKR by design and default does not allow any messages whatsoever to be sent without an invitation and acceptance process which is initiated by both parties being in one another's phone contact.

For group, teams and business purchases, there is an option for a central administrator to **auto-connect known and trusted persons together.**

Is there a closed network model?

Yes by default, based on a patent-pending design and is not optional. For minor accounts, parents can have **100 % control** over who can ever propose connecting to minor children

A Closed Network Model: Full Administrative Access & Control

Only known, trusted connections to keep you and your family safe— providing you with complete visibility and control

How to Think About BUNKR

Is BUNKR a replacement for mainstream messaging?

No and Yes. People will continue to casually use insecure but vastly adopted communication tools. And there will always be people who do not value their person sovereignty. A fast-growing number of people are trusting BUNKR to collaborate with their most trusted people. As our customers have learned they can trust BUNKR, they do move more & more of their life to our platform.

Is BUNKR a transitional Transitional tool?

Yes and No, BUNKR is an on-going platform that families and high performers will trust and rely on for decades to come. BUNKR has customers in over 145 countries who rely on us every day to secure the most sensitive and important aspects of their lives. So, in a sense BUNKR does transition the mission-critical aspects of our customers' lives from vulnerable technologies to a trusted platform, BUNKR.

Is BUNKR part of a broader ecosystem of delayed tech adoption?

Yes and No. BUNKR does work seamlessly with complementary technologies of all kinds and already has partnerships with like-minded organizations around the world. But BUNKR is a sanctuary designed for the flourishment of human beings in which they are protected from technologies which do not have human beings' best interests at heart.

Protecting Players. Powering the Future of Sport.

www.bunkr.life