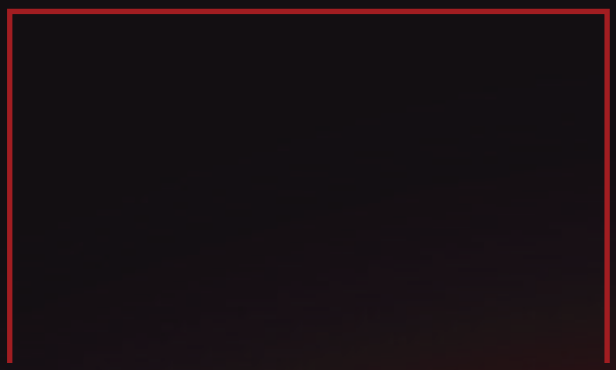
theZphone

Encrypted Mobile Communication

zezel.com
Mobile: Message. Manage.



Secure your mobile data against any threat.

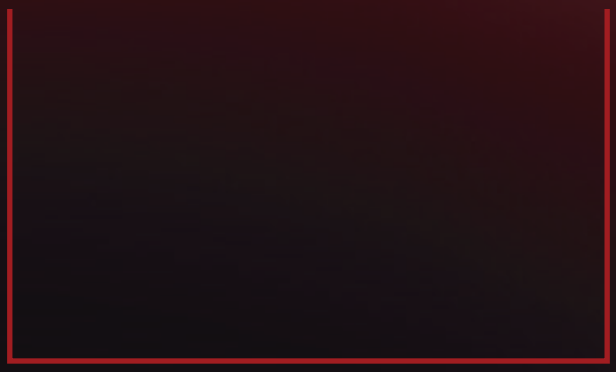


Table of Contents

Regain your Privacy in the Digital World

Can you have data security in the world of mobile communications? The number of agents that have the technological means and incentive to intercept your messages or calls is too high for the answer to be anything but a resounding no.

Zezel.com is a company founded to change that answer into a yes. With the help of the right technology, implemented in the right way, yes, you can regain the security of your data!
theZphone is the pinnacle of our efforts to achieve that aim.

This device comes with its own data plan, runs on a custom operating system, has a suite of special security apps, and uses only encrypted channels for all incoming and outgoing communications. It has been designed to prevent eavesdropping, avoid wiretapping, block malware and spyware, hamper location tracking, and keep your information safe even if the device gets stolen or taken away.

theZphone is the solution you need if you truly value your data and its security.

The Verticals We Protect

GOVERNMENT AGENCIES

Governments handle information of national security importance, as well as the personal data of citizens. Securing it is an absolute must.

POLITICAL PARTIES

Breaches in political campaigns can lead to meddling in the democratic process. Encrypted communications can hamper such attempts.

SECURITY & DEFENSE

Ensuring the safety of people and property requires secure and reliable communications that rule out interception by third-parties.

ENERGETICS

Data leaks in the energy and drilling sector can affect commodity prices and take down markets and economies. Securing communications is a must.

PHARMACEUTICALS

R&D data is one of the pharmaceutical industry's most highly valued assets. Ensuring it is transported securely is absolutely imperative.

FINANCE & BANKING

Using reliable authentication processes is crucial for preventing financial fraud. Our encrypted communication apps provide just that.

SMEs

You don't have to be a multinational corporation to need security, as most cyberattacks target SMEs. Our solutions can secure businesses of any size against cybercrime.

360° Secure OS

The operating system of a smartphone is the foundation for all other software on the device. For theZphone, the aim was to make this foundation as secure as possible. The device runs on Secure OS – a highly modified version of Android 8.1. It focuses on preserving the user-centric experience, drastically reducing the attack surface, and offering extensive security features.

Triple Password Protection

Gaining physical access to a secure device, could give third parties an easy way to collect sensitive data. To protect users against tampering, theZphone requires different password authentications to allow access to the encrypted storage, the OS, and each of the communication apps.

Anti-tamper Wipe

theZphone's bootloader is locked: if anyone tries tampering with it, the device will wipe all stored data. Android's recovery is also modified, to reinstall Secure OS after a wipe or factory reset.

Vulnerabilities Purged from OS

NO GOOGLE SERVICES:

Google's set of APIs that developers utilize in their apps embed things such as location-tracking within Android itself. To ensure that users are not tracked by different apps, all Google Services are completely purged from the phone.

ANTI-DATA-MINING

Regular Android lets apps share data through the content provider that handles the process. In Secure OS, the content provider is modified so every app can access only its own application package blocking all spyware from mining data from your apps.

DISABLED HARDWARE FEATURES

The Kernel is the part of the OS that contains the drivers for the phone's hardware. Our Mobile Device Management (MDM) platform allows disabling features such as the USB, NFC, and Bluetooth, which are easily exploitable.

LIBRARY SECURITY

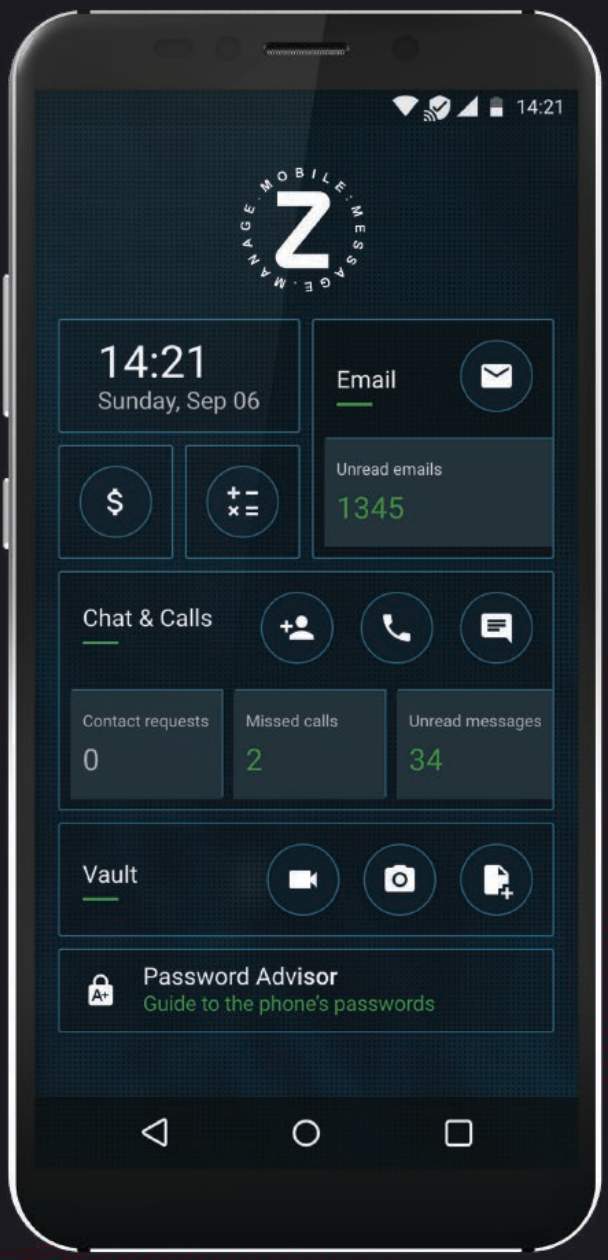
All the libraries of the device, serving as sets of pre-written code used by all apps, are security-hardened. These include SQLCipher, which encrypts the databases of the communication apps with the AES-256 cipher, and an IP Table Firewall, which performs intrusion prevention.

BOOT INTEGRITY CHECK

The boot-up process is one of the most easily exploitable ways to inject malicious software within the OS. At every reboot the custom partition validation of Secure OS scans different partitions of the device's hard drive to check if the phone is not infected with malware.

A Mode for Every Need

To ensure, you have access to all functionalities you might require to do your work, conduct secure communications and protect your data, Secure OS features different modes – each aimed at serving a particular user need.

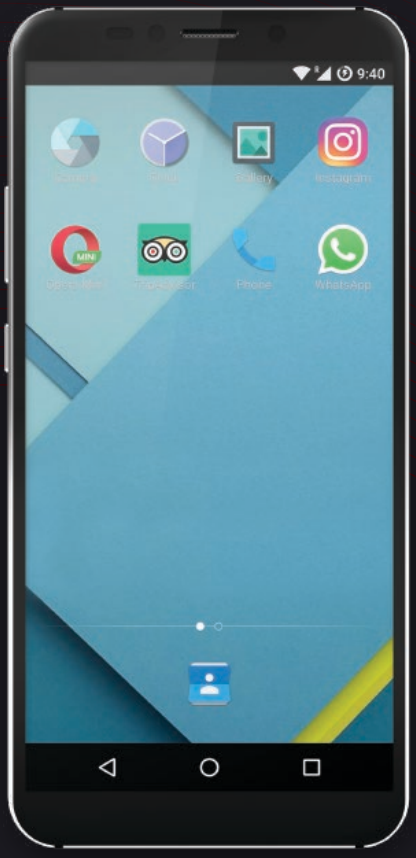


Secure Mode

Serves mainly to establish secure communication between peers and protect the shared sensitive data. Secure Mode gives access to the Encrypted Chat & Calls, Encrypted Email, Encrypted Vault. All chat messages, emails, and calls are end-to-end encrypted with state-of-the-art cryptography unbreakable even for modern supercomputers. It allows users to access the Password advisor, a privacy-centered, encrypted app that lets you store and manage your passwords easily by providing accessible hints.

Emergency Center

Usually, if you're using a secure mobile device, your data is an object of interest to others, which can endanger you or put you in risky situations. The Emergency Center provides you with fast access to critical functionalities such as the one-click Wipe to quickly dispose of all sensitive information you might be carrying or the Incognito Mode, camouflaging your device.



Incognito Mode

Sometimes circumstances require to hide the fact that you're using a specialized mobile security device or to authenticate that there's nothing suspicious on the phone. In such situations, Secure OS can mask itself as a regular Android featuring commonly-used apps such as Instagram or WhatsApp, to protect you against physical inspection.

Encrypted Chat & Calls

All communication is end-to-end encrypted on your device, travels as indecipherable traffic all the way to the recipient, and gets decrypted only on their device. Encrypted Chat & Calls app uses OTR and OMEMO encryption for Peer-to-Peer (P2P) and Group Chats, with the unbreakable AES-256 cipher, and ZRTP to encrypt both P2P and Group Voice & Video Calls.

SELF-DESTRUCTING MESSAGES

Encrypted Chat & Calls allows you to discard messages after you have sent them by setting self-destruct timers and blocking the ability to forward them. Once time runs out, the content gets deleted on both your and the recipient's devices.

PUSH-TO-TALK

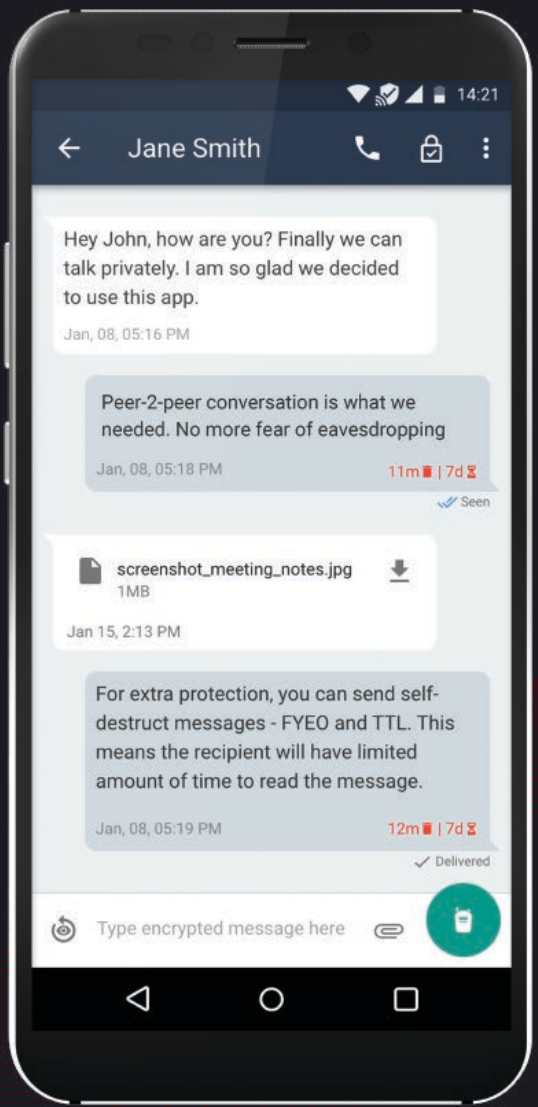
If you find speaking more convenient than typing, you can send short voice recordings via Encrypted Chat & Calls. They are also protected by OTR encryption.

REMOTE WIPE

In case your phone gets stolen or lost, you can remotely wipe all data by sending a predefined message to your Encrypted Chat & Calls profile to ensure no 3rd party can leverage your information.

ZERO-SERVER-TRACE GROUP CHAT

We've taken rigorous efforts to create a group chat that only uses our servers to distribute the encrypted messages and delete the data afterwards, storing it as an encrypted form for a maximum of 7 days and leaving no server trace of your sensitive information.



Zero-server-trace Encrypted Chat & Calls

Zezel.com stores no sensitive information from your communication. The messages in P2P chats don't even reach the premises of our servers. Group chats only use our infrastructure to distribute the shared information, not storing it for more than a week, after which it's deleted leaving no trace. The VoIP calls only use our servers to establish a connection between the peers. These privacy-centered methods guarantee your absolute privacy.

Encrypted Chat & Calls

Competitors

Sender is online; recipient is offline

When you tap send, the app connects to the server, which checks if the recipient's device is online. If it isn't, the message doesn't get sent. It never leaves your device.

When you tap send, the app sends the message to the server, which checks if the recipient's device is online. If it isn't, the message stays on the server and waits for the recipient to come online.

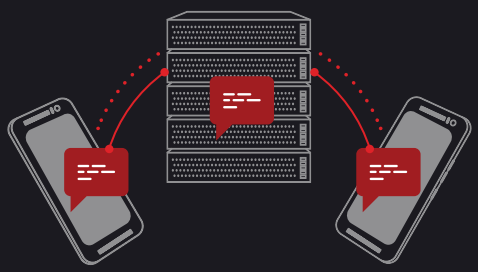
Sender is offline; recipient is online

When the recipient comes online, they do not receive the message you tried to send while they were offline – it never left your phone.

When the recipient comes online, they receive your message which was waiting for them on the server, regardless if you are now online or not.

Both parties are online

The server checks if the recipient is online. If they are, your phone sends the message directly to them.



The messages get sent to the server and then from the server to the recipient.

Encrypted Email

The device also features a full-functionality, encrypted email client, Encrypted Email. It uses an improved implementation of the PGP cryptographic protocol and 4096-bit keys, unbreakable even by modern supercomputers.

FEATURE - RICH

Encrypted Email gives you all the features you would expect from an email client: message filtering, support for multiple accounts, inbox rules, folder management, etc.

STRONGEST AVAILABLE ENCRYPTION

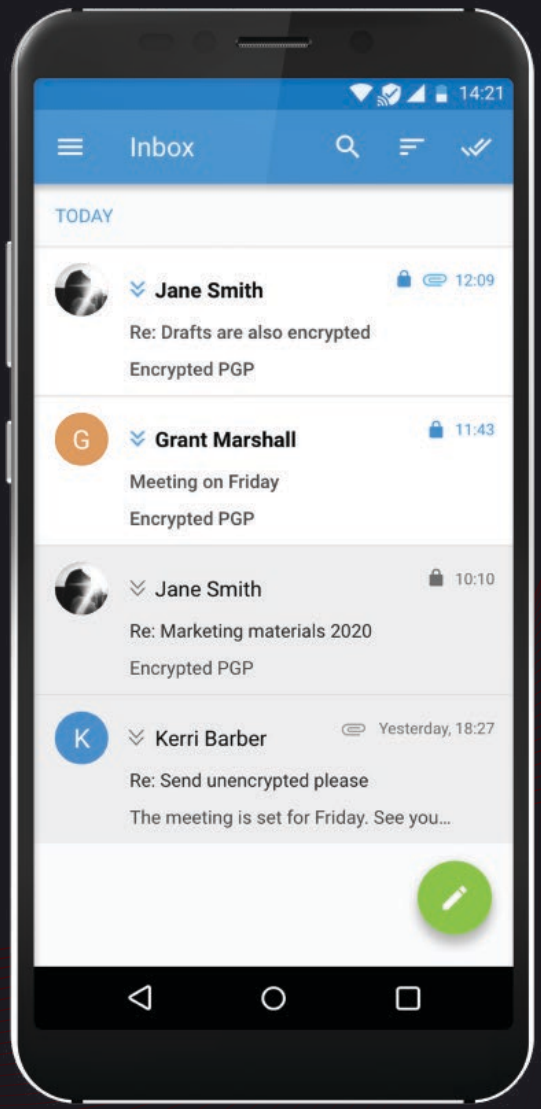
Our Encrypted Email app uses AES-256 cipher with 4096-bit RSA keys. Decrypting messages is out of scope even for supercomputers.

REMOTE WIPE

Similar to Encrypted Chat & Calls, the app can trigger a full wipe of the device if it receives a message containing a specific predefined text string in it which can be used in case the device is lost or stolen.

ENCRYPTED APP DATABASE

All your emails, contact names, logs, and the encryption keys you use for your messages are stored in the app, within an encrypted database inaccessible for other software on the phone.



User-managed Email Private Keys

To ensure that absolutely no one will be able to access the sensitive communication in your emails, the 4096-bit RSA private keys are generated and stored only on the devices of the users that are communicating. Neither Zezel.com nor anyone else can intercept and decrypt your emails.

Encrypted Email

Competitors

Key Generation

The keys are generated by the app on your device.

The keys are generated on the server and then sent to the user's device.

Key Storage

No keys are ever stored on our servers, and there is no way for us to replicate them.

The servers store copies of user keys or can generate identical ones.

Email Traffic

Your emails pass through the servers but cannot be decrypted by anyone but you - with the keys stored only on your device.

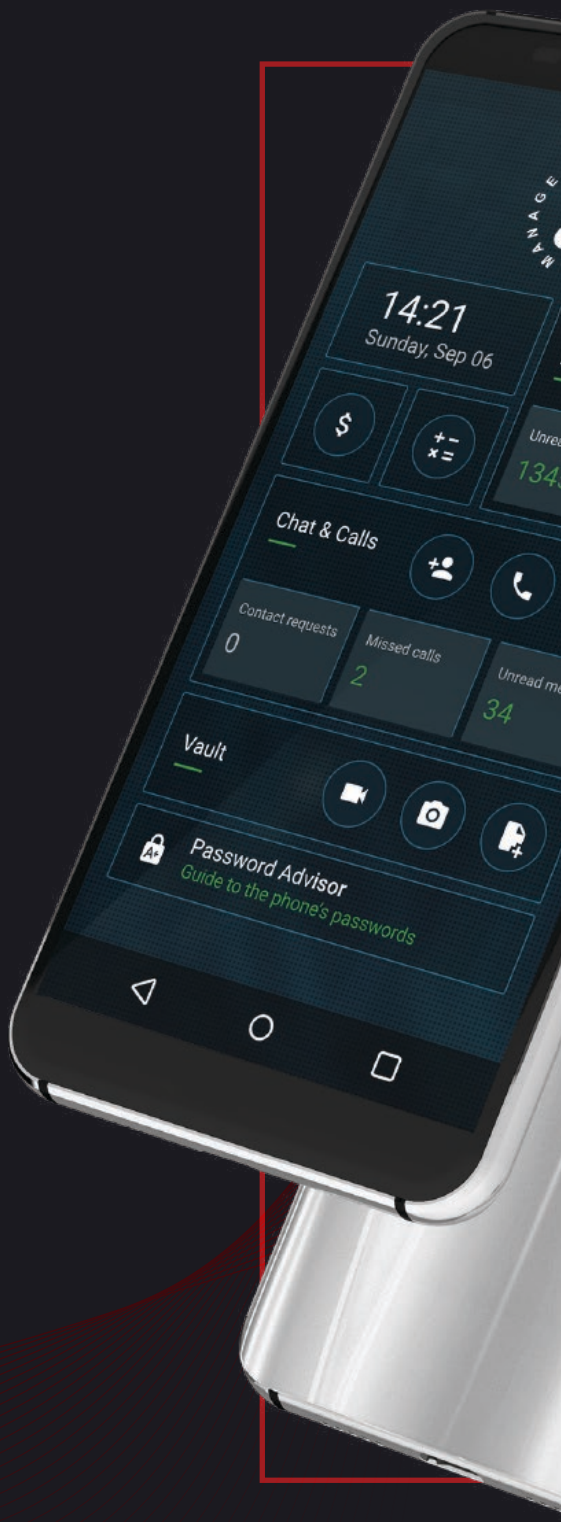
Your emails pass through the servers and can be decrypted with the copies of the keys.

Security-Hardened Hardware

No Data Extraction Possible

Your handset contains information about all your contacts, the messages, and files you have exchanged with them, as well as the times those communications took place. Consumer-grade smartphones and even many secure mobile devices offer little protection for this data in case the device falls into the wrong hands. For example, forensic techniques such as chip-off can be used by adversaries to unmount your phone's eMMC chip and put it in a specialized device that can access all data stored on it.

theZphone offers several layers of protection for data-at-rest that counter techniques like chip-off. First, the entire device storage is encrypted, which means the only way in is by brute-forcing the device password. This is impossible even for supercomputers if you have a strong one. Then, everything on the handset is stored in encrypted databases behind yet another password. Multiple password mismatches trigger a device wipe mechanism. The data could easily be remotely wiped as well.



Guaranteed Hardware Integrity

Many consumer-grade phones reach users already compromised by embedded tracking software or altered hardware. theZphone is a custom encrypted phone, specially developed with security and privacy in mind. Numerous quality assurance methods are implemented in the design and development process to guarantee the integrity of the hardware you're receiving. The attack surface is significantly reduced by rooting out easily compromisable sensors.

Hardware Model Specs:

1.3GHz quad-core processor
Fast multitasking

32GB encrypted storage
No manual extraction of data

3GB RAM
Smoother performance

5.5" HD display
Bigger screen, better view

3200mAh battery
Lasting experience

13MP rear camera, 5MP front camera
Take high-quality photos

Sleek design
Elegant and professional look

No Unauthorized Modifications

Some threats mask themselves as updates pushed to the user. After installing it, such a software could gain significant access and control privileges.

theZphone is paired with mobile device management (MDM) platform, which is the only place where policies can be assigned to a particular handset. This job falls on both our partners and us.

The platform communicates with the device via an SSL-encrypted connection, which eliminates the chance for interference. The device you get out of the box will never be subject to malicious modifications. No malware can be installed on it because all software policies are assigned through the MDM. An app not in policy cannot exist on the handset. Similarly, no malicious third-party app will be able to turn on functions like the camera, Bluetooth, or USB without permission. Your device is practically locked.

Self-hosted Solutions

Even though we have no access to users' sensitive information, we still store some parts of it as encrypted metadata. The technology that protects the information from third parties is the fact that the private keys that decrypt the information are stored only on the users' devices. Even if in the most extreme case, attackers manage to penetrate the defenses of our servers and access the stored data, they cannot decrypt it. This makes your communication data virtually impenetrable.

However, to enable the rapid, frequent, and reliable delivery of large, complex applications, we offer you the ability to self-host our solutions on your own infrastructure for maximum hardware integrity.

Our solutions are deployed on an individual instance (dedicated server) owned and controlled by you. With the current setup provided by Zezel.com, each instance has a capacity for up to 3000 users. The technology allows limitless scalability, and new instances can be added on demand when you exceed the capacity of a server.

The self-hosted versions practically ensure higher integrity and data security and help you establish control over internal sensitive communication, and visibility into various user groups.

Independent Communications

Privacy is all about eliminating third parties from the process and keeping your conversations between you and your contacts — this why we have also saved you the trouble of having to sign up for a mobile data plan and dealing with carriers that have access to sensitive information. Instead, theZphone comes out of the box with a special SIM card that provides unlimited data coverage worldwide.

NO EXTRA FEES

When you use theZphone, Zezel.com is practically your mobile operator. And we don't charge you extra fees for roaming.

WORLDWIDE CONNECTIVITY

The SIM stores multiple IMSI numbers, and can switch between them to always connect to the local operator with the best coverage, ensuring smooth connectivity in more than 180 countries across the globe.

NO TRACEABILITY

Since you sign no contract with a mobile operator, your name is not connected to your handset. You can't be linked to a specific card.

Get in Touch

USA

848 NORTH RAINBOW BLVD. SUITE 1510

LAS VEGAS, NEVADA 89107

CANADA

300 EAGLESON RD. SUITE 24177

OTTAWA, ONTARIO K2M 2C3

EUROPE

372 OLD STREET, SUITE BPM 339369

LONDON UNITED KINGDOM EC1V 9AU

CONTACT NUMBER :
702-605-0390

TOLL FREE :
1-866-560-2455

EMAIL :
mail@zezel.com

WEB :
Zezel.com

zezel.com
Mobile: Message. Manage.

zezel.com

Mobile: Message. Manage.