Business Email Hosting: Providers, DNS Records, Pricing & Security

Category: Technical Blog
November 22, 2026





- Services
- Projects
- Blogs
- About
- Contact
- Languages
  - NL
  - BE

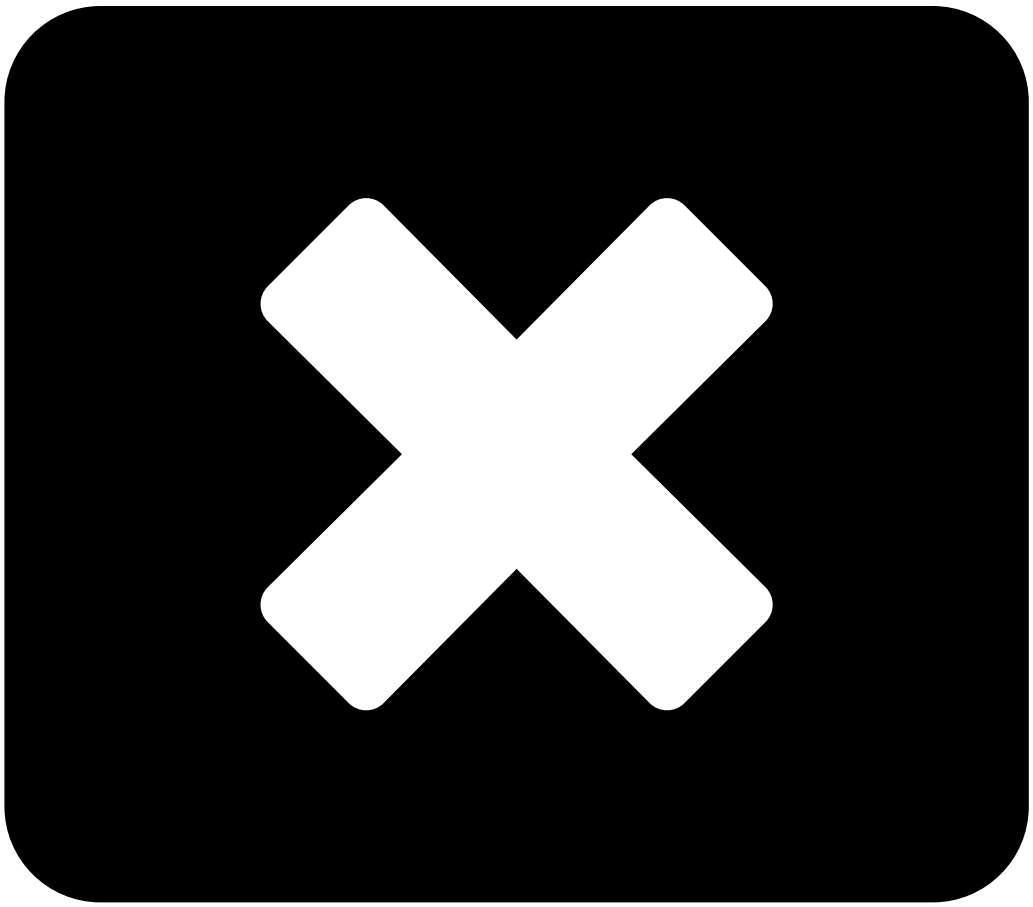
Hamburger Toggle Menu

[redacted]

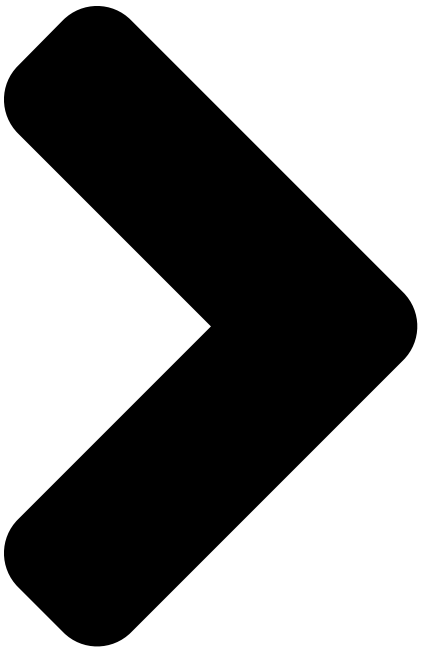
[redacted]

[redacted]

Free Quote

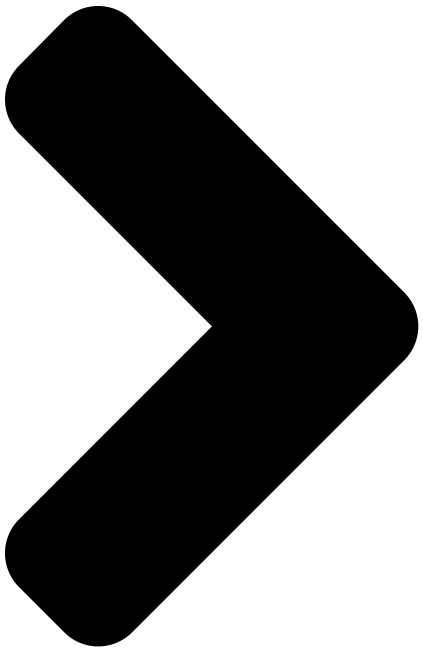


•



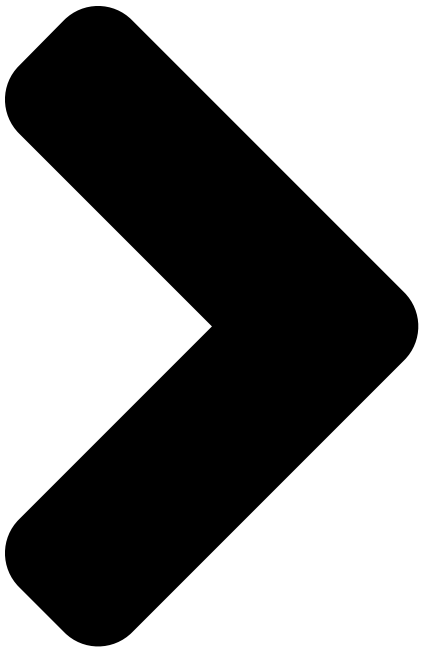
About us

-



Get a detailed quote now online

-



Courses University TSI

-

Login Team TST Digital Solution

OUR PARTNERS











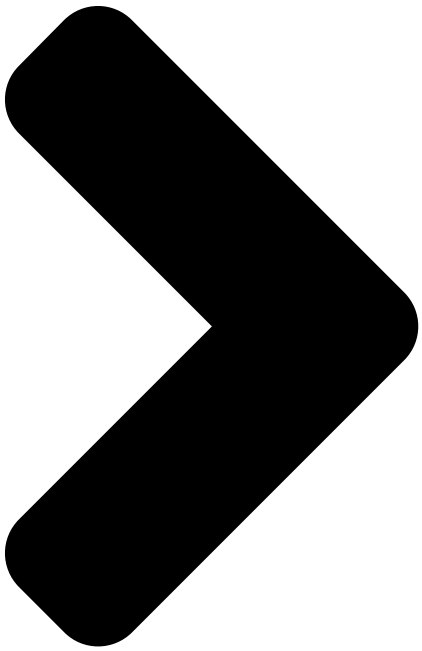


Trending Topic

Publicity

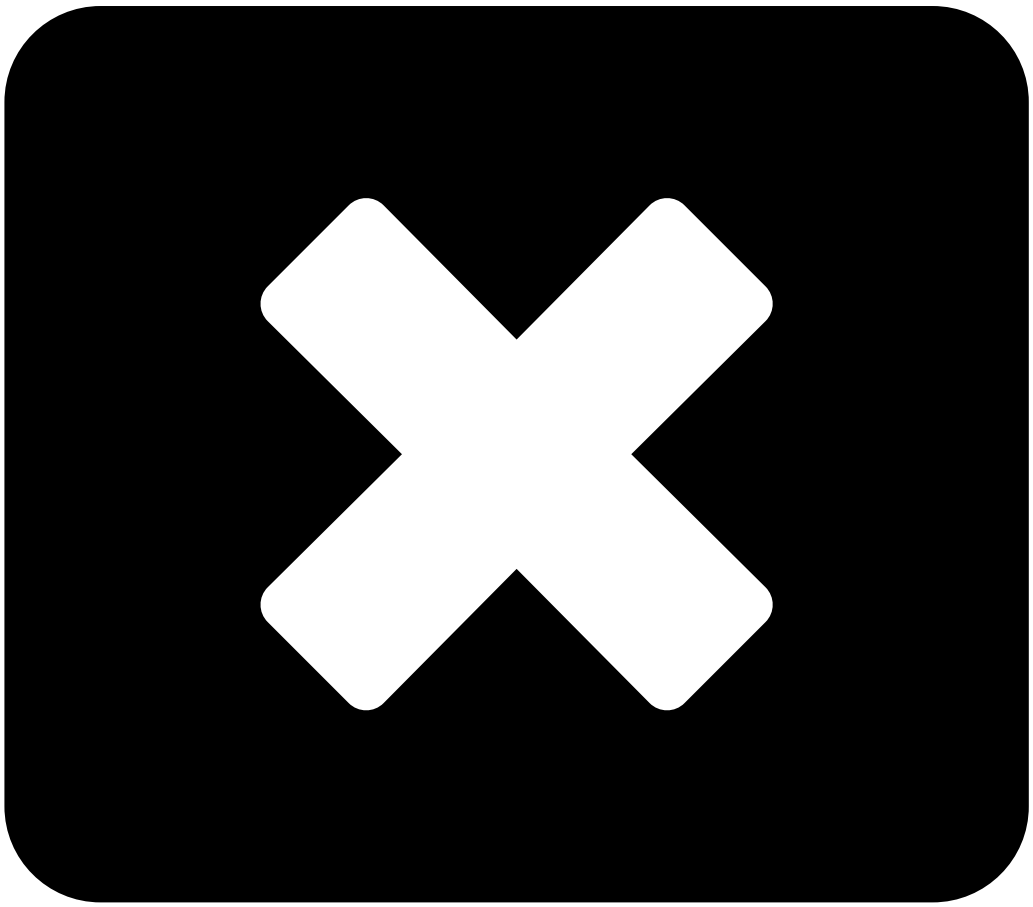
Reach out



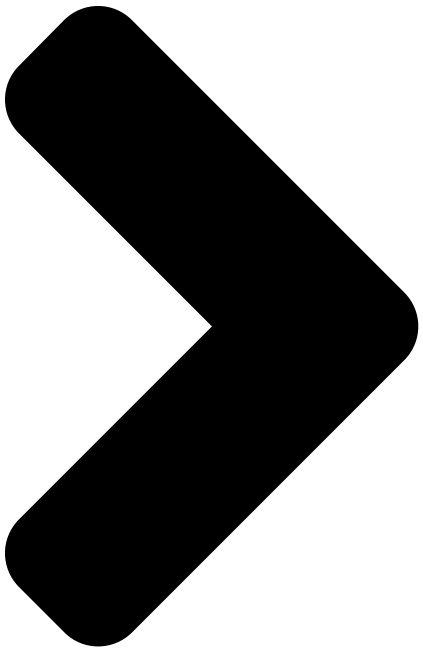


Some projects

Edit Template

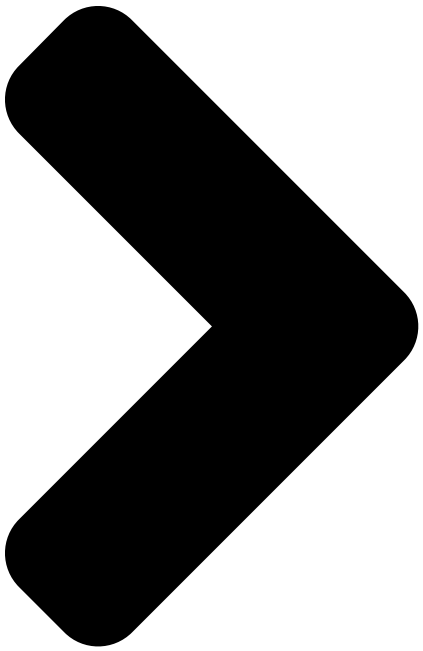


•

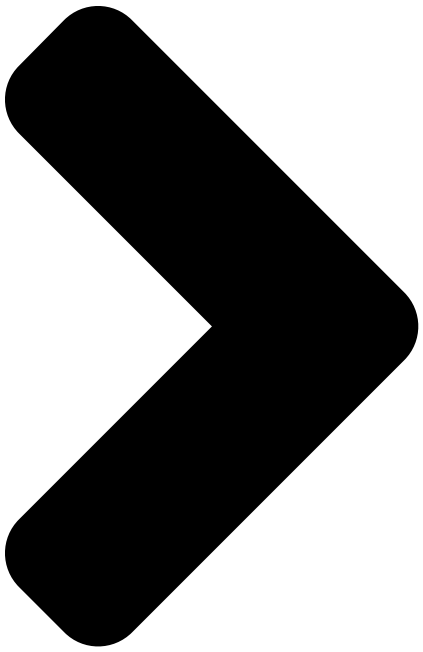


Services

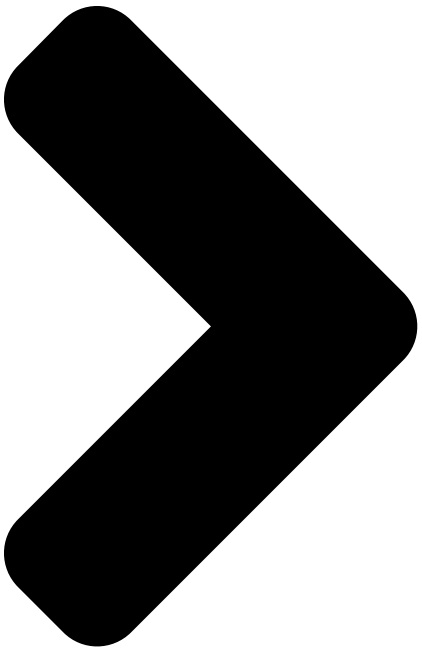
-



Web Design & Development

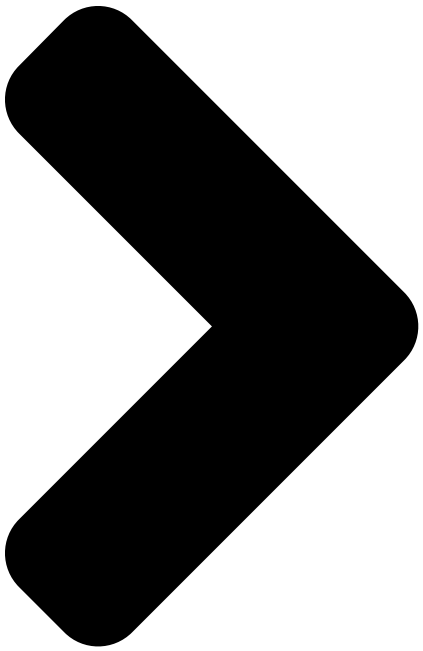


- Hosting
-

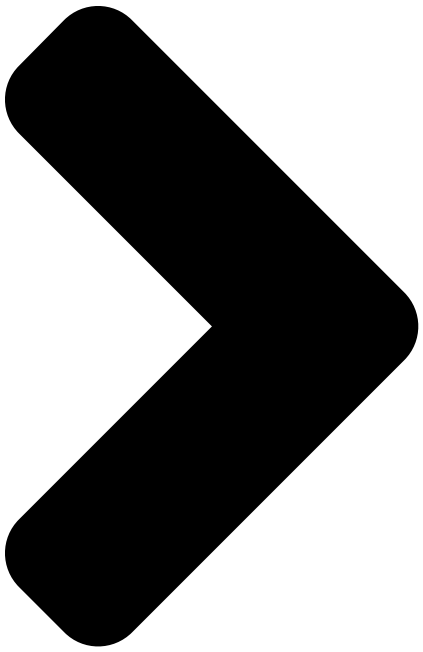


SEO/Ads/GMB/Speedup/Plugins/Technical

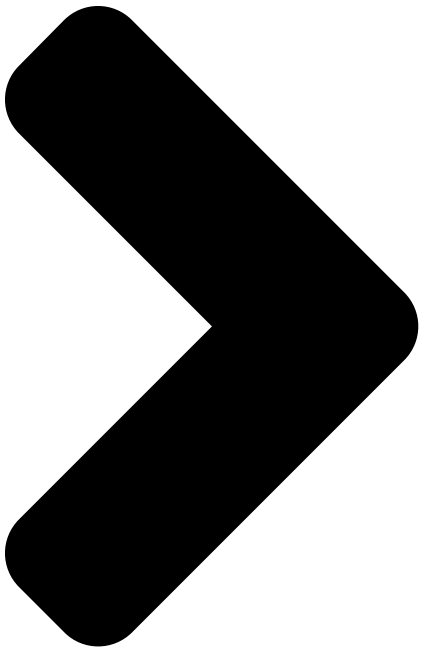
-



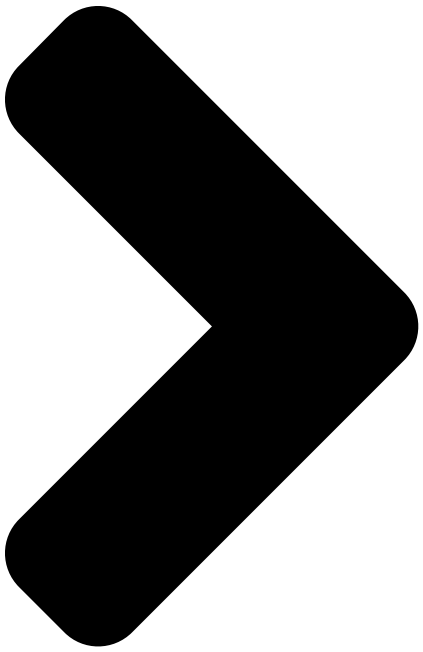
App Design & Development



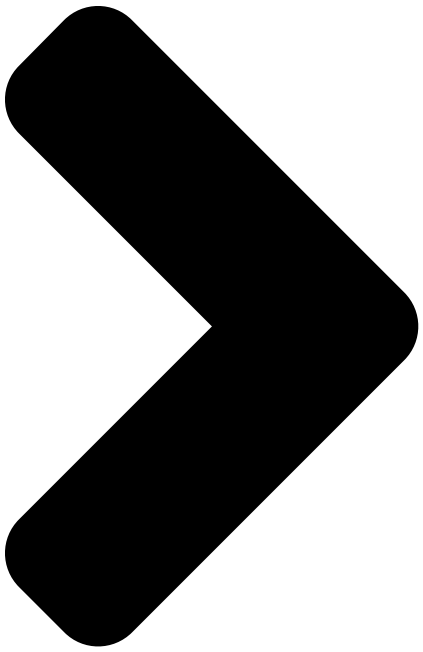
AI Agents



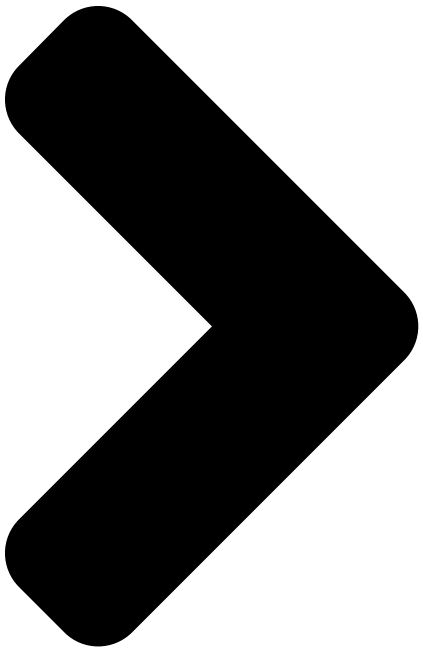
- e-Commerce
-



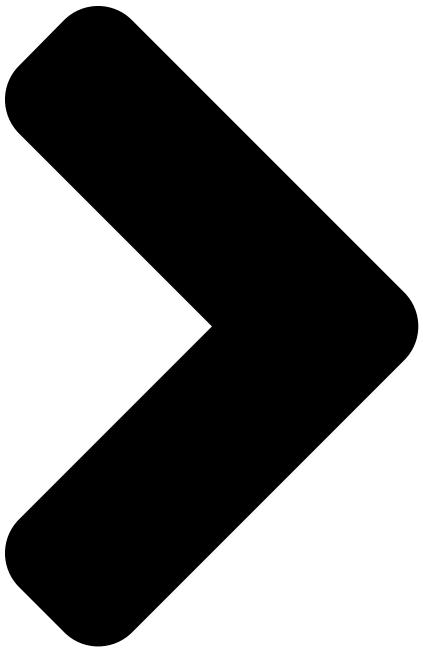
- Branding



- Social Media & Content Creation



- Graphic Design



- Copywriting & Translations

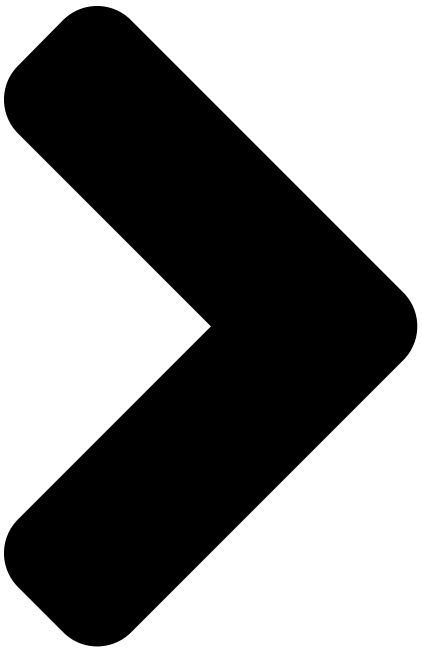


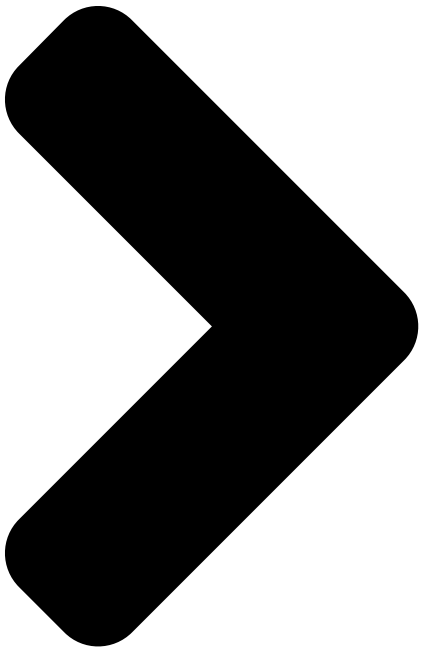
Photo- & Videography

Trending Topic

Publicity

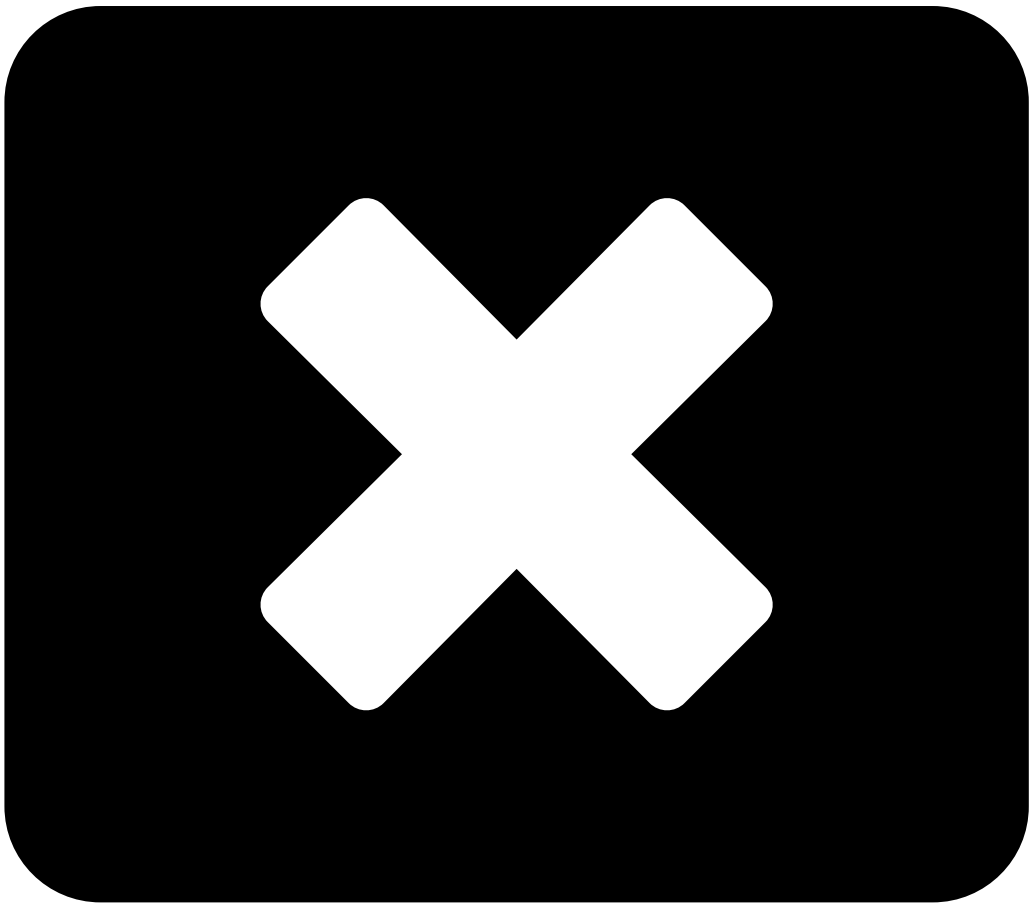
Calculate a quote
online yourself


Digital Solution

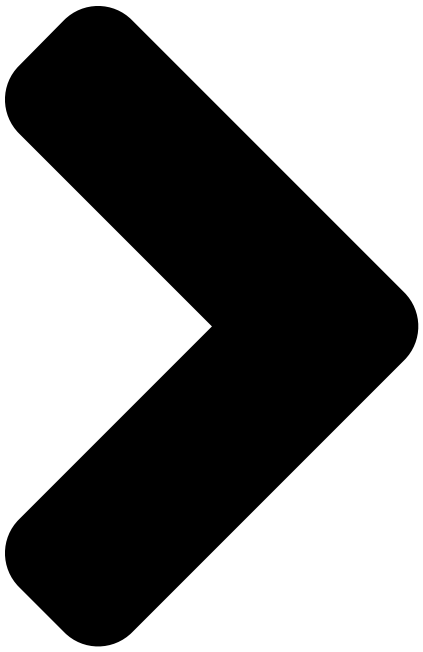


The way we work

Edit Template

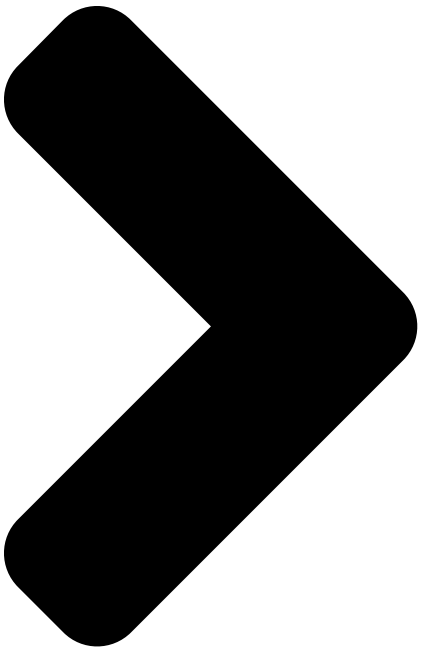


•



Realized projects

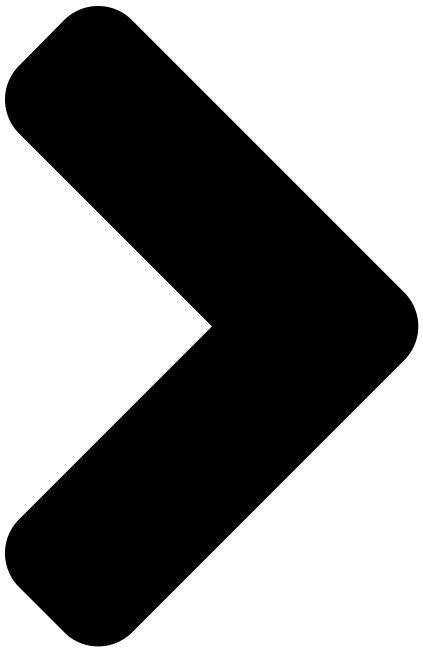
-



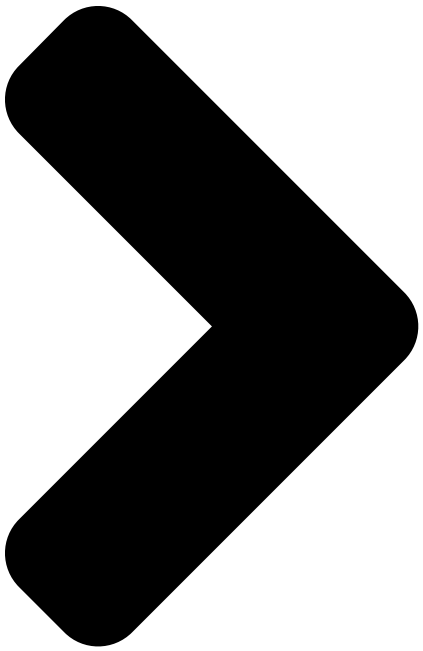
Calculate now your project price

Useful information

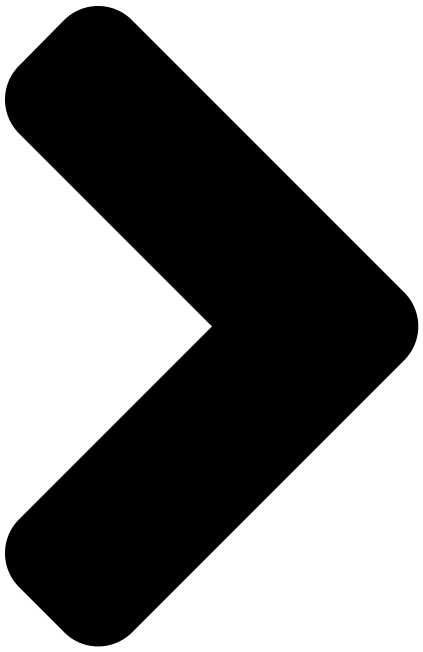
-



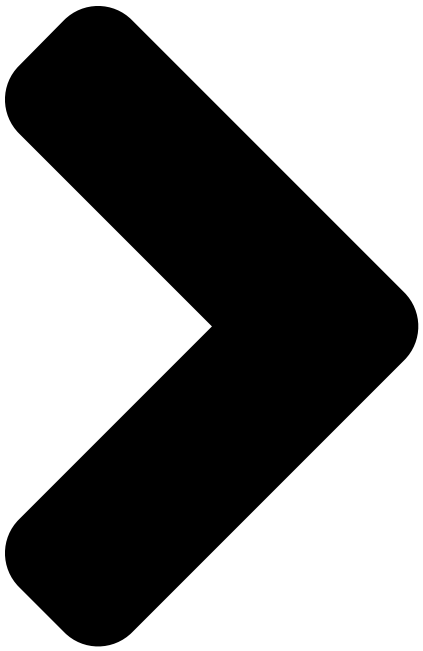
TSI Free Tools



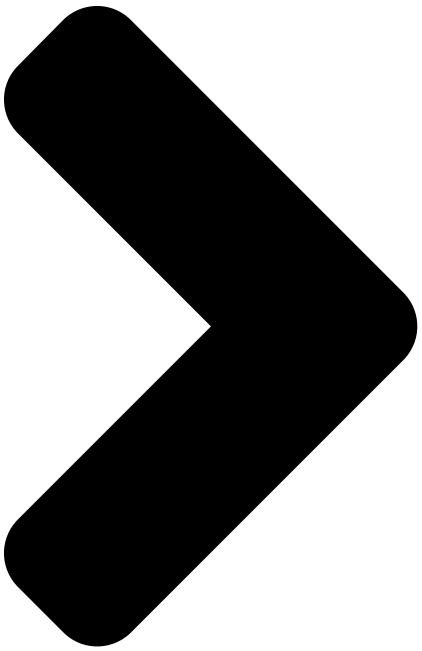
Jobs @ TSI Digital Solution



- Hosting at €75/year



- WordPress plugin TSI Visitor Blocker



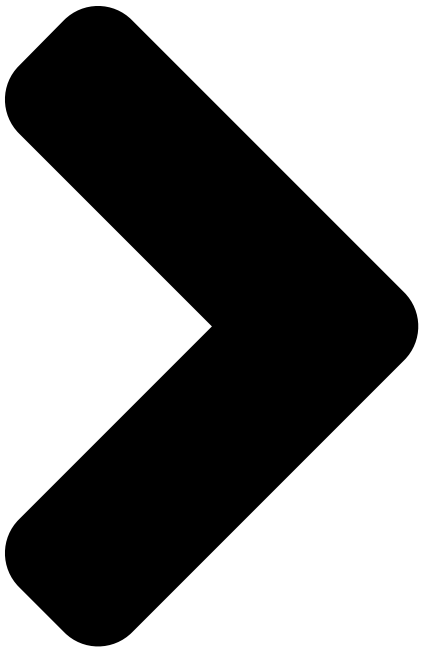
WordPress plugin TSI Careers

Trending Topic

Publicity

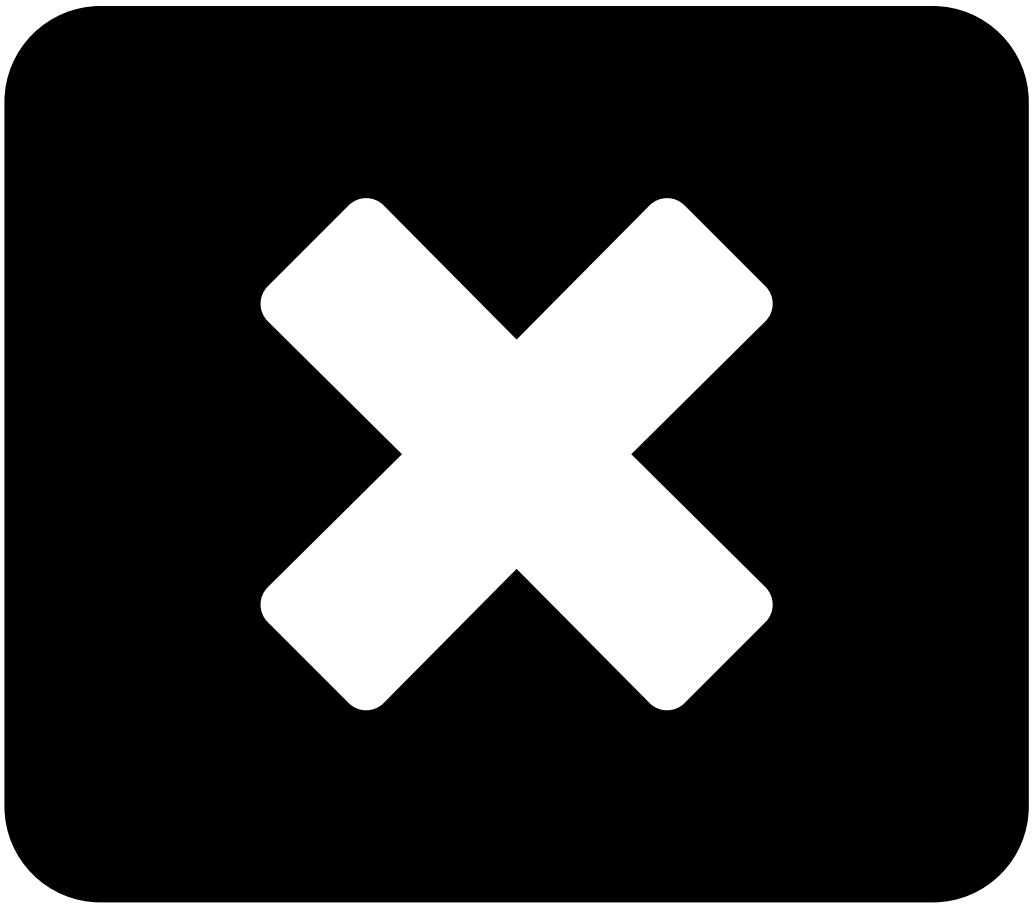
Interesting stuff to read


Digital Solution

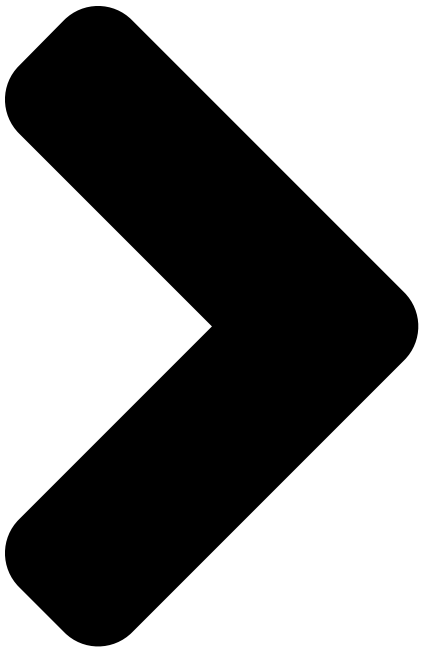


See More

Edit Template

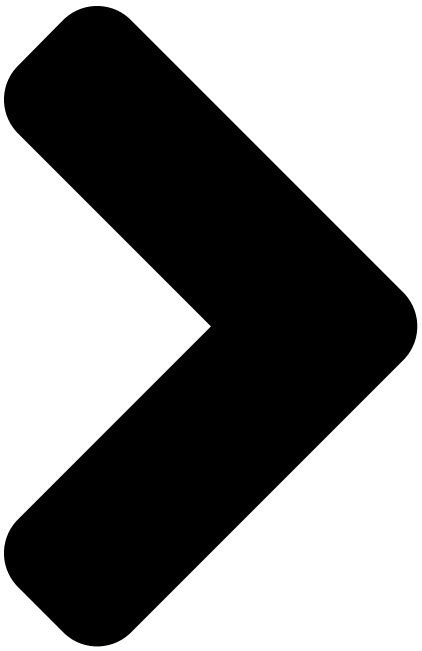


•



Blogs

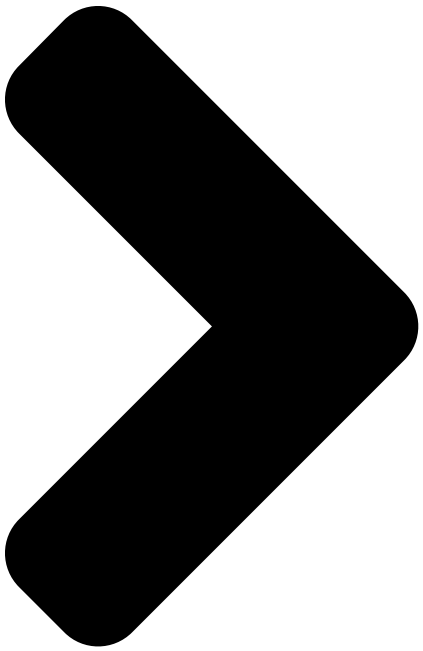
-



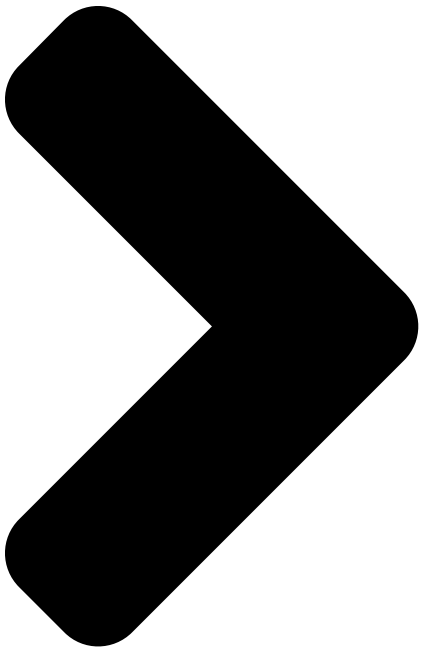
Receive a personalized, detailed estimate online

Some weekly posted topics

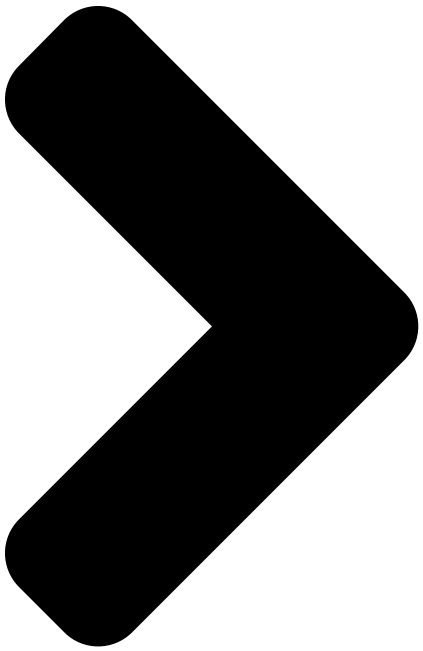
-



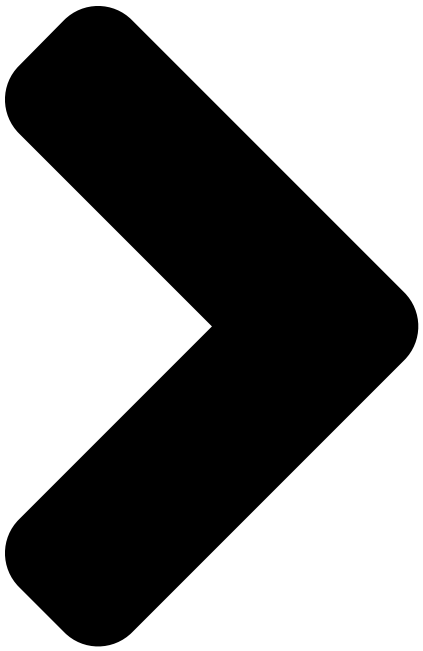
- Cheap Website vs. High Performance



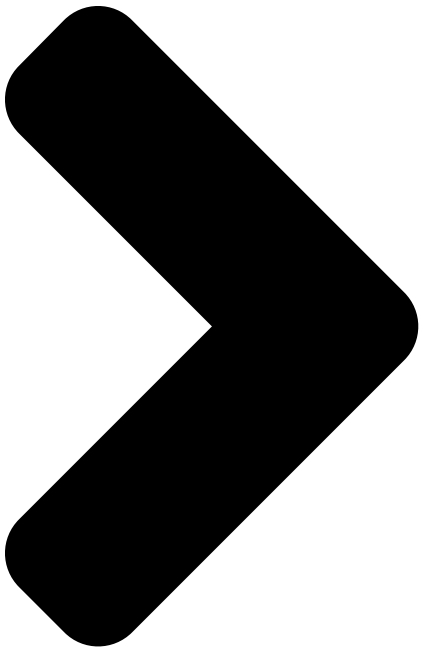
- What Is an AI Agent?



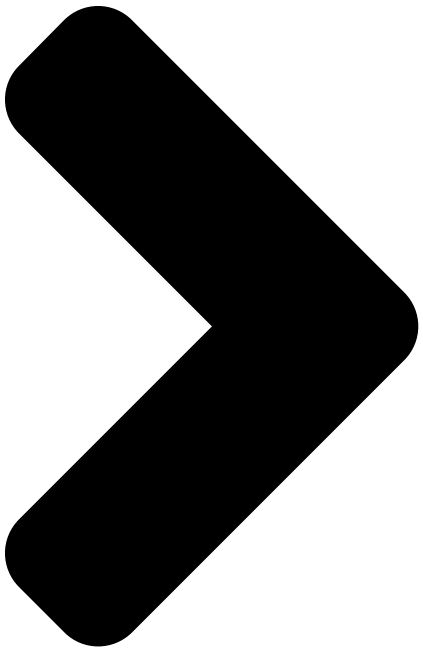
Client Communication in Digital Marketing



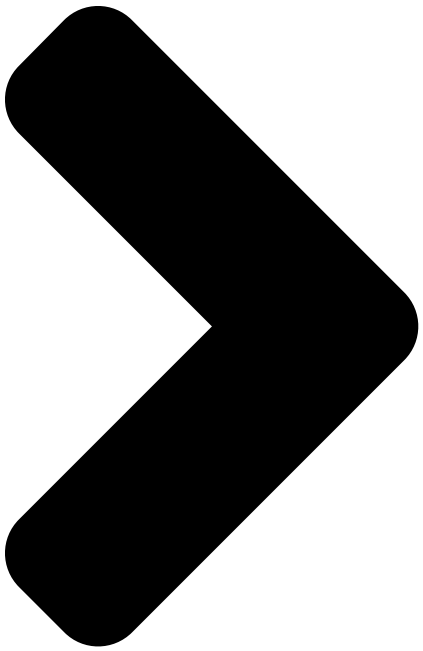
- Human Made Websites vs AI Websites



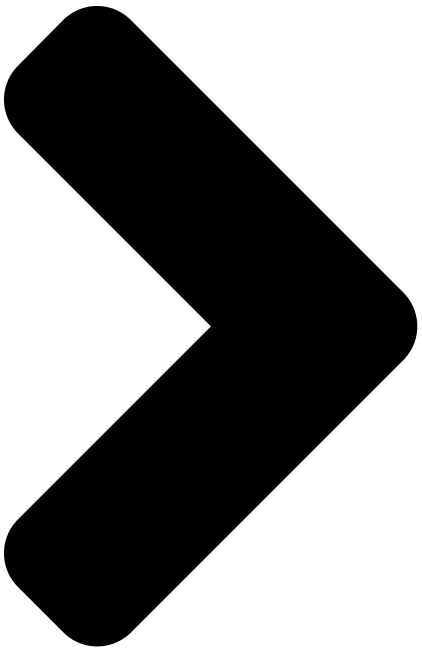
Your Digital Marketing Ecosystem Explained



- Mastering Answer Engine Optimization (AEO)



- Beware the Template Trap

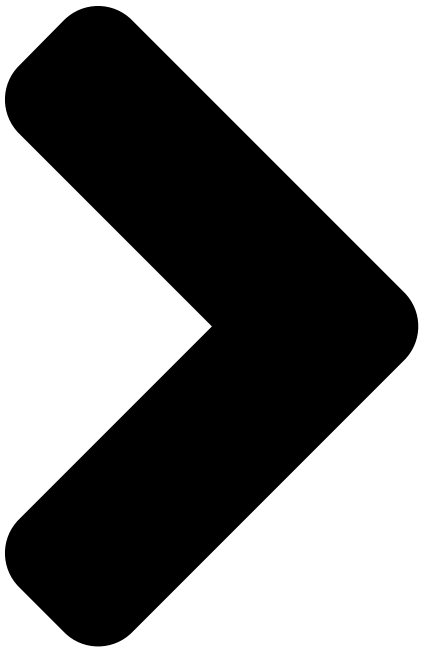


NWOW: Results Matter, Not Presence

Trending Topic

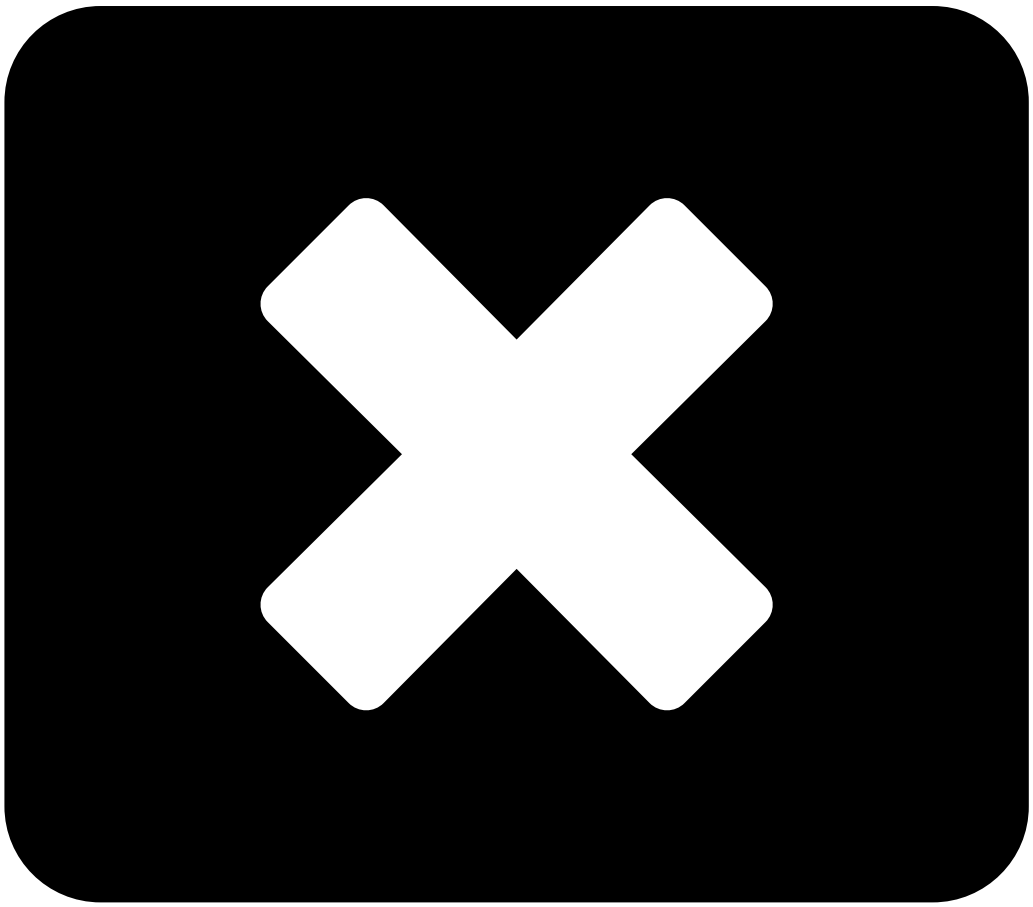
Publicity


Digital Solution

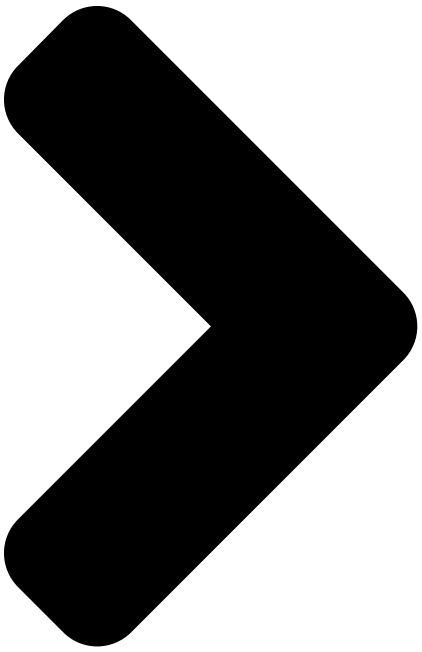


Who we are

Edit Template

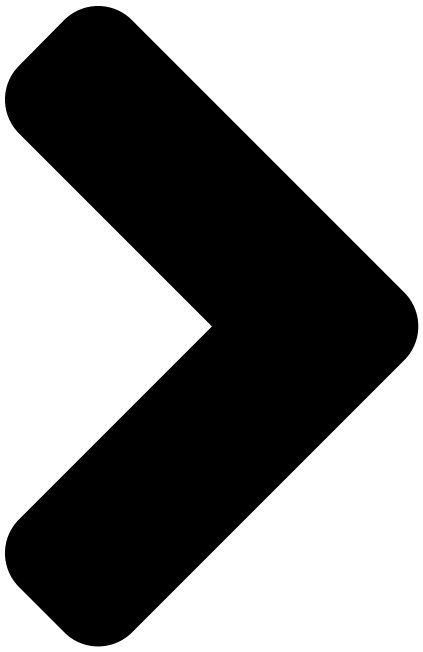


•



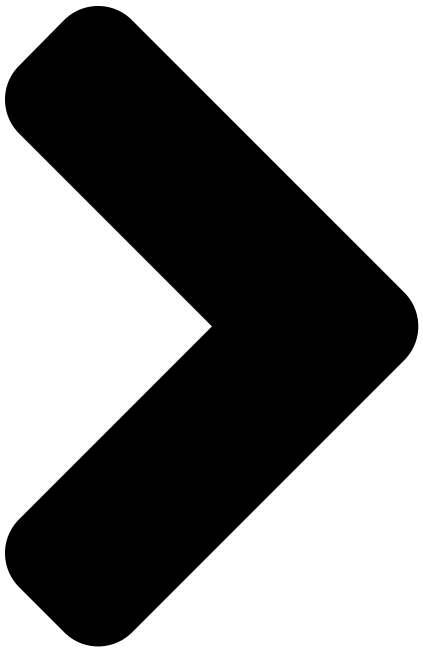
Contact us

-



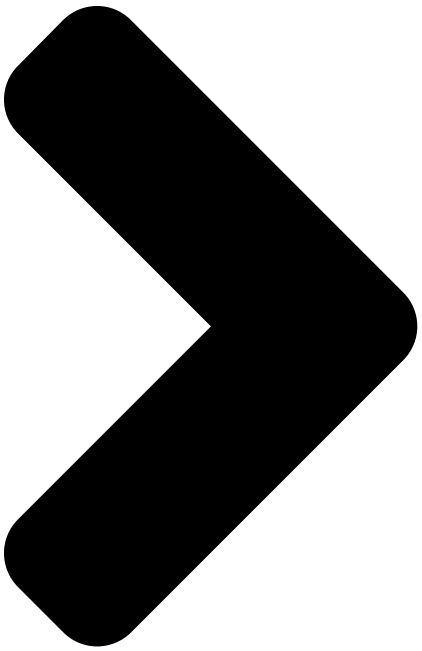
Get your quote online instantly

-



Jobs @ TSI Digital Solution

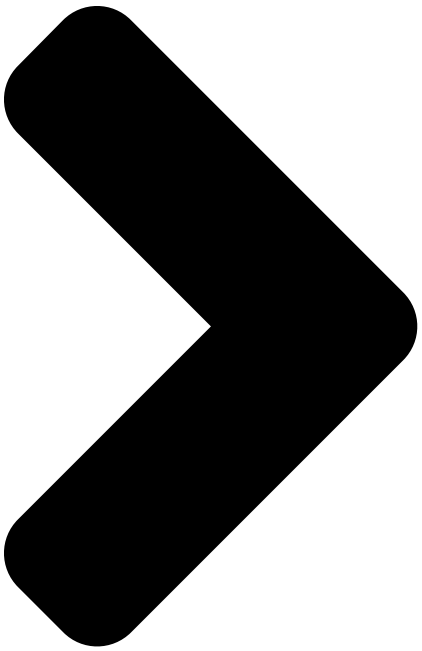
-



Affiliate program

Tools for free

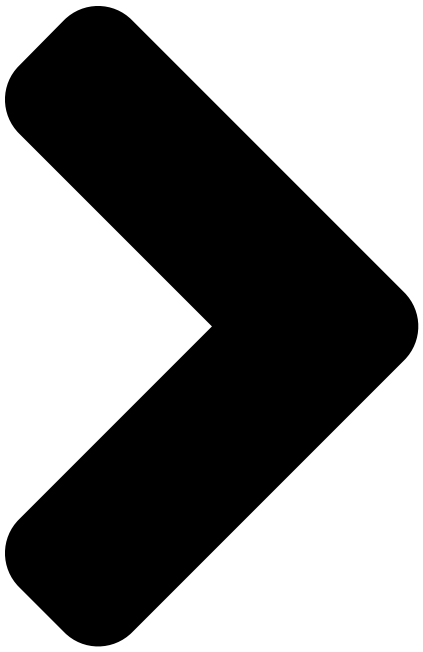
-



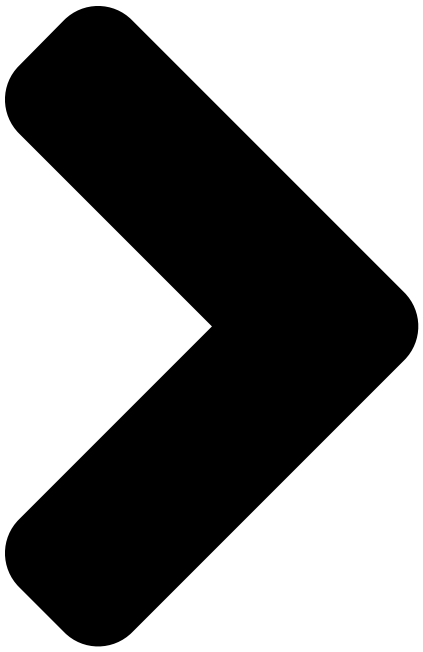
TSI Free Tools

WordPress plugins by TSI

-



TSI Visitor Blocker

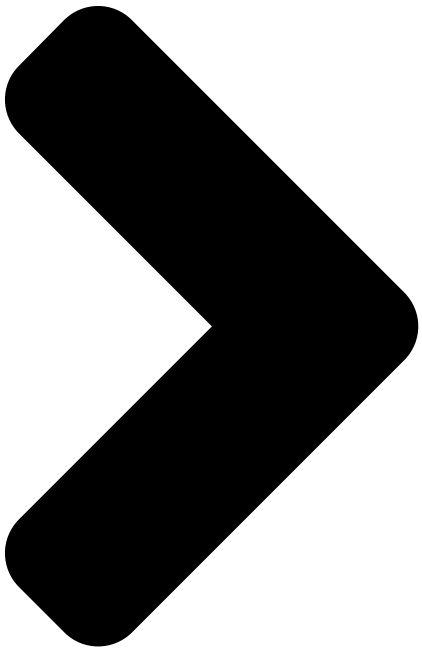


TSI Careers

Trending Topic

Publicity


Digital Solution



See More

Edit Template

Edit Template

Business Email Hosting

Get An Online Quote

Providers, DNS , Pricing & Security

learn how to secure or migrate business email

Imagine sending an important proposal to a potential customer, only to discover that the message has been rejected. Your team cannot access its

inboxes, customer enquiries are going unanswered, and password-reset emails are not reaching the people who need them.

For a business, email problems are rarely just technical inconveniences. They can interrupt sales conversations, delay projects, damage customer confidence and create security risks. Even when employees can still send messages, incorrectly configured DNS records may cause emails to land in spam or be rejected by receiving servers.

What Happens When Your Business Email Stops Working?

Email remains an important communication channel despite the growth of messaging applications and collaboration platforms. According to Eurostat's *Key Figures on Europe 2026*, **81.6% of EU residents aged 16–74 sent or received emails** in 2025. The Radicati Group also forecast 4.73 billion worldwide email users in 2026 in its 2024–2028 email market report. The Radicati figure is an industry forecast, not a measured 2026 total.

These figures illustrate why professional email infrastructure remains relevant to businesses of all sizes.

This is why business email hosting deserves more attention than simply choosing an address that looks professional. Reliable email depends on the provider, domain configuration, authentication records and security controls working together.

Whether you are setting up email for a new domain, changing providers or improving an existing system, understanding the essentials can help you avoid unnecessary downtime and protect your business communications.

What Is Business Email Hosting and How Does It Work?

Business email hosting is a service that allows an organisation to send, receive and manage **email using its own domain name**. Instead of relying on a generic address, a company can use addresses such as info@yourcompany.com, sales@yourcompany.com or firstname@yourcompany.com.

The email provider manages the infrastructure behind those addresses, including mailboxes, message storage, delivery systems and security features. The business connects its domain to that provider through DNS configuration.

Understanding the domain, DNS and email provider

These three elements perform different roles. Your domain is the address people use to find your business online. DNS, or Domain Name System, acts like an internet directory, directing services associated with that domain to the correct destinations. Your email provider operates the mailboxes and systems responsible for sending and receiving messages.

For example, a company might register yourcompany.com with one domain registrar, host its website with another company and use Microsoft 365 or Google Workspace for email. These services can work together even when they are purchased separately.

How an email travels from sender to recipient

When someone sends an email to hello@yourcompany.com, the sending mail server looks up the domain’s MX records to determine which mail servers should receive the message.

The receiving provider then checks the message and may evaluate authentication records such as SPF, DKIM and DMARC. These checks help establish whether the message is authorised and whether its domain identity is being used appropriately. If the message passes the relevant checks and the provider’s filtering systems consider it safe, it can reach the recipient’s inbox. If authentication is missing or incorrectly configured, delivery may be affected.

Authentication does not guarantee inbox placement. Sending reputation, message content, recipient engagement and the receiving provider’s filtering systems also influence delivery.

Why business email remains important

Email is used for more than everyday conversations. It supports customer enquiries, invoices, account verification, order notifications, password resets, contracts and business-to-business communication.

For businesses, this means email infrastructure should be treated as an important part of digital operations rather than an afterthought.

If your business is also building its online presence, explore TST Digital Solution’s website and digital services, which include website development, hosting and technical support.

Which Business Email Provider Should You Choose?

The best email provider depends on how your organisation works, which applications your employees use, how much administration you need and what level of security or privacy you expect.

There is no single provider that is automatically best for every business. The right choice is the one that supports your daily workflow without adding unnecessary complexity.

Business email provider comparison

Provider	Best suited for	Main strengths	Important consideration

Provider	Best suited for	Main strengths	Important consideration
Google Workspace	Collaborative teams and cloud-first businesses	Gmail, Drive, Docs, Meet and shared collaboration	Check storage, plan features and administration
Microsoft 365	Businesses using Office applications	Outlook, Word, Excel, Teams and enterprise administration	Some advanced features depend on subscription
Zoho Mail	Small businesses and cost-conscious teams	Custom-domain email and Zoho application integration	Compare mailbox limits and included features
Proton Mail	Privacy-conscious organisations	Privacy-focused design and encryption features	Check external email compatibility and administration
Fastmail	Businesses wanting focused email hosting	Custom domains, shared addresses and streamlined email	May require separate tools for broader office collaboration
Titan Email	Small businesses, freelancers and startups	Professional custom-domain email, business-focused features, calendar, contacts and productivity tools	Check mailbox storage, device limits, features and pricing included with the Hostinger plan

* *This comparison describes general product positioning, not a ranking of provider reliability or security.*

Google Workspace: Best for collaborative, cloud-based teams

Google Workspace is a strong option for businesses that rely on Gmail, Google Drive, Docs, Sheets, Meet and shared calendars.

Its main advantage is the integration between communication and collaboration tools. Teams can work on documents together, organise shared files and manage meetings within a connected environment.

It is particularly suitable for startups, agencies, remote teams and organisations that prefer browser-based tools. Businesses already using Google’s ecosystem may also find administration and onboarding more straightforward.

Official information: Google Workspace plans and pricing.

Microsoft 365: Best for businesses using Microsoft applications

Microsoft 365 is often a natural choice for organisations that depend on Outlook, Word, Excel, PowerPoint, Teams and SharePoint.

It offers a familiar environment for businesses that work heavily with office documents, internal collaboration and established corporate processes. Depending on the subscription, organisations can also access administrative, compliance and security features suited to more complex IT environments.

Companies that already use Windows devices and Microsoft applications may benefit from keeping their productivity and email systems within the same ecosystem.

Official information: Microsoft 365 business plans.

Zoho Mail: Best for cost-conscious businesses

Zoho Mail is worth considering for small businesses that want professional email hosting without necessarily adopting a large productivity suite.

It provides custom-domain email, administration tools and integration with other Zoho business applications. Organisations already using Zoho CRM or other products in its ecosystem may find this particularly convenient.

It can be a practical option for smaller teams that prioritise essential email functionality and predictable costs. Before choosing a plan, check mailbox limits, storage, migration options and the features included in the subscription.

Official information: Zoho Mail pricing.

Titan Email (Hostinger): Best for small businesses and professional email hosting

Titan Email is a good option for small businesses, freelancers and startups that need professional email addresses with their own domain.

Its main strengths include business email hosting, spam protection, email forwarding, aliases, calendars and contact management. It is particularly suitable for businesses looking for straightforward email hosting without the additional cost of a full productivity suite.

Official information: Titan Email features and limits.

Privacy-focused providers: Best for organisations prioritising data protection

Providers such as Proton Mail and Fastmail may appeal to businesses that place a high value on privacy, data handling and a focused email experience.

Proton Mail is particularly associated with privacy-oriented features and encryption. However, businesses should understand the distinction between encryption in transit, end-to-end encryption and compatibility with ordinary email systems. Not every message exchanged with external recipients receives the same end-to-end protection.

Fastmail offers custom-domain email and a focused communication experience, which may suit organisations that do not need a large office productivity suite.

Privacy-focused providers are worth evaluating when data protection is a

major selection criterion. Businesses should also assess administrative controls, account recovery, compliance requirements, integrations and the provider’s terms before making a decision.

Official information: Proton for Business and Fastmail business pricing.

How Much Does Business Email Hosting Cost?

Business email hosting prices vary depending on the provider, storage requirements, security features, subscription term and number of users.

A small business with three employees may have very different requirements from an organisation with several departments, shared mailboxes and compliance obligations.

What affects the total cost?

The monthly subscription is only one part of the total cost of running business email.

Consider the following:

- **Number of users:** Most business email services charge per user, so costs increase as your team grows.
- **Storage:** Larger mailboxes and long-term retention may require more expensive plans.
- **Security:** Advanced administration, compliance and protection features may only be included in higher tiers.
- **Migration:** Moving existing mailboxes and historical data can require technical assistance.
- **Administration:** DNS configuration, user management and ongoing maintenance may involve internal staff or external support.
- **Additional tools:** CRM systems, marketing platforms and backup services may have separate costs.

Can you get business email with website hosting?

Yes. Some website hosting packages include branded business email as part of a wider website solution.

For example, IST Digital Solution’s hosting package includes a business email address alongside domain and website hosting services. The published offer includes the first year and describes the renewal package and included services.

This can be convenient for startups and small businesses that want their website, domain and professional email arranged together rather than managing several separate providers.

However, businesses with advanced collaboration, retention or compliance requirements should compare bundled email with dedicated platforms such as Google Workspace and Microsoft 365 before deciding.

Which DNS Records Are Needed to Connect Business Email?

DNS configuration is one of the most important parts of setting up business email. Even with a reliable provider, incorrect records can prevent incoming messages from reaching the right destination or cause outgoing messages to fail authentication checks.

The exact records depend on the provider and the services being used. Always copy the current values from the provider’s official setup instructions or administrator dashboard.

MX, TXT, CNAME and SRV records: What do they do?

- **MX records** identify the mail servers responsible for receiving email for a domain. If these records are incorrect, incoming messages may not reach the intended mailboxes.
- **TXT records** store text-based information associated with a domain. They are commonly used for SPF, DKIM and DMARC authentication, as well as domain verification.
- **CNAME records** create aliases that point one hostname to another. Email providers may use them for service discovery, verification or other configuration requirements.
- **SRV records** identify the location of particular services and their associated ports. Some providers use them for service discovery and client configuration.

Not every provider requires every record. The configuration should follow the provider’s documented instructions rather than a generic template.

Understanding SPF, DKIM and DMARC

- **SPF**, or Sender Policy Framework, identifies which sending servers are authorised to send email for a domain. It is published as a DNS TXT record.
- **DKIM**, or DomainKeys Identified Mail, allows outgoing messages to carry a cryptographic signature. The receiving server can use the corresponding public key published in DNS to verify that signature.
- **DMARC**, or Domain-based Message Authentication, Reporting and Conformance, builds on SPF and DKIM. It tells receiving servers how to handle messages that fail DMARC evaluation and can provide reports about authentication activity. A DMARC policy can begin with p=none to monitor results, then move to p=quarantine or p=reject once legitimate sending sources have been identified and configured.

DMARC passes when at least one of the two authentication paths, SPF or DKIM, passes with the required alignment to the domain in the visible From address. Configuring both correctly is recommended because it provides more resilience, particularly when messages are forwarded or sent through different services.

Practical DNS configuration example

Consider a fictional business using yourcompany.com with a hosted email provider. Its DNS zone might contain records with the following structure:

Record type	Host / Name	Purpose	Example structure
MX	@	Routes incoming email	Provider-supplied mail server and priority
TXT	@	SPF authentication	v=spf1 include:PROVIDER-SPF ~all
TXT	selector._domainkey	DKIM authentication	Provider-supplied public key
TXT	_dmarc	DMARC policy	v=DMARC1; p=none; rua=mailto:dmarc@yourcompany.com
CNAME	Provider-specified hostname	Service verification or discovery	Provider-supplied destination

**This is an illustrative configuration, not a set of records to copy directly into a live domain.*

The actual MX hostnames, priorities, SPF include mechanisms, DKIM selector names and public keys must come from your chosen provider. The SPF example deliberately uses a placeholder because each provider publishes its own authorised sending infrastructure.

A few important configuration rules can prevent common problems:

- **Use the provider's exact MX records.** A wrong hostname or priority can disrupt incoming mail.
- **Maintain one SPF record per hostname.** If multiple services send email for your domain, their authorised sources should normally be combined into a single SPF policy rather than published as separate SPF records.
- **Watch the SPF DNS lookup limit.** SPF evaluation is subject to a limit of 10 DNS-querying mechanisms and modifiers. Exceeding it can cause a permanent SPF error.
- **Publish the correct DKIM key.** The selector and public key must match the signing configuration used by your provider.
- **Start DMARC carefully.** Monitoring with p=none helps identify legitimate senders before enforcing a stricter policy.
- **Check for existing records before making changes.** Replacing an existing SPF or MX record without understanding its purpose can break other services.

After updating DNS, allow time for the changes to propagate according to the records' TTL values. Then test both incoming and outgoing email rather than assuming that a successful DNS save means the setup is complete.

How Do You Secure Business Email?

Business email accounts often contain customer information, contracts, invoices, login links and internal discussions. A compromised mailbox can expose sensitive information and allow attackers to impersonate employees or suppliers.

Email security should therefore be part of the initial setup, not something added only after an incident.

Account protection and access management

Multi-factor authentication (MFA) adds another verification step beyond a password. Where supported, passkeys or hardware security keys can provide stronger protection against phishing.

Businesses should also apply sensible access controls. Employees should have access only to the mailboxes and administrative functions they need. Shared accounts should be avoided where individual user accounts and delegated mailbox access are available. When an employee leaves, their account access should be reviewed promptly. Recovery addresses, administrator permissions, forwarding rules and connected applications should also be checked.

Protecting email delivery and domain reputation

TLS helps protect email connections while messages travel between supporting mail servers. However, TLS does not automatically provide end-to-end encryption, so organisations handling sensitive information should understand the protection their provider actually offers.

Additional technologies can strengthen email transport and domain trust:

- **DNSSEC** helps protect DNS responses against certain forms of tampering.
- **MTA-STS** allows a domain to publish a policy requiring supporting sending servers to use secure TLS connections when delivering email.
- **TLS reporting** helps domain owners identify email transport problems.
- **BIMI** can allow eligible organisations to display a verified brand logo in supporting email clients, subject to the relevant requirements.

These technologies serve different purposes. They are not substitutes for correct SPF, DKIM and DMARC configuration, account security or employee awareness.

What do major email providers require from senders?

Authentication requirements are not just theoretical best practices. Major mailbox providers publish rules designed to reduce spoofing, phishing and unwanted email.

Google’s sender guidelines require all senders to Gmail accounts to configure SPF or DKIM, use TLS for transmission, maintain valid forward and reverse DNS for sending infrastructure and keep reported spam rates below 0.3%. Senders

who exceed 5,000 messages per day to personal Gmail accounts must also configure both SPF and DKIM, publish DMARC and meet alignment and unsubscribe requirements for applicable marketing messages.

Yahoo's sender guidance also sets authentication requirements, including SPF or DKIM for all senders and SPF, DKIM and DMARC for bulk senders. It advises bulk senders to keep spam complaint rates below 0.3% and provide functional unsubscribe mechanisms for relevant marketing mail.

These requirements matter even if a business does not send thousands of messages every day. They demonstrate why domain authentication, responsible sending practices and reputation management should be part of a professional email setup.

Read the official Google Email Sender Guidelines and Yahoo Sender Best Practices for the latest requirements.

What Happens When Email DNS Records Are Incorrect?

Incorrect email DNS records can create problems that are not always immediately obvious. A business may continue sending messages for a while, but recipients may experience delivery delays, spam placement or outright rejection.

Common consequences include:

- **Incoming email failures:** Incorrect MX records can send messages to the wrong destination or prevent delivery.
- **Outgoing authentication failures:** Missing or incorrect SPF and DKIM records can cause authentication checks to fail.
- **DMARC policy problems:** A strict policy can block legitimate messages if authorised sending services have not been configured properly.
- **Domain reputation damage:** Poor authentication and suspicious sending activity can affect how receiving providers treat a domain.
- **Business disruption:** Missed enquiries, delayed invoices and failed password-reset emails can affect daily operations.

The difficulty is that a message can appear to send successfully from the sender's mailbox without necessarily reaching the recipient's inbox.

How to diagnose and fix common email problems

Start by checking the provider's current DNS requirements against the records published for your domain. The DNS configuration section above explains what each record does and which common mistakes to look for.

Review message headers and provider logs where available. These can help identify whether SPF, DKIM and DMARC passed, whether a message was rejected and which server handled it.

If the problem began after a DNS change, review the previous configuration and consider whether a record was overwritten or removed. Avoid making

several unrelated changes at once, as this can make troubleshooting more difficult.

How to Migrate Business Email Without Losing Messages

Changing email providers can improve security, reduce costs or give a business access to better collaboration tools. However, a poorly planned migration can interrupt communication, lose access to old messages or cause outgoing emails to fail authentication.

A successful migration is not just about moving mailboxes. It involves preparing the domain, transferring data, coordinating DNS changes and testing the new environment.

Prepare before changing your email provider

1. Start by creating an inventory of existing mailboxes, aliases, shared mailboxes, forwarding rules, groups, calendars and contacts. Identify which accounts are actively used and which contain historical information that must be retained.
2. Check the new provider’s migration tools and confirm that mailbox storage limits are sufficient. Where possible, create the new user accounts and prepare the destination mailboxes before changing the MX records.

It is also sensible to lower the relevant DNS TTL values in advance, following your provider’s guidance. This can help changes take effect more quickly, although it does not guarantee that every sending server will immediately use the new destination.

Preserve old emails and verify outgoing authentication

Use the migration method supported by your providers, such as IMAP migration or an official migration tool. Confirm that messages, folders, attachments and relevant mailbox data have transferred successfully.

Do not cancel the old email service immediately after changing MX records. Keep it active during the transition so that you can retrieve older messages, identify mail still arriving at the previous service and resolve any migration gaps.

Before considering the migration complete, verify the new provider’s outgoing authentication:

1. Confirm that the new provider’s SPF requirements are included in your domain’s existing SPF policy.
2. Enable DKIM signing and publish the correct provider-supplied public key.
3. Check that DMARC alignment works with the new sending domain configuration.

4. Send test messages to different external providers and review their authentication results.
5. Test replies, forwarding, shared mailboxes, mobile devices and important business applications.

Pay particular attention to systems that send email independently of the main mailbox provider. These might include website contact forms, CRM platforms, invoicing software, booking systems and marketing automation tools. They may need their own authorised sending configuration.

A sensible migration includes a rollback plan, a clear communication window for employees and a period of monitoring after the switch. Keep the previous service available until the new environment has been tested and the business is confident that all important messages and workflows are working correctly.

Business Email Setup Checklist

A professional email setup should be tested before employees begin relying on it for customer communication. Saving DNS records is only one part of the process. You also need to confirm that messages can travel in both directions and that the provider can authenticate outgoing mail.

Use this checklist when setting up a new email service or completing a migration:

☐ Confirm that all required MX records match the provider’s current instructions.
☐ Check that there is only one valid SPF record for the relevant hostname.
☐ Confirm that all legitimate sending services are included in the SPF policy.
☐ Enable DKIM signing and verify the published selector and public key.
☐ Publish a DMARC record and review alignment results before enforcing a strict policy.
☐ Send test messages to Gmail, Outlook and other external mailboxes.
☐ Review message headers to confirm SPF, DKIM and DMARC results.
☐ Test incoming messages, outgoing messages, replies and attachments.
☐ Test website contact forms, CRM notifications and automated business emails.
☐ Check mailbox access on desktop, browser and mobile devices.
☐ Confirm MFA, recovery methods and administrator permissions.
☐ Keep a record of the final DNS configuration and migration date.

For ongoing maintenance, review authentication reports, account access and sending behaviour periodically. Recheck the configuration whenever a new marketing platform, website service or third-party application begins sending email on behalf of your domain.

The Future of Business Email

Business email will continue to evolve as organisations adopt cloud services, automated workflows and AI-powered tools. Email is unlikely to disappear as a

core business communication channel, but the systems responsible for protecting and managing it will become more sophisticated.

Authentication standards are likely to remain a major focus as providers work to reduce spoofing, phishing and unauthorised bulk sending. Organisations should expect greater emphasis on correctly configured SPF, DKIM and DMARC, alongside secure transport and account protection.

AI will also influence how businesses manage email. Intelligent filtering, automated classification, writing assistance and threat detection can reduce manual work and help teams respond more efficiently. However, AI-generated phishing and more convincing impersonation attempts may also increase the importance of verification and employee awareness.

For businesses, the practical lesson is straightforward: email infrastructure should be treated as an essential part of digital operations. A well-managed provider, accurate DNS records and consistent security practices will remain important regardless of how the technology develops.

Conclusion: Professional Email Starts With the Right Infrastructure

Business email hosting is more than a way to create professional-looking addresses. It is a critical part of how an organisation communicates with customers, manages internal work and protects its digital identity.

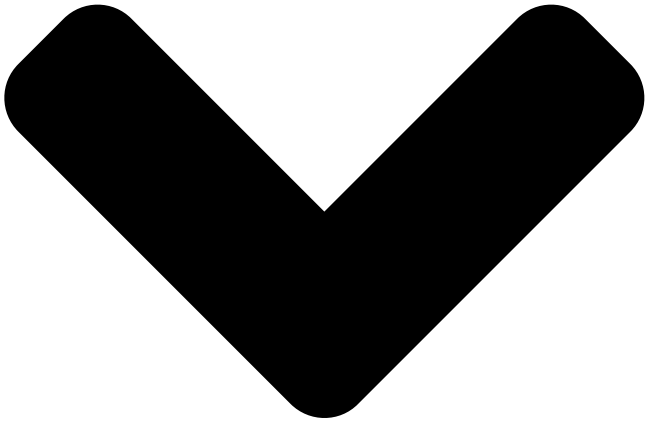
Choosing the right provider is only the first step. Correct MX, SPF, DKIM and DMARC records help ensure that messages reach their intended destinations and that receiving systems can verify your domain. Strong authentication, secure access and careful migration planning help reduce the risk of disruption and compromise.

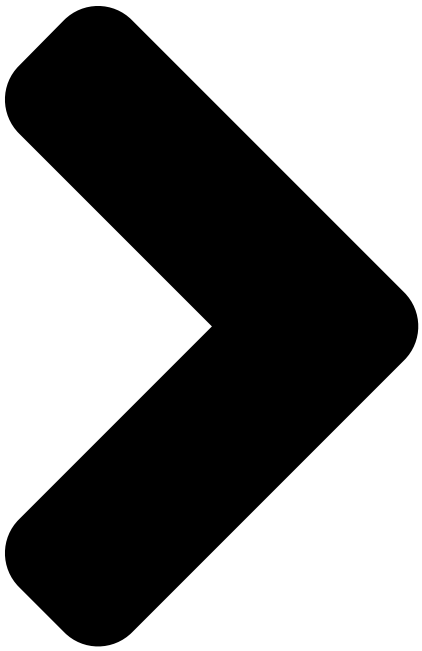
For businesses setting up email for the first time, a bundled hosting solution may be a convenient starting point. Organisations with more advanced collaboration, security or compliance needs may benefit from a dedicated email platform.

If you are building a new website or reviewing your existing setup, explore TSI Digital Solution's hosting and business email package. It brings together website hosting, a domain and branded business email in one package.

Frequently Asked Questions (FAQ)

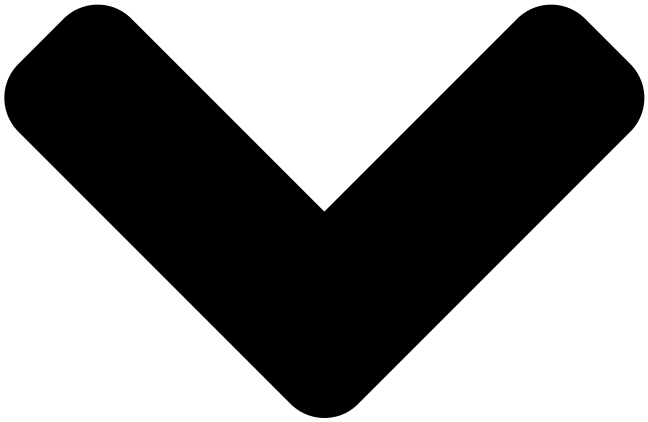
What is the best email hosting provider for a small business?

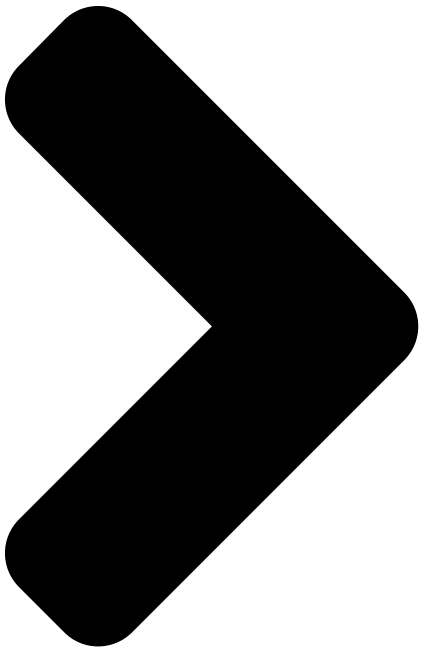




The best provider depends on how the business works. Google Workspace suits teams that rely on Google’s collaboration tools, Microsoft 365 is a strong option for businesses using Outlook and Office applications, and Zoho Mail, Titan can suit organisations seeking a more cost-conscious email service. Privacy-focused providers may be preferable when data protection is a leading consideration.

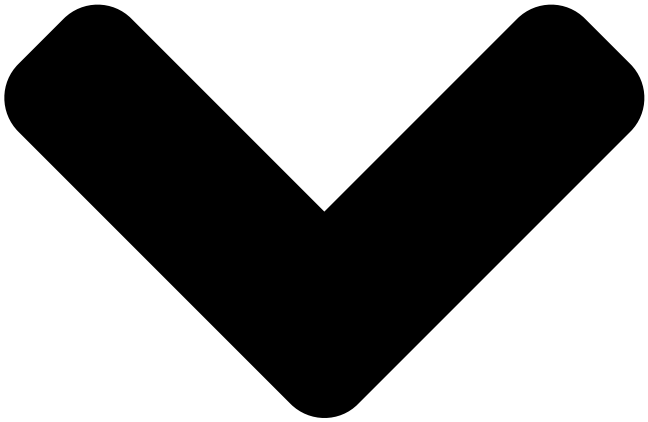
Which DNS records are required for business email?

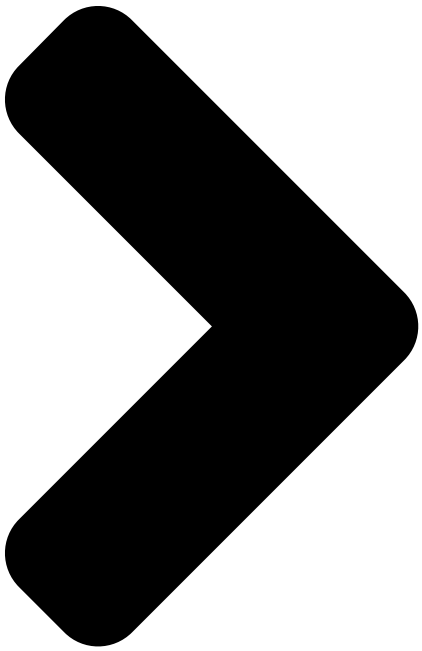




Most hosted email services require MX records for incoming mail and TXT records for domain verification and authentication. SPF, DKIM and DMARC are important for validating outgoing email. Some providers also require CNAME or SRV records for additional services. Always use the exact configuration supplied by your provider.

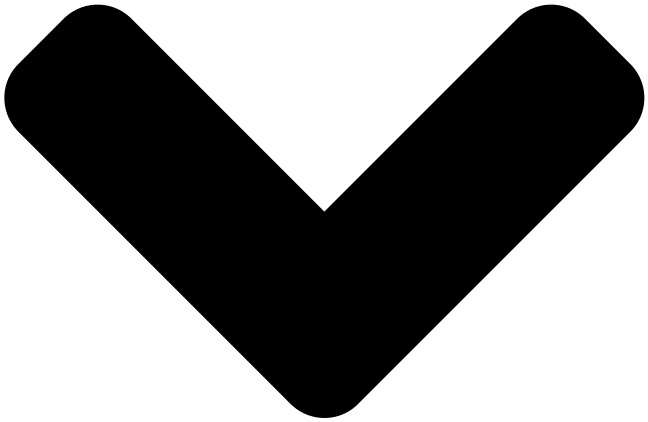
What is the difference between SPF, DKIM and DMARC?

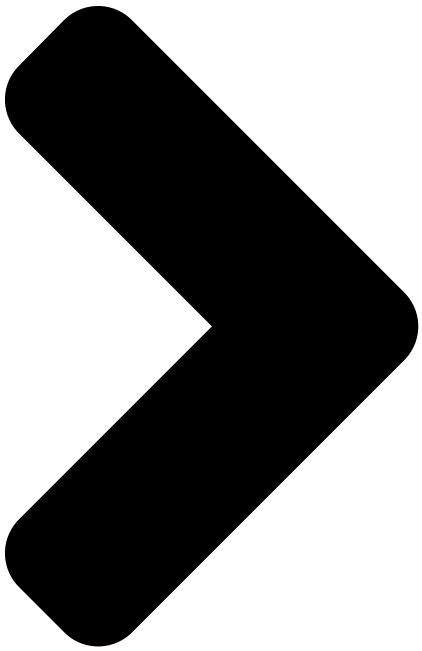




SPF identifies which servers are authorised to send email for a domain. DKIM adds a cryptographic signature that receiving servers can verify. DMARC uses SPF and DKIM results, together with domain alignment, to define how receiving servers should handle messages that fail authentication and to provide reporting.

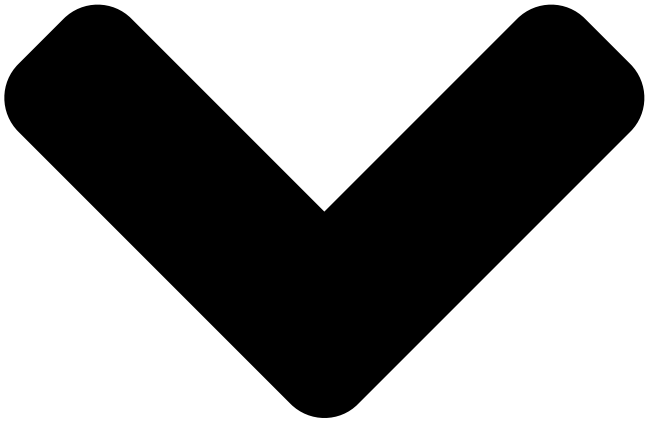
Can I change my business email provider without losing old emails?

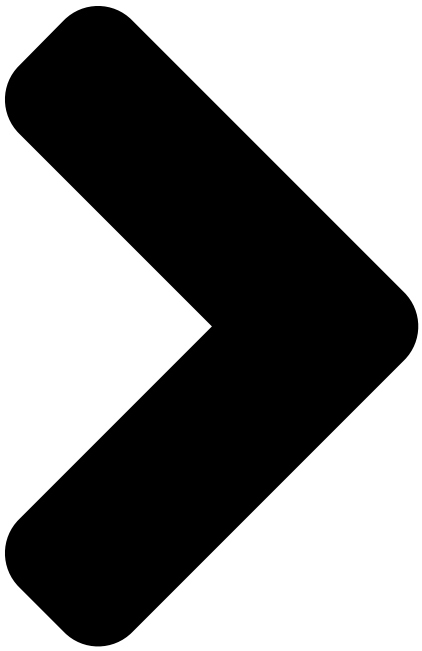




Yes, provided the migration is planned properly. Mailboxes and relevant data can be transferred using supported migration tools or protocols. Keep the old service active during the transition, verify that messages and attachments have transferred and test the new system before cancelling the previous subscription.

Why are my business emails going to spam or being rejected?





Possible causes include incorrect SPF, DKIM or DMARC records, poor sending reputation, suspicious message content, sending-volume issues or problems with the recipient’s filtering system. Review email headers, authentication results and provider logs to identify the cause. Correct DNS configuration is an important starting point, but it does not guarantee inbox placement.

The best provider depends on how the business works. Google Workspace suits teams that rely on Google’s collaboration tools, Microsoft 365 is a strong option for businesses using Outlook and Office applications, and Zoho Mail, Titan can suit organisations seeking a more cost-conscious email service. Privacy-focused providers may be preferable when data protection is a leading consideration.

Most hosted email services require MX records for incoming mail and TXT records for domain verification and authentication. SPF, DKIM and DMARC are important for validating outgoing email. Some providers also require CNAME or SRV records for additional services. Always use the exact configuration supplied by your provider.

SPF identifies which servers are authorised to send email for a domain. DKIM adds a cryptographic signature that receiving servers can verify. DMARC uses SPF and DKIM results, together with domain alignment, to define how receiving servers should handle messages that fail authentication and to provide

reporting.

Yes, provided the migration is planned properly. Mailboxes and relevant data can be transferred using supported migration tools or protocols. Keep the old service active during the transition, verify that messages and attachments have transferred and test the new system before cancelling the previous subscription.

Possible causes include incorrect SPF, DKIM or DMARC records, poor sending reputation, suspicious message content, sending-volume issues or problems with the recipient’s filtering system. Review email headers, authentication results and provider logs to identify the cause. Correct DNS configuration is an important starting point, but it does not guarantee inbox placement.

Reach Out to Us

Need help choosing or connecting business email?

Contact TSI Digital Solution to discuss your website, domain and email requirements. Ask about the right setup for your business and how to avoid common DNS and configuration problems.

Leave a Reply

Logged in as TSI Digital Solution. Edit your profile. Log out? Required fields are marked *

Message*

Post Comment

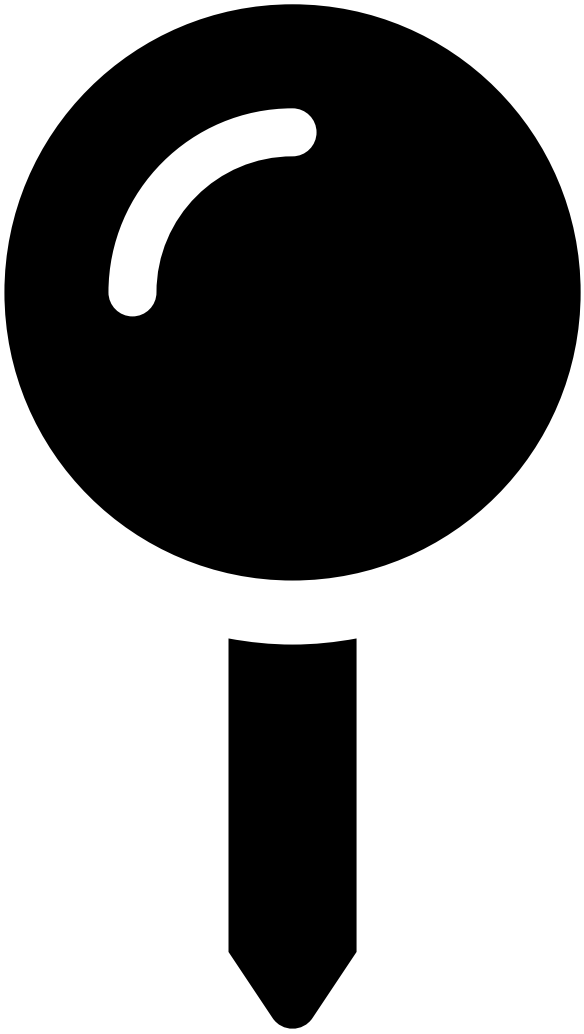
Go back >

Get in Touch

We Reflect

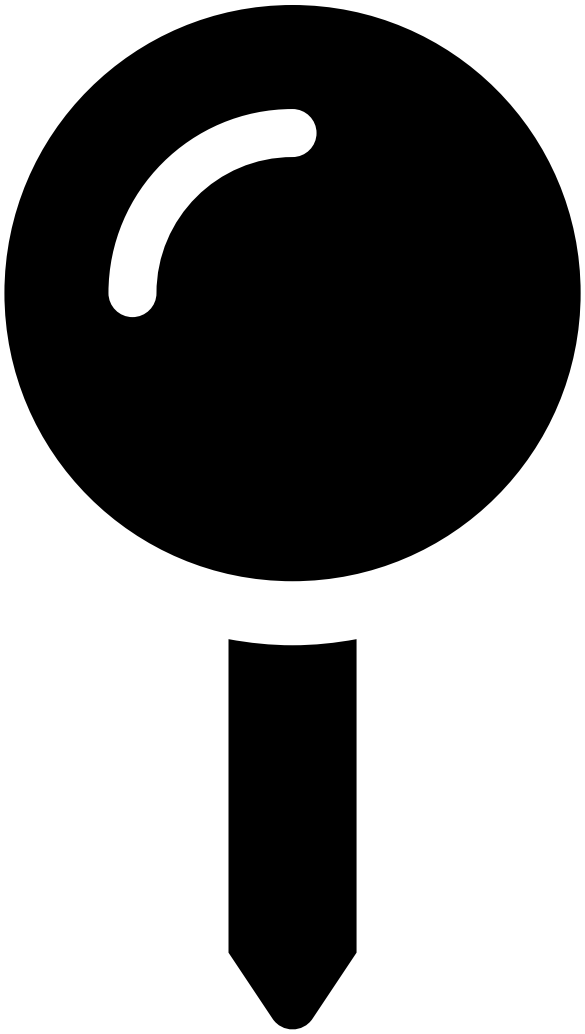
Your Wishes

Contact



TSI Digital Solution
(Brand of PT Tripple SoRa Indonesia)

Jl. Sunset Road No.815 Seminyak, Kuta, Badung, Bali – 80361, Indonesia

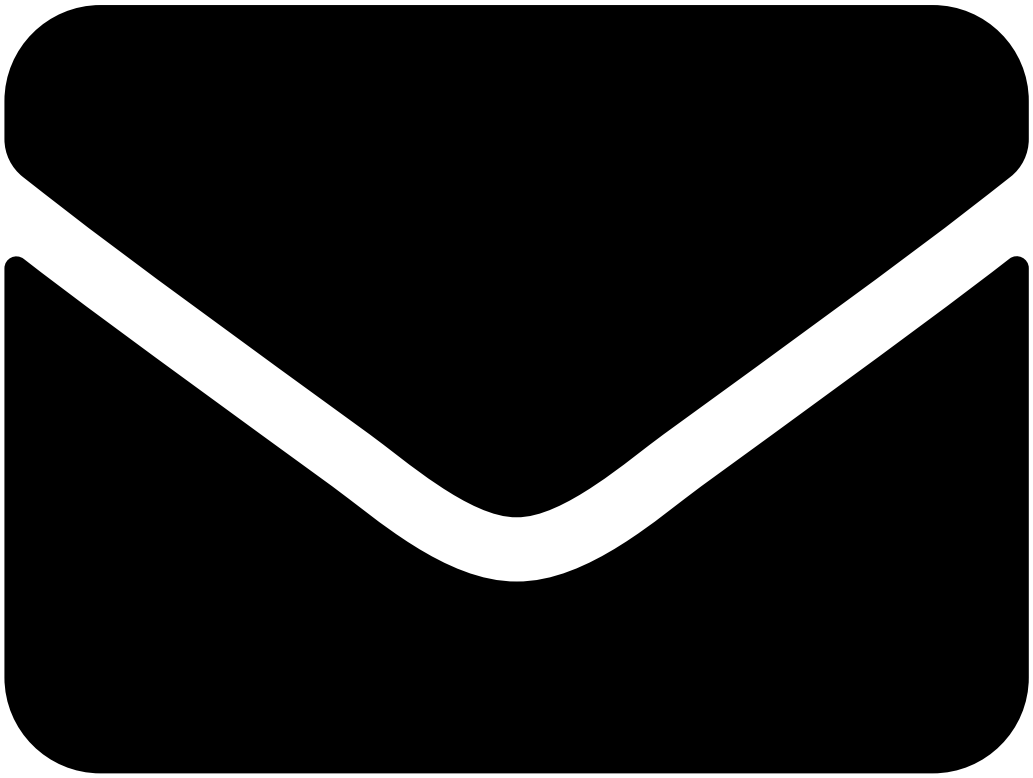


TSI Digital Solution
(Brand of PT Tripple SoRa Indonesia)

Jl. Sunset Road No.815 Seminyak, Kuta, Badung, Bali – 80361, Indonesia



+(62) 813-3936-1507



contact@tsidigitalsolution.com

Services

- Website/e-Commerce
- Apps
- AI Agents

- Technical/SEO

- Branding

- Social Media

- Graphic Design

- Copywriting

- Photo-& Videography



tsidigitalsolution.com
tsidigitalsolution.be
tsidigitalsolution.nl

Copyright © 2022 –

TSI Digital Solution | All rights reserved.

Edit Template