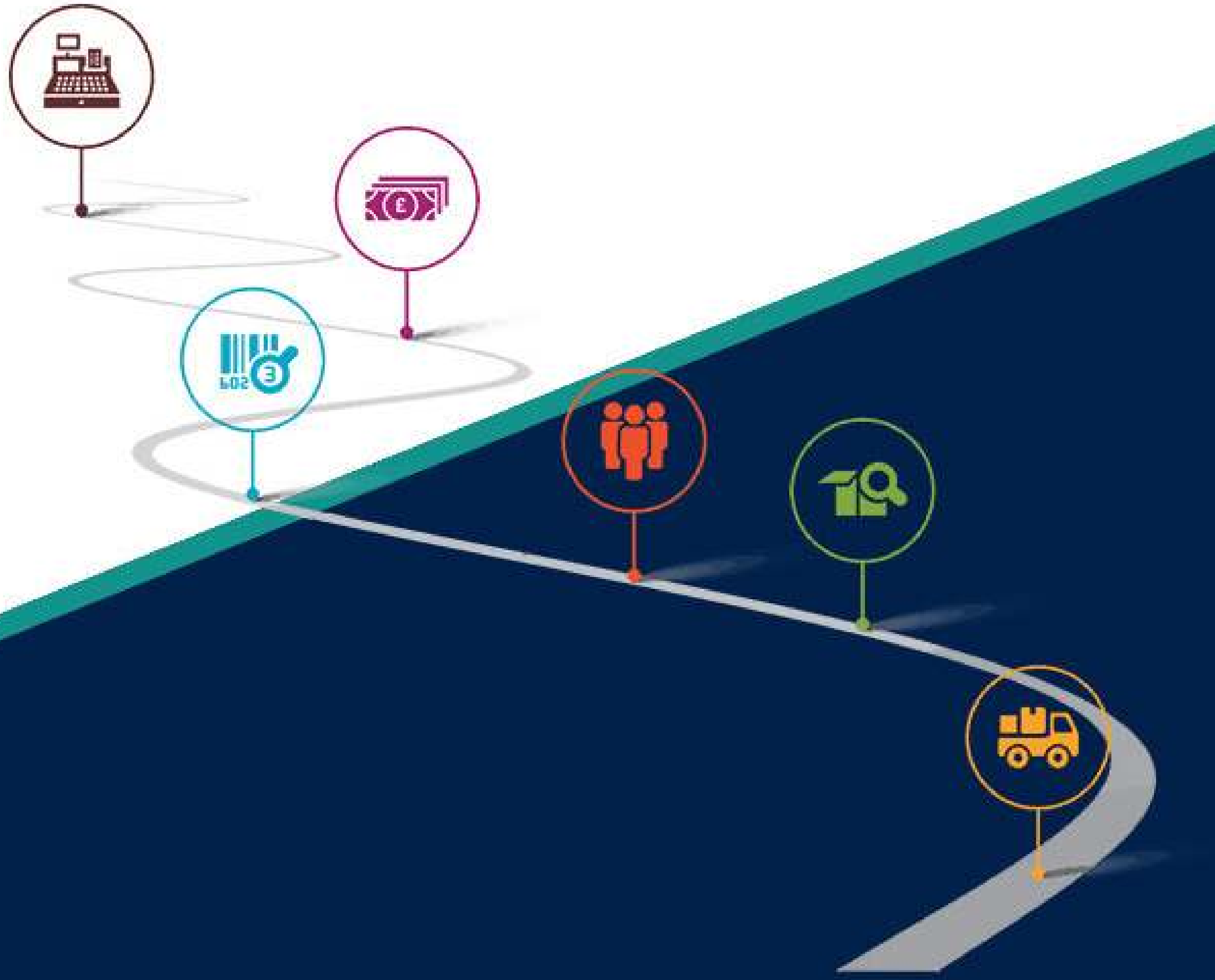
The Portal People
integrated ebusiness



Beginners Guide To Domain Names

Knowledge Series

Table Of Contents

If you've ever wondered what a domain name is and how it works, you’re in the right place. Let’s break it down, from buying a domain to understanding what happens behind the scenes with those mysterious DNS services and zone files.

What is a Domain Name?

Simply put, a domain name is your website’s address in the form of a human friendly name on the internet. It’s what people type into their browsers to find your site, like yourbusiness.co.uk or greatblog.com. Think of it like your home address but for the web.

When you buy a domain name, you're essentially renting a spot on the internet. You don't own the domain outright forever, but you get exclusive rights to use it for as long as you keep paying for it. If you stop renewing it, someone else can swoop in and register that domain.

What Happens When You Buy a Domain Name?

Buying a domain name is more like leasing it. You're paying to have the right to use it for the period you paid for, typically one to ten years, depending on the provider. Once your time is up, you either renew the lease or risk losing it to someone else.

Ownership: Do You Actually Own It?

Not exactly. You’re more of a tenant than a homeowner. While you have the rights to the domain for as long as you keep paying, you don’t actually “own” it in the sense of permanent possession. You’re really leasing it from a domain registrar like GoDaddy or Namecheap, who manage domains on your behalf.

Domain Endings: What’s the Difference Between .co.uk, .com, .org, and Others?

You’ve probably noticed that websites end in different ways .com, .co.uk, .org, and the rest. These endings are called Top-Level Domains (TLDs), and they serve different purposes. Here's a breakdown of some of the most common:

- **.com**: The most common, short for “commercial.” It’s typically used by businesses but is now a go-to for just about anything.
- **.co.uk**: This is for businesses and websites in the UK. It gives a local feel, which can be good if your audience is mainly in the UK.
- **.org**: Originally for non-profits, but nowadays, anyone can use it.
- **.net**: Once meant for network companies, but now it’s a general option like .com.
- **.gov**: Reserved for government websites.
- **.edu**: Used by educational institutions.

TLD's can also relate to countries for example:

- **.is**: Iceland
- **.it**: Italy
- **.je**: Jersey
- **.jm**: Jamaica
- **.jo**: Jordan
- **.jp**: Japan

You can find a more comprehensive list on the IONOS website

Who Governs All This?

At the top of the domain name pyramid sits ICANN (Internet Corporation for Assigned Names and Numbers). ICANN is like the boss of domain names globally. They manage the whole domain name system (DNS) and decide who can operate specific TLDs.

For country-specific domains like .co.uk, Nominet is the governing body in the UK. They manage all the .uk domains and ensure that they’re functioning properly.

How Do Domain Names Actually Work?

Let’s say you type example.com into your browser. What’s happening behind the scenes?

The Browser Looks for the IP Address: Every domain name is linked to an IP address, a series of numbers that identify where the website lives on the internet. Since IP addresses are a pain to remember, domain names make it easier for us humans.

Domain Name System (DNS): This is where DNS comes in. DNS is like the phonebook of the internet. When you type in a domain name, DNS translates it into the corresponding IP address so your browser knows where to find the website.

DNS Services and Zone Files: What Are They?

DNS might sound complicated, but it’s really just a system that converts easy-to-remember domain names into IP addresses. Without it, we’d all be memorising long strings of numbers instead of web addresses like coolsite.co.uk.

DNS Services

When you buy a domain, DNS services usually come as part of the package. These services are like air traffic control for your domain, directing requests to the right “destination” (i.e., web server, email server, etc.) when someone types your domain name into their browser or sends an email to your domain.

Zone Files: A Deeper Dive

A zone file is a simple text file that contains all the essential instructions for directing traffic to your domain. Think of it as the instruction manual for your domain name. It includes the IP address of your website, but that's not all—zone files can do much more than just handle websites. They control where your emails go, verify your domain for security, and more.

Here are some key types of records found in a zone file:

- A Record (Address Record): This is the most basic type of record, which maps your domain name to the IP address of your web server. So when someone types example.co.uk into their browser, the A record tells DNS where to send them.
- MX Record (Mail Exchange Record): Want email for your domain? The MX record tells the internet where to deliver emails sent to @yourdomain.co.uk. It points to the mail servers responsible for receiving and sending emails for your domain.
- TXT Record (Text Record): This is where things get a bit more interesting. TXT records store text information for various purposes, including domain verification and email authentication.

Examples of TXT Records

- SPF (Sender Policy Framework): An SPF record is a type of TXT record that helps prevent email spoofing. It lists which mail servers are allowed to send emails on behalf of your domain. Without SPF, spammers could pretend to send emails from @yourdomain.co.uk, which could cause deliverability issues and make your emails look dodgy.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): This is another type of TXT record used to protect your domain from email fraud. DMARC works together with SPF and DKIM (more on that in a second) to ensure that emails sent from your domain are legitimate. It also allows you to receive reports on any suspicious activity involving your domain name.
- DKIM (DomainKeys Identified Mail): DKIM adds a digital signature to your emails, verifying that the email hasn't been tampered with and really comes from your domain. It’s a bit technical, but basically, it ensures the integrity of your emails.
- CNAME Record (Canonical Name Record): A CNAME record points one domain name to another domain. For example, you might want www.yourbusiness.co.uk to automatically redirect to yourbusiness.co.uk without the "www". CNAME records handle that!
- NS Record (Name Server Record): These records point to the name servers that are responsible for your domain. Name servers are like phone operators for your domain, routing traffic and requests to the correct places (your web host, email provider, etc.).
- SRV Record (Service Record): SRV records are used to define the location of servers for specific services. For example, if you use VoIP (Voice over IP) or chat services, an SRV record might direct users to the correct server for those services.

Why All These Records Matter

All these different types of records allow your domain to do more than just host a website. They control how emails get delivered, who can send emails from your domain, and ensure the smooth functioning of various services tied to your domain name.

For instance, setting up SPF, DKIM, and DMARC records helps protect your brand's reputation and reduces the risk of your emails ending up in spam folders. It also makes it much harder for spammers to use your domain for phishing attacks.

How Do You Manage Zone Files?

Most domain registrars or hosting providers will have a DNS management panel where you can edit your zone file. It might seem a bit daunting at first, but most platforms offer easy-to-use interfaces so you don't need to be a tech expert to manage it.

Why Do DNS Changes Take Time to Propagate?

When you make changes to your DNS records, such as updating an IP address or adding a new MX record for email, those changes don't happen instantly. You might notice that the update takes anywhere from a few minutes to up to 48 hours to take effect. This delay is due to something called TTL (Time to Live).

What Is TTL (Time to Live)?

TTL is essentially an expiration date for DNS records that tells other servers how long to keep the current information before checking for updates. Every DNS record has a TTL setting, which is usually measured in seconds. For example, a common TTL value is 3600 seconds (1 hour).

When someone tries to visit your website or send an email, their device asks the DNS for the relevant information (such as the IP address or mail server). The DNS will look at its cached information—data it has stored from the last time it checked—and use that unless the TTL has expired. Once the TTL expires, the DNS server will go back to your domain's authoritative DNS servers to fetch fresh data.

How TTL Affects DNS Propagation

Here’s why TTL matters for DNS changes:

- **Low TTL (e.g., 300 seconds / 5 minutes)**: When the TTL is low, DNS servers will check for updates more frequently. This means that if you make a change to your zone file, such as pointing your domain to a new IP address, the changes will propagate faster. However, a lower TTL means that DNS servers will query your authoritative DNS more often, potentially increasing the load on your servers.
- **High TTL (e.g., 86400 seconds / 24 hours)**: A higher TTL means that DNS servers will cache the old data for longer before checking for updates. If you have a high TTL, changes to your DNS records may take longer to propagate—sometimes up to 48 hours. However, high TTL values reduce the number of queries to your DNS servers, which can be beneficial for reducing server load.

Why You Might See Delays of Up to 48 Hours

When you make a change to your DNS records, servers around the world need to refresh their cached data based on your TTL settings. If the TTL is set high (e.g., 24 hours or more), those servers will keep using the old information until the TTL expires. This is why DNS changes can sometimes take up to 48 hours to fully propagate across the globe.
Even if you set a low TTL, some DNS servers (especially in remote or less frequently updated regions) might not immediately check for updates. That's why there can still be a bit of unpredictability, with some users seeing the changes within minutes and others taking longer to experience the updated DNS.

How to Minimise Propagation Delays

If you know you’ll need to make a DNS change (for example, moving your website to a new host), you can prepare ahead of time by temporarily lowering the TTL on the relevant records. For instance, you could set the TTL to 300 seconds (5 minutes) a day or two before making the change. This way, when the change happens, it propagates more quickly. Once the change has fully taken effect, you can increase the TTL again to reduce the load on your DNS servers.

The Portal People
integrated ebusiness

The Portal People Ltd
Tel: 01323 385 391
Web: portalpeople.uk