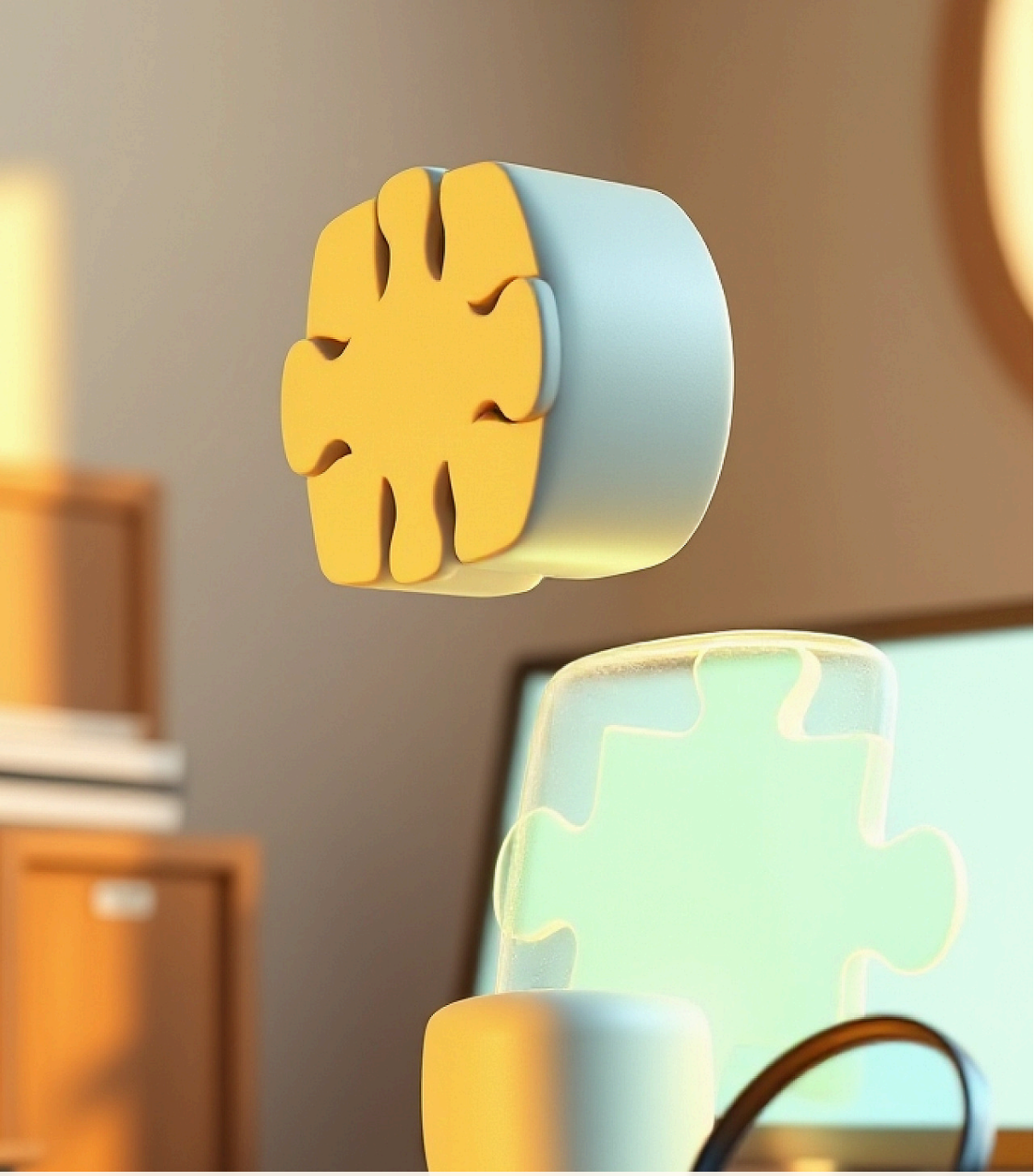
Why is HTTPS used?



www.yzokul.com.tr

Why is HTTPS used?



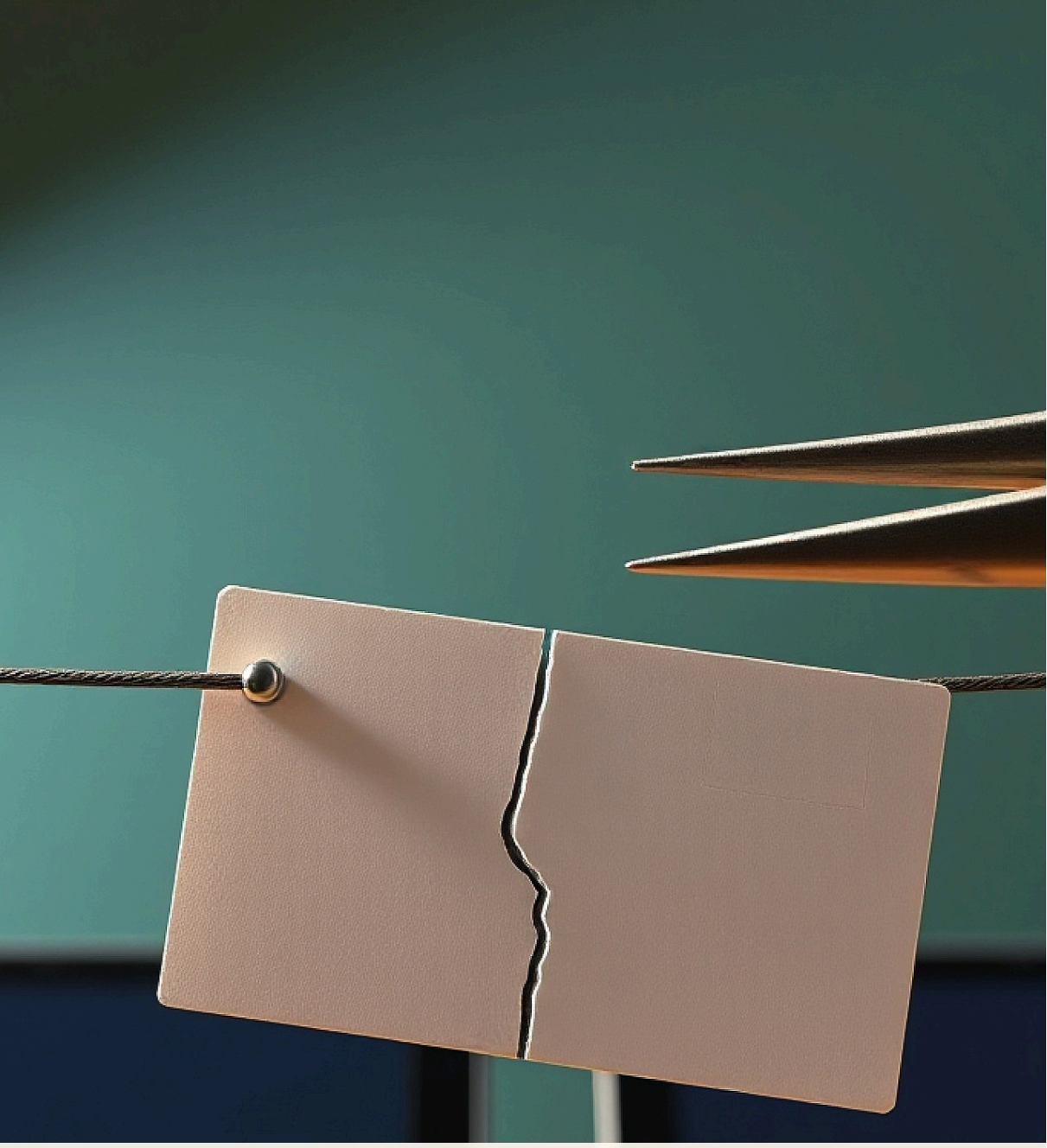
Why is HTTPS used? The short answer is that HTTPS is HTTP sent over an encrypted, tamper-checked connection. HTTP is the set of rules your browser uses to talk to a website. Encryption scrambles the traffic so others cannot easily read it. Tamper-checking means changes in transit are noticed. Each part of this answer is unpacked on the pages that follow.



When you open a website, your browser and the website's server exchange requests and replies. These messages follow a set of rules called HTTP, which stands for HyperText Transfer Protocol. In plain HTTP, those requests and replies travel as ordinary readable text. That plain exchange is exactly what HTTPS will wrap in protection. Understanding HTTP first makes the reason for HTTPS clear.



Imagine sending a postcard through the mail: anyone who handles it can read the message on the back. Plain HTTP traffic works the same way on a shared network, such as public Wi-Fi. Someone on the same network can look at the traffic and read what is being sent. This readability is the first problem HTTPS is designed to fix. It is not about hiding everything, but about protecting the content.



A second problem with plain HTTP is that traffic can be changed as it passes. A middle person on the network could quietly alter the data in transit. The receiver would then get different information without noticing. This is called a man-in-the-middle attack, and it can affect forms, downloads, or page content. HTTPS addresses this risk by making silent changes detectable.



HTTPS is the same HTTP conversation, but carried inside an encrypted tunnel. The browser still requests pages and the server still replies; the web works the same way. Only the wrapping changes: the traffic is protected as it travels. Think of it as putting the postcard inside a sealed envelope. The address is visible, but the message is not.



Encryption turns readable traffic into scrambled data that outsiders cannot easily understand. Both ends, the browser and the server, hold the keys needed to turn it back into plain text. Anyone watching the network sees only scrambled bytes, not the content. This protects things like passwords, messages, and form entries. Encryption is the first protection that HTTPS adds.



The encrypted connection also checks whether the data arrived unchanged. This property is called integrity protection. If someone alters the data in transit, the change is noticed instead of silently accepted. The receiver can reject tampered data rather than trust it. Integrity protection is the second protection that HTTPS adds, and it works alongside encryption.



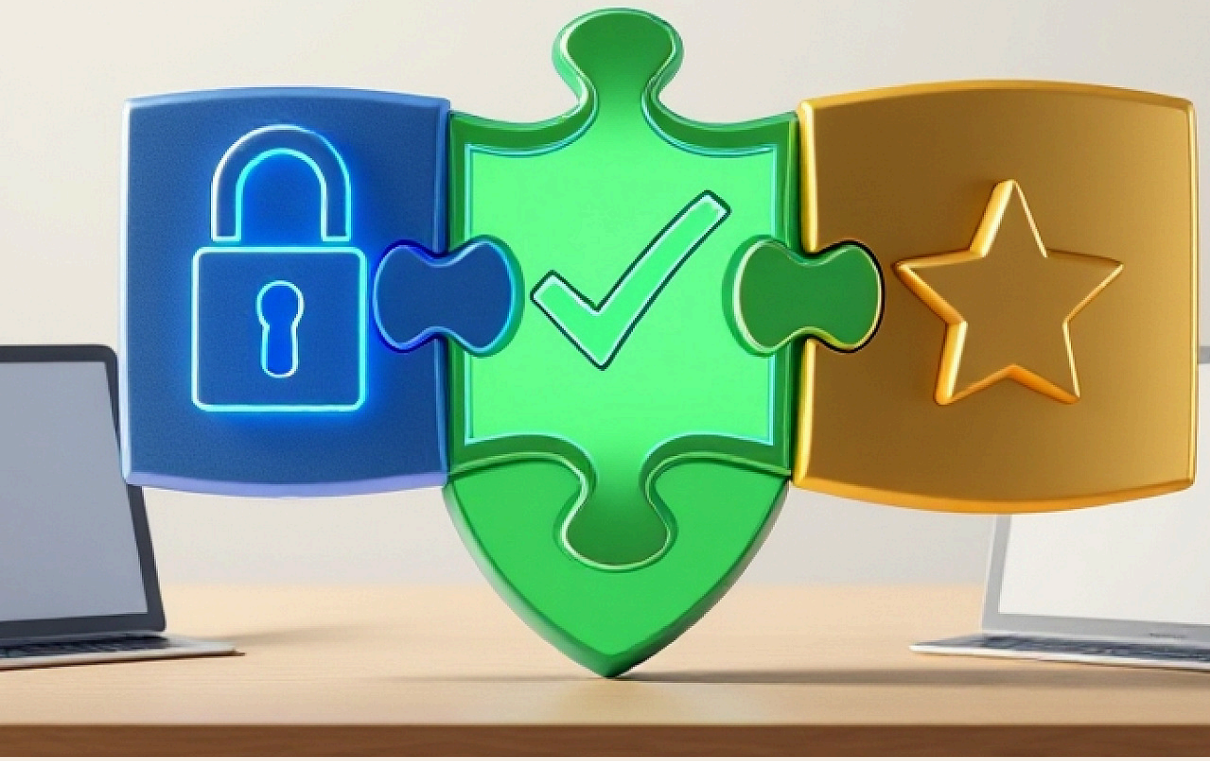
A server presents a certificate, which works like an ID card for the service. The browser checks this certificate before trusting the connection. The certificate helps confirm which service you are actually connected to. It does not judge the site's content; it only supports identity. This identity check is the third protection that HTTPS adds.



Trusted certificate authorities sign certificates. These are organizations whose job is to verify identities and issue signed certificates. Your browser carries a list of authorities it trusts. A valid signature links the certificate to an identity that has been checked. If the signature does not match, the browser treats the certificate as untrusted.



When the certificate does not check out, the browser shows a warning instead of quietly proceeding. The warning may say the connection is not private or the certificate is invalid. This is the identity check doing its job. You can then decide not to continue. A warning is not a guarantee of danger, but it is a signal to be careful.



Putting the pieces together: HTTPS provides encrypted content, integrity checks, and a checked identity, all in one connection. Encryption keeps the content hidden from outsiders. Integrity protection makes silent changes detectable. The certificate helps confirm the service you reached. Each piece covers a different risk, and together they protect the connection.



HTTPS protects the connection, not the honesty of the site's content. A secure tunnel can still carry misleading information. The site may be accurately identified yet still offer inaccurate claims. Connection security and content trust are separate matters. HTTPS does its job even when the content is wrong.



Separate two questions: is the connection private and intact, and is the information on the page accurate? HTTPS answers the first question. It does not answer the second. A site can use HTTPS and still publish false or misleading content. Always judge the information itself, not just the connection.



A common mistake is believing the padlock icon means the site is trustworthy. The padlock only tells you the connection is protected. It does not mean the site's owners are honest or the content is correct. Treat the padlock as a sign of connection security, not a sign of truth. Check the site's information separately.



Another common mistake is believing HTTPS makes you fully anonymous. It hides the content of your traffic, but others may still see that you connected to a particular site. The domain name can be visible even when the page content is encrypted. HTTPS protects content, not the fact of connecting. Full anonymity requires other tools and habits.



What to remember: HTTPS encrypts and integrity-checks ordinary web traffic and helps verify the service's identity. These protections make reading and silent changing much harder for others on the network. But a protected connection and trustworthy content are separate matters. Use HTTPS as a baseline, and still judge the information you read.