HTTPS & TLS

What the padlock actually guarantees, and what it does not.

Computing

TLS wraps HTTP in encryption, using a certificate to prove the server controls the domain and a key exchange to agree a secret nobody watching can derive.

CURRENT	PORT	CERT LIFE
TLS 1.3	443	≤ 90 days typical

- Confidentiality: nobody in between can read it.
- Integrity: nobody in between can alter it undetected.
- Authenticity: the server controls that domain name.
- It does NOT mean the site is trustworthy or legitimate.
- Certificates are free and automatic — there is no cost excuse.
- HSTS tells browsers never to try plain HTTP again.

LOOK FOR IT

A phishing site can have a perfectly valid certificate. The padlock says 'encrypted', not 'safe'.

TLS 1.3 removed the older weak options and cuts the handshake to one round trip. Disable everything below TLS 1.2.