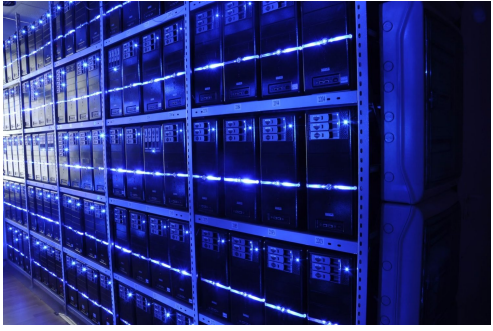
The Internet and its Uses

IGCSE Computer Science ▪ Topic 5

IGCSE Computer Science

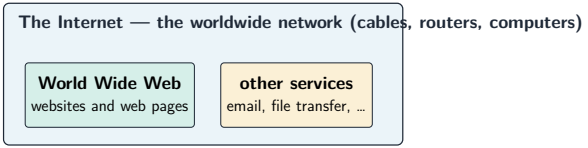
What we will cover

1. Internet vs the web
2. URL & the browser
3. How a page reaches you
4. Cookies & blockchain
5. Cyber threats
6. Keeping data safe



1 Web basics

Internet vs the world wide web



- The **internet** 互联网 is the **infrastructure** 基础设施 – the huge worldwide network of computers and the cables, routers and connections that join them.
- The **world wide web** 万维网 (WWW) is a collection of **websites** 网站 and web pages that you view using the internet.

The internet and the world wide web

A router joins your home network to the internet and sends data to the right place

A URL is an address in three parts

the parts of a URL

A **uniform resource locator** 统一资源定位符 (URL) is a text address you type into a **web browser** 网页浏览器. In `https://www.example.com/books/index.html`:

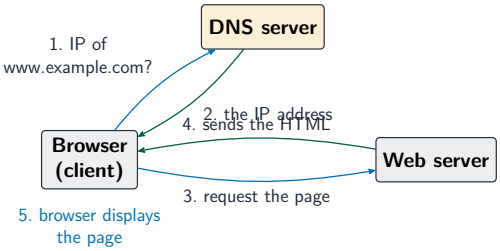
- `https` – the **protocol** 协议, the rules for transferring the page
- `www.example.com` – the **domain name** 域名 of the web server
- `/books/index.html` – the file's path on that server

What a browser actually does

rendering 渲染	turns the page's **hypertext markup language** 超文本标记语言 (HTML) into what you see
displaying	puts the finished page on the screen and follows the links you click

It also manages how the page is presented – layout, text and images – which is why the same page can look different in two browsers.

How a web page reaches you



1. you type a URL and press enter – a name, not a number
2. the browser asks a **DNS** 域名服务 for the IP
3. the DNS returns the IP address
4. the browser contacts the **web server** 网络服务器
5. the server sends back the HTML
6. the browser renders the page

> DNS is the internet's phone book – name in, IP address out.

2 Data and trust

Cookies

	session	**persistent**
kept on close?	no	yes
used for	basket, short-term	remembering you between visits

A **cookie** 网络跟踪器 is a small text file a site stores on your device to remember things – logins, preferences, basket contents.

> Session cookies die when you close the browser; persistent ones survive to recognise you next time.

A cookie is a small text file

a cookie

a small text file
stored on your computer
remembers settings / login

A small text file the site stores on your computer. It can hold your preferences, the contents of a basket, or personal details such as a login or address, so you do not type them again – and it can also track what you look at.

What a cookie is for

What it holds	A small text file the site stores in your browser – a session id, a language choice, items in a basket.
Track user preferences	Sites use them to **track user preferences** 跟踪用户偏好 between visits, so you stay logged in and the settings persist.
The other use	Third-party cookies follow a visitor *between* sites to build an advertising profile – the reason for consent banners.
Privacy settings	**Privacy settings** 隐私设置 in a browser control which cookies are accepted, and clearing them logs you out of everything.

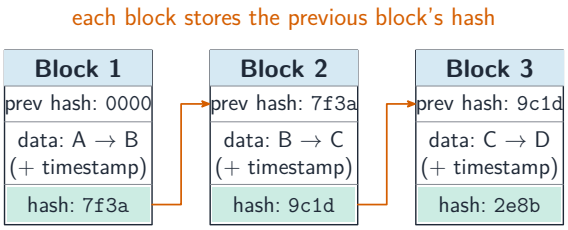
A cookie cannot run code. What makes it sensitive is not what it does, but what it lets a site *remember*.

Digital currency

A **digital currency** 数字货币 is money that exists only in **electronic form** 电子形式.

> Stored and moved by computer, and spendable online. The problem is trust: what stops someone spending the same money twice, or editing the records? That is the question blockchain exists to answer.

Blockchain



A **blockchain** 区块链 is a shared **digital ledger** 数字账本 of every transaction. Each block holds the data, a **timestamp** 时间戳, a **hash** 哈希值, and the hash of the block before.

> Change one old block and its hash changes – breaking every block after it. That chained hash is what makes tampering obvious.

3 Security

Cyber threats

brute force 暴力破解
try many passwords
fast until one works

data intercep
"listen in" to st

DDoS 分布式拒绝服务
flood a server un-
til it cannot respond

malware
virus, wo
spyware,

phishing / social engineering – trick a person into giving up secrets

A padlock: cyber security locks data and systems against malware, phishing and unauthorised acce

The cyber-security threats, by what each does

DDoS 分布式拒绝服务	flooding a server with so many requests that it cannot respond, so the website goes down
hacking 黑客攻击	gaining access to a system without permission
pharming 域名欺骗	secret code sends you to a fake website even when you type the correct address
phishing 网络钓鱼	fake emails or messages that trick you into giving away private details
brute-force attack 暴力破解	trying every password until one works
data interception 数据拦截	reading data as it travels across a network

Phishing needs you to click; pharming does not. That difference is why one is beaten by care and the other only by technical defences.

Three attacks, and the words behind them

Brute force attack	A **brute force attack** 暴力破解 tries every combination until a password works – which is why length beats complexity.
Distributed denial of service	A **distributed denial of service** 分布式拒绝服务 (DDoS) attack floods a server from many machines at once, so real users cannot get through.
DNS	The **domain name service** 域名服务 turns a name into an IP address; poisoning it sends visitors to the attacker's server instead.
Hash value	A **hash value** 哈希值 is a fixed-length fingerprint of data. Passwords are stored hashed, so a stolen database does not hand over the passwords.

For each threat name the target, the method and one defence. That triple answers almost every question in this topic.

Malware – know the differences

virus	attaches to a file; spreads when opened
worm	spreads over a network on its own
Trojan	pretends to be useful software
spyware	secretly records what you do
ransomware	locks files, demands payment

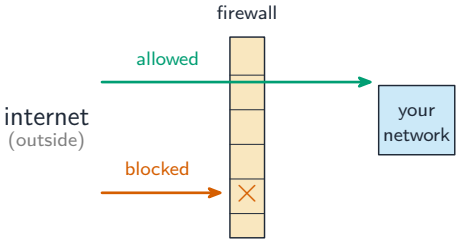
The key distinction: a worm needs no file and no user action – it copies itself across the network. A virus needs a file to be opened.

The malware types

virus 病毒	attaches to a file and needs a person to run it
worm 蠕虫	copies itself across a network with no human action
trojan horse 特洛伊木马	disguised as something useful, so you install it yourself
spyware 间谍软件	records what you do – often a **keylogger** 键盘记录器 capturing what you type
adware 广告软件	floods you with unwanted adverts
ransomware 勒索软件	encrypts your files and demands payment for the key

These attacks steal personal data, delete or change files, stop a service working, cost money, and make users lose trust in a company.

Keeping data safe



- **firewall** 防火墙: checks traffic in/out, blocks the disallowed
- **authentication** 身份验证: password, **biometrics** 生物识别, two-step
- **access levels** 访问权限: see only what you need
- anti-malware, updates, **proxy server** 代理服务器

Against phishing the defence is a person: check the spelling, the urgent tone, and the real URL behind a link.

How data is kept safe

firewall 防火墙	checks traffic entering and leaving, and blocks what breaks the rules
anti-malware 反恶意软件	**anti-virus** 杀毒软件 and **anti-spyware** 反间谍软件 – scan for and remove harmful software
authentication 身份验证	proving who you are: a strong password, **two-step verification** 两步验证, or **biometrics** 生物识别 (fingerprint or face)
encryption 加密	scrambles data so an interceptor cannot read it – it does not stop theft, it makes theft useless
automatic updates	updates fix weak points in software, and automating them means they are not forgotten
reading carefully	bad spelling or an urgent tone marks a phishing message, and a strange URL marks an unsafe link

The last two cost nothing and stop the commonest attack there is. Technical defences cannot help a user who types their password into a fake page.

Worked example – breaking down a URL

`https://www.example.com/books/index.html`

- `https` is the **protocol** 协议 – the rules used to transfer the page; the `s` means the transfer is encrypted.
- `www.example.com` is the **domain name** 域名, which identifies the web server and which a DNS server turns into an IP address.
- `/books/index.html` is the **file path and file name** of the resource on that server.

Name each part *with its job*. "The first bit" and "the last bit" describe the URL without explaining anything.

Exam tips

- The **internet** is the worldwide network (the infrastructure); the **world wide web** is the pages you view on it – do not mix the two up.
- Learn how a page loads: the browser asks a **DNS** for the site's IP address, then requests the page from the **web server**, which returns the HTML.
- Match the malware types: **virus** (attaches to a file), **worm** (spreads by itself across a network), **Trojan horse** (pretends to be useful), **spyware**, **ransomware**.
- Match each threat to a defence: phishing/pharming $\rightarrow$ check the URL; brute force $\rightarrow$ strong passwords + two-step verification; interception $\rightarrow$ encryption; hacking/DDoS $\rightarrow$ a firewall.
- A **session** cookie is deleted when you close the browser; a **persistent** cookie is saved to remember you between visits.

4 Recap

Topic 5 – key takeaways

1 Net vs web

internet is the network; web runs on it

2 DNS

name in, IP address out

3 Blockchain

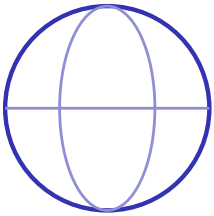
chained hashes make tampering obvious

4 Safety

firewall, authentication, access levels

Check yourself

1. What does a DNS turn a URL into?
2. Which malware spreads with no user action?
3. Which cookie survives closing the browser?
4. What checks traffic in and out of a network?



Answers **1.** an IP address **2.** a worm **3.** persistent **4.** a firewall