INSIDE STORY

HOW THE INTERNET WORKS

COVER NOT FINAL

WRITTEN BY
CRAIG STEELE

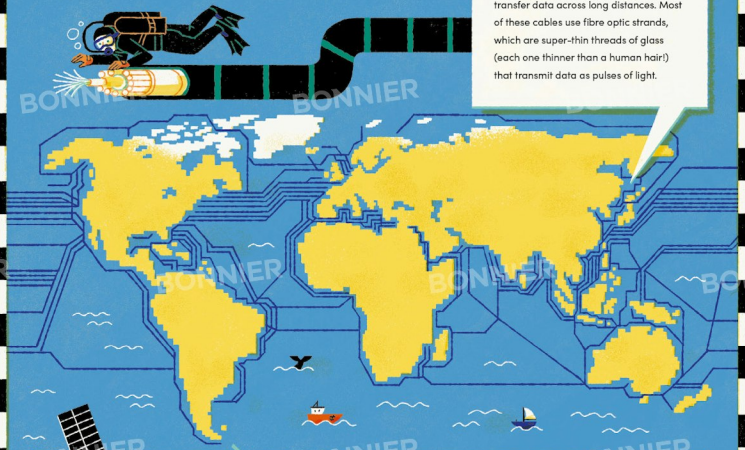
ILLUSTRATED BY
TERRI PO

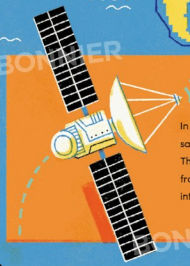
THE INFRASTRUCTURE OF THE INTERNET

Some parts of the internet you can see easily, like your broadband router at home. But did you know most of the internet's structure is actually hidden? Below the sea there are long lines of cables, above you, thousands of satellites orbit Earth, and dotted around the globe are warehouses full of powerful computers. These work together to form the physical foundation of the internet – it's infrastructure – and each one plays an important role.

Cables

There are hundreds of thousands of miles of internet cables zig-zagging across entire continents, and along the seabed, undersea cables are laid to connect countries and islands. These are used to transfer data across long distances. Most of these cables use fibre optic strands, which are super-thin threads of glass (each one thinner than a human hair!) that transmit data as pulses of light.





Satellites

In less populated and more rural areas of the world, satellites are used to connect people to the internet. They orbit high above Earth, beaming signals to and from ground stations. These satellites also provide internet access to people travelling in aeroplanes.

5G Cell Towers

When you use the internet on your phone while out and about, it connects to a nearby cell tower using a high-speed 5G connection. These cell towers are used by mobile network operators (like EE or O2), who send your data through their own networks before it goes to the internet.

Home Wi-Fi

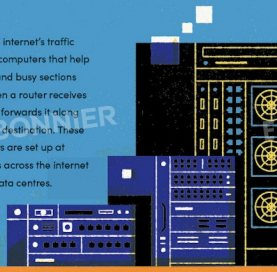
All of your devices at home are most likely connected to the internet using a technology called wireless fidelity, better known as Wi-Fi. Instead of wires or cables, data from your devices is transmitted to a home router using radio waves. The router gives you access to the internet, and it's a smaller, less powerful version than the ones in data centres.

Data centres

A data centre is a giant building that processes data for the internet. They're filled with powerful computers called servers that store the files, code and databases needed by websites and apps. Servers handle millions of requests from across the internet and send data to your device in a fraction of a second. These centres have thousands of machines running all day which get very hot, so need to be cooled constantly. One cooling system uses 4 million litres of water per day, that's the same amount used by a town of 10,000 people!

Routers

Routers are like the internet's traffic officers – they are computers that help data navigate around busy sections of the internet. When a router receives a packet of data, it forwards it along the right path to its destination. These powerful computers are set up at important junctions across the internet world, such as at data centres.



Internet Service Provider

To connect to the internet at home or work, people pay a company called an internet service provider (ISP) for access. They provide network equipment (like a wireless router) and manage the connection to make sure users have reliable speeds, making getting online a breeze.

Internet Exchange Points

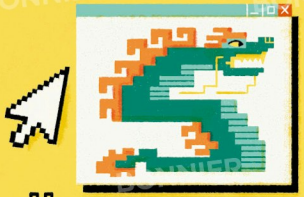
An internet exchange point (IXP) is a location where different ISPs connect their networks to each other. By sharing traffic, data can take the shortest route across multiple networks. Companies that use the internet sometimes keep copies of popular data at an IXP so that it doesn't have to travel as far to reach people, for example, film and TV streaming sites.

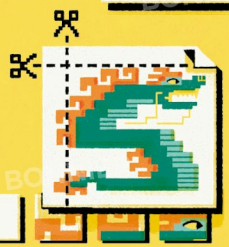
HOW DATA IS SENT ACROSS THE INTERNET

Have you ever thought about the journey your emails, chats, YouTube videos – really every webpage ever – takes to get to you? They travel across continents, under oceans and into your home, before finally reaching your phone, laptop or computer. Photos, videos and web pages are all just data files. When we transfer data across the internet, each computer involved must follow a set of rules – called the Internet Protocol – to make sure that every file reaches its destination quickly and accurately.

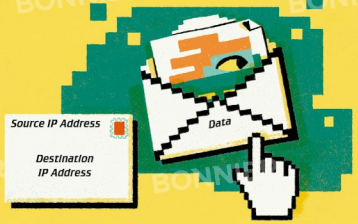
Data on a journey

Rosa wants to download an image of a dragon to use as a cool wallpaper on her phone. Here's how that file is transmitted across the internet, using the Internet Protocol rules:





Step 1 First, the image is chopped into small packets, which are easier to transfer. A small 1 megabyte image file like this might be broken down into 700 packets.



Step 2 Each packet is made up of two parts. The payload and the header. The payload is data from the dragon image file. The header is like a label for the packet, which includes the destination IP address (where the file is going) and the origin IP address (where it's being sent from). It also includes other useful information, like how many packets there are in total.

Packets travel across the world through the internet in the blink of an eye. For example, a packet can travel from a computer in New York to London in 145 milliseconds.

Step 3 The packets are sent individually across the internet, where routers are used to forward each packet towards its destination. As they travel, the packets take different paths. Some can even get lost and "drop" off the network, needing to be retransmitted (sent again).

Step 4 When all the packets have arrived at their destination IP address – Rosa's phone – they're assembled into the correct order using the information in their headers, creating the photo of the dragon.

INTERNET UPDATE

WHAT IS AN IP ADDRESS?

Every device connected to the internet is given a unique Internet Protocol (IP) address. This allows the computers, phones, tablets, routers and all other devices connected to the internet to recognise and communicate with each other.

An IPv4 (version 4) address is typically a group of numbers that looks like this: 108.177.122.139

Most of the time, your gadgets get given a different address every time they connect to the internet – called a dynamic IP address – but some computers get an address that never changes – a static IP address.

INTERNET UPDATE

WHAT IS BINARY?

Computers only understand electrical signals that are either "on" or "off". We represent those signals using two special numbers: 1 and 0. We call these binary digits or "bits" for short. Every file on a computer, laptop, or phone is represented using a sequence of bits

CYBER CRIME ON THE INTERNET

How safe is the internet? Most of our experiences using it are positive, but there is a darker – and sometimes dangerous – side to being online. As more people use the internet for shopping and banking, criminals find more chances to steal money and personal information. But there are ways we can protect ourselves and stay safe online.

Malware most wanted

One way to protect ourselves from cyber crime is to understand what it looks like. Malware, short for malicious software, is used to attack computer systems, destroy data or steal personal information. It can come in a few forms:

VIRUS

A virus is a computer programme which spreads by infecting other files or sending copies of itself through emails and chats between contacts. Viruses can be used to steal sensitive information or delete important files.

TROJAN HORSE

Sometimes malware hides inside an innocent-looking app or game. When you try to use it, the virus is activated. It's named after the famous Greek myth where soldiers snuck into Troy inside a wooden horse.

RANSOMWARE

Ransomware locks you out of a computer system and blocks you from accessing your files. Criminals then demand money (a ransom) to let you back in.

Hacking the human

It's much easier to trick a human than it is to break into a computer, so a main tool if a criminal wants certain information, they'll try to trick a person into making their computer less secure. This is called phishing, and here's how it might happen:

Imagine a cyber criminal wanted access to an email account, they might set a trap that allows them to obtain the password. This is done by creating convincing emails pretending to be from someone's family or friends, or by posing as a trustworthy company and creating a realistic-looking website. Criminals use trust to reel you in and gain your information, so keep an eye out for suspicious messages and friend requests or offers that are too good to be true.

The dark web

The internet is also used by criminals who want to buy and sell illegal goods or do harmful acts. Weapons and dangerous materials are traded in underground markets on a part of the internet called the dark web. These illegal websites are hidden from search engines, and can only be visited using special software. The traders use tools to try and make themselves untraceable, to try and avoid being caught.

Who protects us from cyber crime?

Lucky for us, there are thousands of people whose job is to protect us from cyber criminals.

ETHICAL HACKERS

hack into computer systems, but they're not criminals! Companies ask them to find weak spots in their online systems, then they report their findings and security teams fix the problems to prevent cyber crime.

DIGITAL FORENSICS SPECIALISTS

work with the police to gather evidence and help solve cyber crimes. Rather than dusting for fingerprints, they pull information from computers' storage or analyse server logs for criminal activity.

CYBER THREAT RESEARCHERS

study how criminals attack computer systems and try to spot common patterns or weaknesses. This research helps security experts invent new techniques to tackle cyber crime.

ON ASSIGNMENT

PROTECT YOURSELF FROM CYBER CRIME

You can also protect yourself and your family from cyber criminals. Complete this checklist to strengthen your digital security, then help your family to follow the steps too. Supporting others to stay safe online makes you a good digital citizen.

1. USE STRONG PASSWORDS FOR ALL YOUR ACCOUNTS

Make them long and use random words so they are hard to guess.

2. CHECK YOU HAVE ANTIVIRUS SOFTWARE INSTALLED ON YOUR COMPUTERS

Most computers have antivirus software built in, you just need to make sure it's activated.

3. MAKE SURE YOUR APPS ARE UP TO DATE

Updating your apps to the latest version helps patch any security problems.