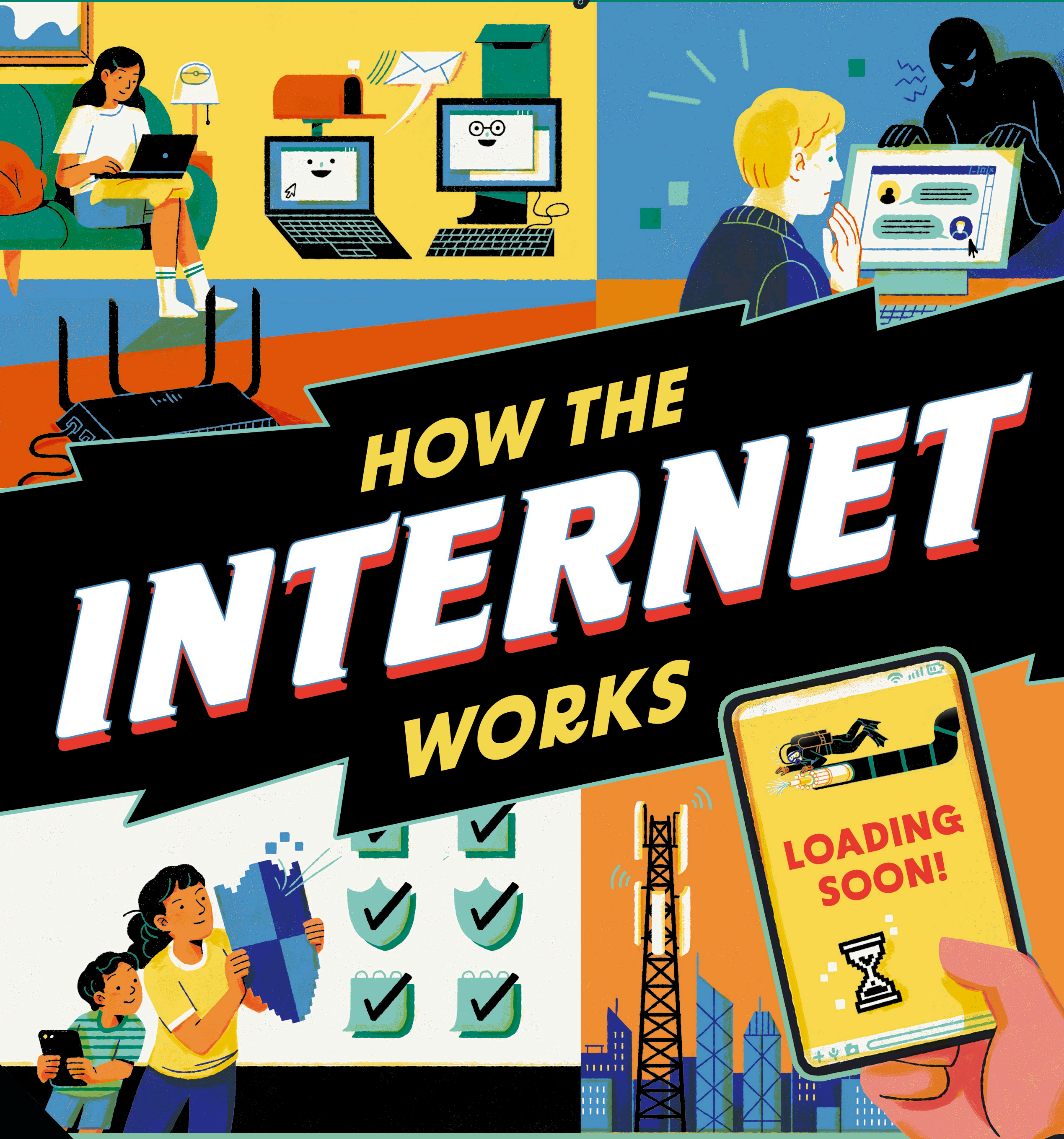
INSIDE STORY

HOW THE INTERNET WORKS



WRITTEN BY
CRAIG STEELE

ILLUSTRATED BY
TERRI PO

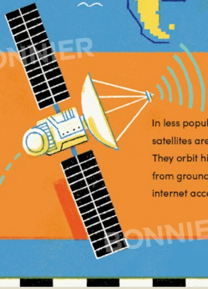
COVER NOT FINAL

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.

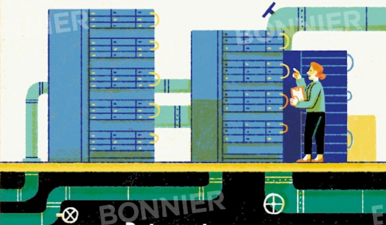


Satellites

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.



Data centres

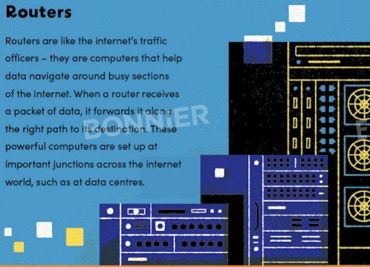
A data centre is a giant building that processes data for the internet. They're filled with powerful computers called servers that store the files, code and databases needed by websites and apps. Servers handle millions of requests from across the internet and send data to your device in a fraction of 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!

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.

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

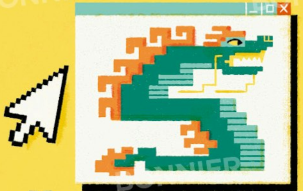
An Internet exchange point (IXP) is a location where different ISPs connect their networks to each other. By sharing traffic, data can take the shortest route across multiple networks. Companies that use the internet sometimes keep copies of popular data at an IXP so that it doesn't have to travel as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

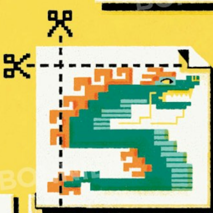
HOW DATA IS SENT ACROSS THE INTERNET

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:

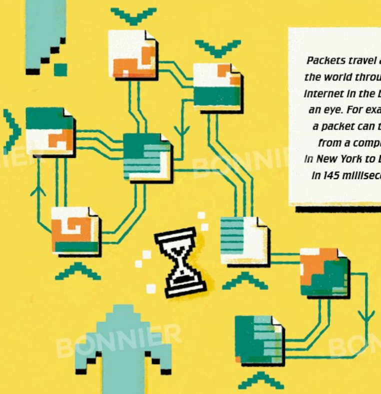




Step 1 First, the image is chopped into small packets, which are easier to transfer. A small 1 megabyte image file like this might be broken down into 700 packets.

Source IP Address
Destination IP Address
Data

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.

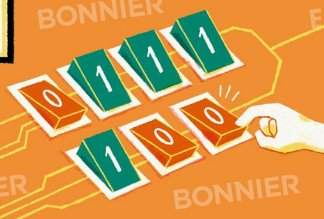
INTERNET UPDATE

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

PROGRAMMING LANGUAGES FOR THE WEB

If you want to really understand how the web works, you need to explore the computer code behind each page. When you peek, you'll see that web developers use a combination of programming languages to create amazing websites. Different languages are used for specific jobs, helping all the parts of a website work together smoothly.

Speaking the right language

Programming languages are divided into two types:

FRONT-END LANGUAGES are used to write the code that creates the parts of websites you see and interact with in your web browser. This includes the layout, design, buttons and menus.

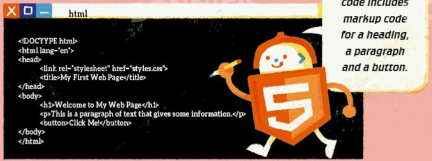
BACK-END LANGUAGES are used to write the code that runs behind the scenes on the server. They handle important tasks like data storage, user logins and processing orders.

HTML and CSS

Every web page uses two important front-end languages: **HTML** (HyperText Markup Language) and **CSS** (Cascading Style Sheets). They are known as markup languages as they set out (or mark up) instructions for how a web page should look.

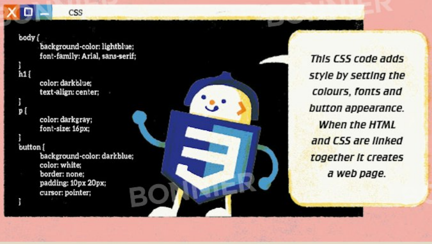
HTML is like the skeleton of a webpage – it's used to make the structure of the page and the things that go on it, including headings, images, paragraphs of text, and buttons.

CSS lists the instructions for how those different parts of the page should look, such as what fonts and colours should be used and where they should be used on the page.



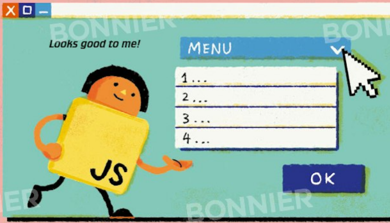
```
<!DOCTYPE html>
<html lang="en">
<head>
        <link rel="stylesheet" href="styles.css">
        <title>My First Web Page</title>
</head>
<body>
        <h1>Welcome to My Web Page</h1>
        <p>This is a paragraph of text that gives some information.</p>
        <button>Click Me!</button>
</body>
</html>
```

This HTML code includes markup code for a heading, a paragraph and a button.



```
body {
        background-color: lightblue;
        font-family: Arial, sans-serif;
}
h1 {
        color: darkblue;
        text-align: center;
}
p {
        color: darkgray;
        font-size: 16px;
}
button {
        background-color: darkblue;
        color: white;
        border: none;
        padding: 10px 20px;
        cursor: pointer;
}
```

This CSS code adds style by setting the colours, fonts and button appearance. When the HTML and CSS are linked together it creates a web page.

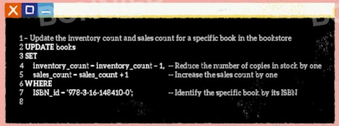


Making websites interactive

JavaScript is the most popular front-end programming language. It brings web pages to life by making them interactive (reacting to users' actions). It can check if a form is filled out correctly, create menus that open and close, and upload photos or videos to posts. Anytime you interact with a web page – whether you swipe, press a button or type something in – that's JavaScript at work!

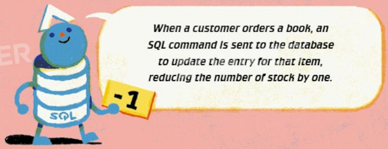
Connecting to databases

Databases on servers store information that websites need, like users' account details and lists of products. Web developers use a back-end language called SQL (Structured Query Language) to request information from the database or to add, remove or update entries.



```
– Update the inventory count and sales count for a specific book in the bookstore
UPDATE books
SET
    inventory_count = inventory_count – 1,  -- Reduce the number of copies in stock by one
    sales_count = sales_count +1            -- Increase the sales count by one
WHERE
    ISBN_id = '978-3-16-148410-0';          -- Identify the specific book by its ISBN

```



When a customer orders a book, an SQL command is sent to the database to update the entry for that item, reducing the number of stock by one.

Coding dynamic websites

PHP is another back-end programming language used on servers. Web developers love using PHP because it can automatically create web pages for them. Imagine an online bookshop with thousands of books to sell. Instead of making a separate webpage for each book, developers create a template page with spaces for the title, price and description. When a user clicks on a book, the PHP code runs alongside SQL commands to grab the correct details from the database, fill in the template and send the finished page back to the user.

ON ASSIGNMENT

CHECK OUT SOME FRONT-END CODE

Did you know you can peek behind any website to see its HTML and CSS code? Here's how to do it:

1. Open a website that you trust in your browser. Always browse safely and with an adult's permission.
2. Right-click on the page and select "Inspect" or "View Page Source" from the menu.
3. A panel will open, showing you the HTML and CSS code used to build that page!
4. Explore the code to see how different elements are styled and structured.

USER GENERATED CONTENT

It used to be the norm to get all our information and entertainment from big media companies. They were the ones with the tools needed to create books, newspapers, music and movies, and had the know-how to share it with huge audiences. But now, thanks to the internet, anyone with a phone or computer can create something and share it with the world! We call this user-generated content because it's made by the users of the internet.

Everyone can be a creator

In the early days, if you wanted to share something online, you had to know how to build a web page. Then new websites like GeoCities and Piczo made it easy for anyone to create web pages of their own. Social media sites like MySpace, Facebook and YouTube simplified uploading photos, music and videos, and suddenly everyone had the tools to create and share something on the web.

INTERNET ALERT!

WEB 2.0

When user-generated content started to take off, this was such a big change in the way people used the internet that people began calling it "Web 2.0".

INTERNET ALERT!

BEING A RESPONSIBLE CREATOR

Just because you can post something, doesn't always mean you should. What you say or do online can have real world consequences such as causing people harm, so it's important to think about how your posts might affect others.

We make the web

Nowadays, the biggest websites rely on us people making content! Many social media sites don't actually make their own content – they need us to upload ours. Social media sites would be totally empty without our posts. Even meme pages wouldn't exist without people creating and sharing funny content.

Helping people be heard

One benefit of user-generated content is that it gives a voice to people who usually might not be heard. Traditional media is hard to break into, but user-generated content doesn't have the same barriers. A poet could post themselves performing their latest work, or a teenager might vlog about life in their small town. A refugee can even tell their story, giving us a glimpse into worlds we don't otherwise see.

Breaking the news

User-generated content also has a role to play in our news cycle: social media sites buzz with the latest news as soon as it happens. When there's a big event, users post photos and updates straight to social media for others to read and share. Sometimes they even break stories too! Being able to post instantly means important stories can reach people around the world long before traditional news outlets.

Can you rely on it?

Anyone can post anything online, which means there's a wide range in the quality and accuracy of what you'll see. Some user-generated content is well made and researched, but other content might be full of misinformation or be completely fake. Before you take something as fact, check the sources (where the information came from), see if it's backed up by evidence and consider whether the creator might have a bias or agenda for posting it.

Who made this!?

Do you find it annoying when people copy you? I bet you do, and copying is a problem online too. Content creators need to respect copyright laws, which are laws which say you can't use someone else's work without permission.

Sometimes well-known companies get caught red-handed stealing ideas too. There have been cases where companies have seen a a design for a t-shirt or a piece of jewellery and copied it without asking. They then sell these items, making money off someone else's hard work. How would you feel if someone else became rich or famous from your idea?

HOW CREATORS MAKE MONEY

We've seen how businesses have been able to use the internet to make money, but what about creators? No matter whether they are blogging, creating video content or producing podcasts, plenty of people are building huge audiences online who love what they do and make. But how do they turn a fun hobby into something that actually pays the bills? The good news is, there are lots of ways for creators to make a profit from their passion!

Time for an advert break

Often before YouTube videos and during podcast breaks, there will be an advertisement to watch or listen to. Online tools like Google's AdSense match adverts with creators' audiences. For instance, an ad for a new phone might be interesting to viewers of a YouTuber that reviews tech. Creators get paid to let these adverts run before or during their content, but they don't always get to choose which ones show up. A typical YouTuber might earn around 30p for every 1,000 views of an advert, though this can vary.

Collaborations and sponsorships

Think about the people you follow online. You love what they create, and you trust their opinions. So if they recommend something, you'd probably check it out, right? When a company spots a popular gaming streamer, they might partner with them to promote their products. They know that if the gamer is seen using their headset, their followers are more likely to want one too. The company might pay the gamer to show the product in action. This is called a sponsored post.

Being honest about ads

If a creator is being paid to promote a product, they should be upfront about it. In some countries it's the law. It helps prevent people from being misled by hidden adverts. Creators should clearly label any content that they're being paid to make, like sponsored posts, giveaways or free products they've been sent to review so you can decide if it's something you're truly interested in.

INTERNET ALERT!

AFFILIATE LINKS

Creators use special links to direct their audiences to products. When followers click on them and make a purchase, the creator earns a small percentage of the sale.

Nano influencers

You don't need millions of followers to make money on the internet. **Nano influencers** are creators with fewer than 10,000 followers. Their content is aimed at a small group of people who really care about a certain niche. They often partner with really specific companies who make products aimed at a small number of people.

Selling directly to fans

Creators don't always partner with other companies to make money – they can sell merchandise like hoodies, mugs and stickers, or even custom art pieces or music. Superfans are willing to pay a lot to have something created just for them. Some creators offer subscriptions, where fans pay monthly for behind-the-scenes videos or early access to new content. Platforms like Patreon are perfect for musicians, vloggers and artists, while Substack is popular for writers and authors.

ON ASSIGNMENT

IT'S YOUR TURN TO BE THE INFLUENCER

If you were a creator, what would you want to share with the world? Follow the steps below and plan out what your online career might look like.

1. Pick your message
What do you love doing or talking about? Maybe you'd teach people how to bake, review your favourite games or raise awareness about protecting the planet.

2. Choose your platform
How would you share your message? Would you write a blog, film videos or create a podcast? Think about what would work best with your personality – are you in front of the camera or behind it? Are you a writer or a talker?

3. Plan your first post
Write down your ideas and think about what will make your message stand out and get people to pay attention! A catchy heading or title, or a special video effect could do the trick.

WHO MAKES THE INTERNET?

Millions of people are behind the websites, apps and services we use on the internet everyday. Some people work for themselves, while others will work for tech companies, which can be both big and small. Nowadays, nearly every company needs a technology team – from high street shops selling goods online, to restaurants taking reservations and banks managing people's accounts. There are companies that exist only online too. Behind it all are talented technical professionals with a range of important jobs.

Check out PhaserFlix, a made-up video streaming company that has a library of science fiction films and TV shows. Customers pay to watch videos on their website, mobile app or on a smart TV. These are the jobs that make it happen:

SOFTWARE ENGINEERS build the app and website. They write the code that underpins the entire service.

FRONT-END ENGINEERS create the code for the parts of a website or app that you see and interact with. For a video streaming app, that's the video player and the features that let you browse or search the library. They write code with front-end programming languages and make use of tools called frameworks, like React and Angular, to build web apps.

Part of a front-end engineer's job is to make sure web pages load quickly, even when using older computers or a slow connection. This is called performance optimisation. A way to do this is to have images download just before someone scrolls to that part of the webpage, rather than having them all download at once.

BACK-END ENGINEERS develop and maintain the code for the areas of an app or website you don't see. At PhaserFlix, this includes managing databases of videos, making sure the videos load quickly and that the servers can handle millions of people watching a series at the same time.

Managing servers is a crucial job for back-end engineers. If millions of PhaserFlix customers want to stream a new movie, the back-end engineers will "spin up" extra servers to cope with the increased demand. This is called scaling. When servers are dealing with lots of requests at the same time, developers use a technique called load balancing, where they redirect requests to less busy servers.

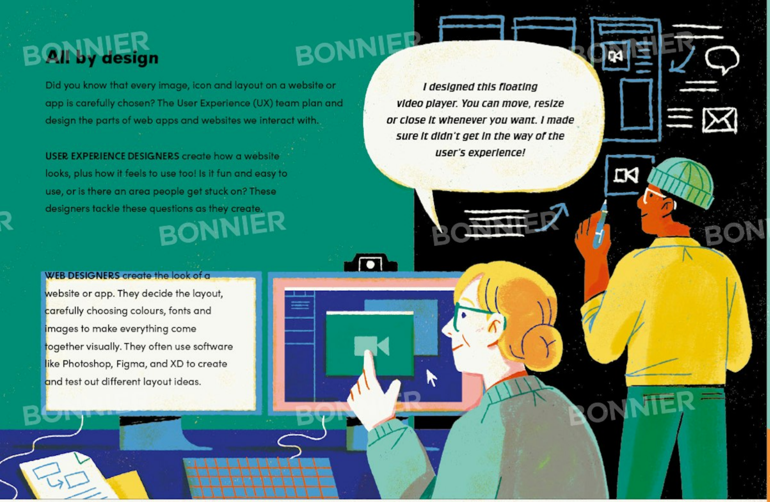
MACHINE LEARNING ENGINEERS create a tool used by many websites today: the recommendation engine. This is a system that predicts what customers might want to see. On PhaserFlix, the recommendation engine suggests the best sci-fi film to watch, while on other sites it might recommend a new song to add to your playlist. Recommendation engines use data from customers' viewing history to predict what they might enjoy. This is a really important system for lots of online businesses, because the better the recommendation engine is at making suggestions, the more likely someone is to keep using a website.

All by design

Did you know that every image, icon and layout on a website or app is carefully chosen? The User Experience (UX) team plan and design the parts of web apps and websites we interact with.

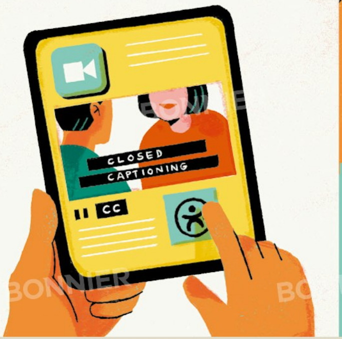
USER EXPERIENCE DESIGNERS create how a website looks, plus how it feels to use too! Is it fun and easy to use, or is there an area people get stuck on? These designers tackle these questions as they create.

WEB DESIGNERS create the look of a website or app. They decide the layout, carefully choosing colours, fonts and images to make everything come together visually. They often use software like Photoshop, Figma, and XD to create and test out different layout ideas.


I designed this floating video player. You can move, resize or close it whenever you want. I made sure it didn't get in the way of the user's experience!

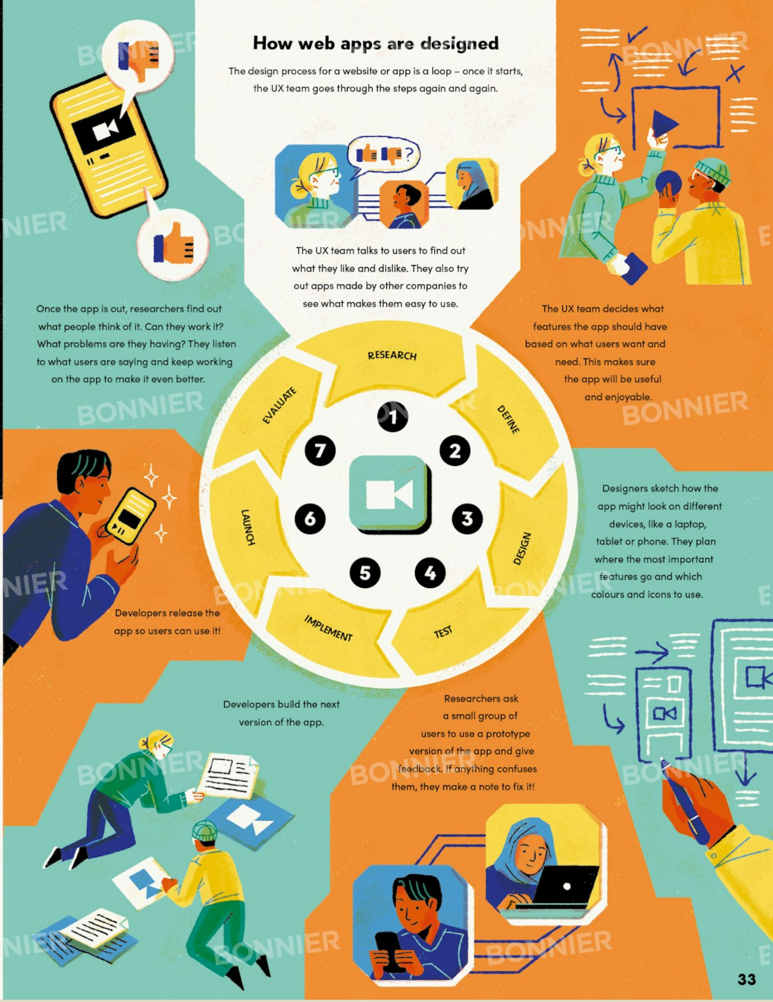
USER EXPERIENCE RESEARCHERS find ways to make websites easier to use. By watching how users navigate their site, they identify problems and pass them along to the design team who make improvements. A UX researcher might create two versions of a webpage that asks users to make a new account. They'll measure how long it takes people to fill out each form to see which version was quicker and easier to complete. This technique is called A/B testing.

ACCESSIBILITY SPECIALISTS make sure websites and apps can be used by everyone, including people with disabilities. They create features which remove barriers that hinder some users' experiences, for example closed captions for people who are deaf or hard of hearing and audio descriptions for people with low vision.



How web apps are designed

The design process for a website or app is a loop – once it starts, the UX team goes through the steps again and again.



The UX team talks to users to find out what they like and dislike. They also try out apps made by other companies to see what makes them easy to use.

The UX team decides what features the app should have based on what users want and need. This makes sure the app will be useful and enjoyable.

Designers sketch how the app might look on different devices, like a laptop, tablet or phone. They plan where the most important features go and which colours and icons to use.

Researchers ask a small group of users to use a prototype version of the app and give feedback. If anything confuses them, they make a note to fix it!

Developers build the next version of the app.

Developers release the app so users can use it!

Once the app is out, researchers find out what people think of it. Can they work it? What problems are they having? They listen to what users are saying and keep working on the app to make it even better.

OPEN SOURCE TECHNOLOGY

Behind every web app and website is something called source code. This is the collection of computer code that controls the app or site. On the internet, one way to classify apps and websites is whether people can access the source code or not. Closed source means the code is private and details about how it works are hidden. This can be to prevent other people from copying it or trying to break it. Open source means the code has been shared for anyone to look at, mess around with or turn into something new.

Sharing is caring

What's so special about open source? Well plainly, by sharing code for free can speed up new tech breakthroughs. Anyone and everyone – from solo coders to giant companies – can jump in and help at any time to make the internet even better. Being able to freely remix and reuse other people's code and discover new ways to make it work is the reason internet technology improves so rapidly.

WHY DO YOU VOLUNTEER ON OPEN SOURCE PROJECTS?

As a coder and digital artist, I've used the open source app Blender to design 3D models for a long time! I joined Blender's open source community to get involved with others like me. We share ideas, troubleshoot bugs together and invent new tools that help other 3D artists – and me, too. I've learned so much that I don't mind not being paid, and without a free tool like Blender, I would have never started designing. It feels good to give something back.

The problem with open source

Working on an open source project takes a lot of time and effort. While it can feel rewarding to make a better internet for everyone, some people benefit more than others. Big tech companies like Google, Amazon and Meta can include open source code as part of the products they sell without having to pay the people who work on it. In turn, they end up making money off passionate people working for free.

Open source projects also face a risk of abandonment. Volunteers can stop contributing at any point, either because they lose interest in the project or become too busy in other parts of their lives. Is it smart for tech companies to rely so heavily on volunteers to maintain some of the internet's most critical apps? To keep these important projects going, we may need to find better ways to support open source contributors, including encouraging companies to pay them for their work.

The open source community

Some of the most important tools we use on the internet are open source projects...

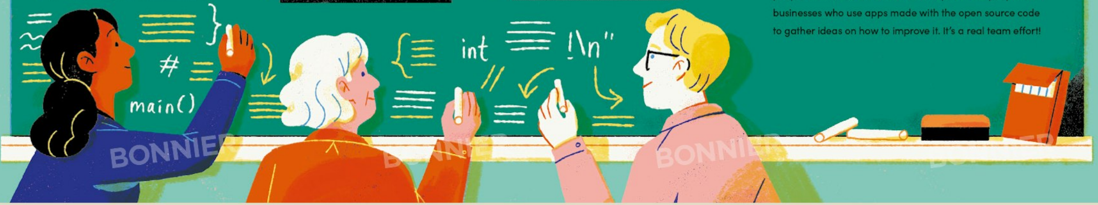
Tens of millions of web servers use an open source software called Apache to host and manage websites.

The Firefox web browser is used by millions for its speed and privacy features.

Nearly half of all websites in the world are built using an open source app called WordPress.

... and many people all over the world volunteer their time and skills to work on them. These people are called open source contributors. Some are software engineers who use open source code to build their own apps. They study how the code works, add their own features, then share the updated code so everyone can benefit from it.

But not every open source contributor is a coding genius. Some focus on writing documentation – instructions for how people should use the code. Others speak with people and businesses who use apps made with the open source code to gather ideas on how to improve it. It's a real team effort!

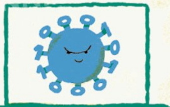


CYBER CRIME ON THE INTERNET

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 sometimes 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.

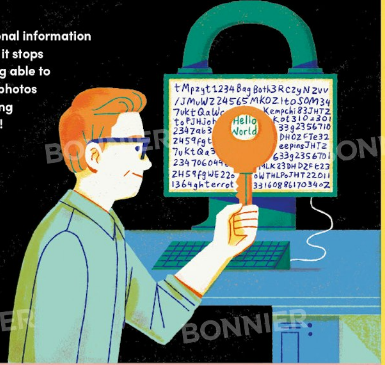
☑ **1. USE STRONG PASSWORDS FOR ALL YOUR ACCOUNTS**
Make them long and use random words so they are hard to guess.

☑ **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.

ENCRYPTION

Tech companies have another technique to keep our personal information safe and secure on the internet. It's called encryption, and it stops cyber criminals (or anyone else for that matter!) from being able to see things like your private chats with friends, your family photos or sensitive information like your medical records or banking details. It's so clever, it makes this information unreadable!

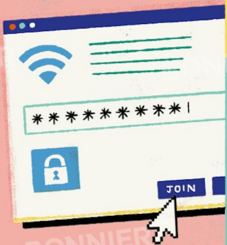


How encryption works

Encryption software scrambles files so that no one else can view or change them. It works by using a mathematical function that changes the file's data into a mixed-up form. Then the data is locked by something called an encryption key. This key can be created with a password, passcode or biometric data like a fingerprint or face scan. Encryption is powerful because once a file is encrypted, it's basically impossible to access without the key.

Where encryption is used

Encryption is used all over the internet to keep many kinds of information safe.



PRIVATE CONVERSATIONS

Encryption is used on messaging and video calling platforms to create a secure communication channel, stopping people from snooping on you when you're messaging your mates or video calling your grandparents

PROTECTING YOUR PERSONAL FILES

When you store files online in places like iCloud, Google Drive and other storage servers, encryption is used to protect your files from unauthorised people trying to access them.

KEEPING YOUR WEB BROWSING SAFE

Web browsers encrypt the data that is passed between your computer and the website you're on. When you log into a website or buy something online, encryption protects your password and payment information while it's being sent. When you see 'https' in the address bar of your web browser, encryption is being used to create a secure connection.

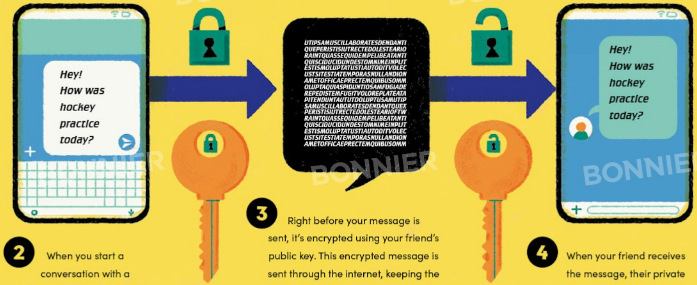
WIRELESS NETWORKS

Do you use a password to connect to your WiFi at home? If so, your WiFi network uses encryption too. It protects the data being sent and received from all the devices connected to it.

Sending messages securely

You might wonder, if your messages get scrambled, how can someone on the receiving end read them? Lots of messenger apps use a technique called End-to-end encryption, meaning messages are encrypted and decrypted on each side of the conversation.

1 The messenger app creates two encryption keys – a public key, and a private key. Anything that is encrypted using your public key can only be decrypted using your private key. Your private key is never shared with anyone.


Hey!
How was hockey practice today?
Hey!
How was hockey practice today?

2 When you start a conversation with a friend, you both exchange your public keys.

3 Right before your message is sent, it's encrypted using your friend's public key. This encrypted message is sent through the internet, keeping the contents private. Even the makers of the messenger app won't be able to read it.

4 When your friend receives the message, their private key is used to decrypt it. Now they can see the message.

Breaking encryption

Unless you have the correct key, it's extremely difficult to decrypt a file. Someone might try a "brute force attack", where a computer program tries to guess every possible key. But even super-fast computers can take thousands of years to guess the right key.

When is something *too* secret?

Most of the time, encryption is used to protect our information, but there is a downside to this powerful technology. Criminals also use encrypted communications to hide what they are doing. Nonetheless, most people think this technology is still essential to protect regular citizen's private information.

PROTECTING YOUR PERSONAL DATA

To make the most of the internet, sometimes we need to share information about ourselves. When you buy something online, you need to tell the company your name and address so they know where to send the package. Often we need to share even more sensitive information – like our full names, date of birth or banking information. We rely on companies to protect that data, and they have specialist teams who keep it safe. Yet, it's crucial to understand the risks involved and as a responsible digital citizen, there's lots to be aware of when sharing personal data online.

Data breaches

When someone gets access to data they don't have permission to see, it is called a data breach. Most data breaches happen by mistake, such as an employee losing a USB drive with customer information or accidentally giving the wrong people access to private data. Other times, they happen on purpose, like when a cyber criminal wrongfully tries to access certain data.

Companies have a responsibility to protect our personal data. There are different laws around the world that set out the rules on how our data should be handled and stored. Companies can be fined or even put on trial if a data breach happens. If your personal information has been involved in a data breach, the company should tell you and explain what you need to do next.

Mega meta-data

Photos uploaded to the internet contain information about what time the photo was taken, the type of camera used and even the exact coordinates of where it was taken! This is called meta-data. Most social media sites remove this sensitive data before an image is posted, but if you send a photo through a messenger app or email, the meta-data could still be there. Anyone who had that photo could extract the meta-data and find out where it was taken and when. This is another reason it's important to be mindful of who you share your photos with.

INTERNET UPDATE

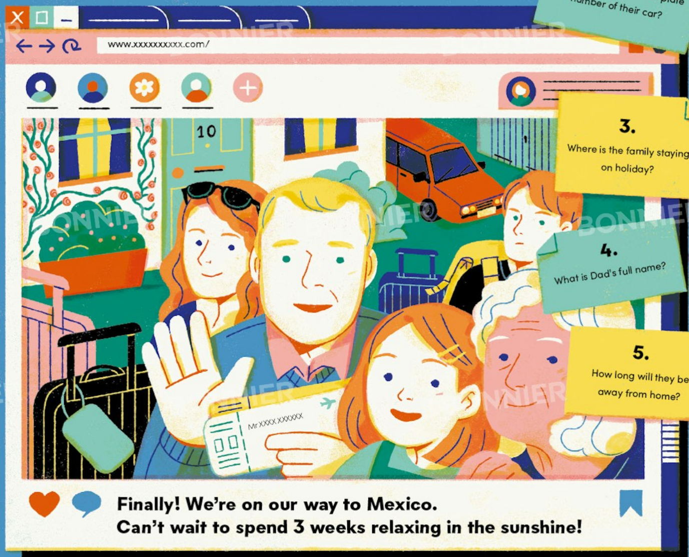
THE RIGHT TO BE FORGOTTEN

You can email any company to ask them what information they hold about you and request they delete it – but some don't make it easy! Internet activists are campaigning to give people "the right to be forgotten". They want to make it easier for information about us to be deleted if it's wrong, out of date or just not relevant.

ON ASSIGNMENT

EVERY PHOTO TELLS A STORY

Sometimes we share our personal data by choice. People film vlogs, take photos and share what they are up to on social media. But oversharing your life can risk your safety. Look closely at this social media post. How might Jennifer be accidentally revealing personal information about her family? What are the risks of sharing this photo?



Finally! We're on our way to Mexico.
Can't wait to spend 3 weeks relaxing in the sunshine!

1. Can you spot the house number?

2. What's the registration plate number of their car?

3. Where is the family staying on holiday?

4. What is Dad's full name?

5. How long will they be away from home?

Doxxing

Doxxing is when a person deliberately posts someone else's personal information on the internet. It could be their phone number, or details about where they live or go to school. You should never do this. It's cruel and distressing for the person involved and can put someone in danger. Even with your friends, remember to respect people's privacy and not share personal information about others.

INTERNET UPDATE

GAMERTAGS

Never use your real name when playing games online. Instead, be like the pro gamers and call yourself by your "gamertag". That way you can show off your personality or interests without sharing private information.

HOW OPEN IS THE INTERNET?

When we say something is neutral, that means it doesn't pick a side. It's fair and treats everyone the same. Net neutrality is all about letting all people have the freedom to access internet data equally, rather than letting tech companies and internet service providers have control over who can access it, how and when.

Being fair to everyone

Supporters of net neutrality think that ISPs should treat all legal internet activity the same. They shouldn't give special treatment to certain websites, block people from areas of the internet or allow people faster and better access because they are willing to pay more.

But critics think the net neutrality rules are too strict. People use the internet for different reasons – you might be watching YouTube while somewhere else, the internet is being used to share news of a natural disaster. Are these things as important as each other, or do some things need special attention?

Rules for a fairer internet

To make things more complicated when it comes to governing the internet, there isn't one rule that applies around the world. Each country has its own laws that say how ISPs should handle net neutrality. Here are some of the most common rules:

RULE 1: NO THROTTLING

If you love streaming or playing online games, you know a fast internet connection is important. But these things cause a lot of data traffic – much more than just browsing the web. Because of this, an ISP might want to slow down your internet speed – this is called throttling. By slowing your connection, you might pay more for your speeds to not be limited. Net neutrality rules say all traffic should be treated equally.

RULE 2: NO BLOCKING

Net neutrality says you should have the freedom to visit any website or online service without your ISP stopping you. Of course, sometimes an ISP needs to block a website, for example, if it's illegal, but they can't block you from somewhere they'd rather you didn't visit, like a rival company's website.

RULE 3: NO TRICKY BUSINESS DEALS

Imagine you're about to buy a new pair of trainers, when suddenly, as you click the buy button, you're taken to a totally different shop. Why? Because that shop has a deal with your ISP and gives them money for every sale. Net neutrality rules say you should be able to choose where you shop without your ISP trying to make money from it.

What do you think?

There's an ongoing debate around net neutrality. Have a look at different people's opinions and see where you stand.

Net neutrality is crucial to my small business. It means my website has the same chance of reaching customers as bigger businesses.

Mike
ONLINE PET FOOD SHOP OWNER

I have mixed feelings about net neutrality. Streaming takes up a lot of bandwidth. It's responsible for more than half of the internet's traffic worldwide, so some customers end up paying more to support heavy streamers. It feels a little unfair.

Lisa
INTERNET SERVICE PROVIDER EMPLOYEE

Net neutrality helps me spread the message about climate change. ISPs can't make it harder for activists to share important news by slowing their websites or making them pay extra.

Sophie
CLIMATE ADVOCATE

If we paid a little more based on what we actually do online, ISPs could use that extra cash to invest in research and improving the infrastructure. That could mean faster speeds and more reliable internet for everyone.

Ajay
TELECOMS NETWORK ENGINEER

Net neutrality is a must for gamers. No one wants to lose a game just because their connection is being slowed down on purpose!

Alex
A PROFESSIONAL ESPORTS GAMER