future » engineer

CTRL + ALT + PROTECT

The Adventures of Suraksha Nagar

A guide to safely navigating the Internet

Contents

This handbook will help you explore the digital world safely while having fun online. Through stories of 7 friends, you'll learn about scams, privacy, misinformation, and responsible internet use.

In the cheerful town of Suraksha Nagar lived seven best friends–Meera, Rahim, Jaspreet, Susan, Shubham, Siddharth, and Noor.

Meera -The Adventurer

Rahim - The Protector

Susan - The Privacy Champion

Shubham - The News Navigator

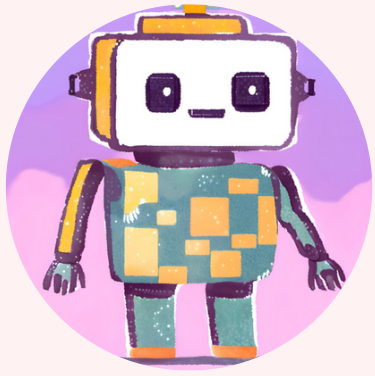
Siddharth - The Helper

Jaspreet - The Detective

Noor - The Changemaker

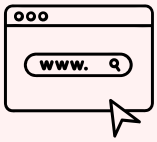
Amit Bhaiya

Glitch



It was a sunny afternoon in Suraksha Nagar, and the cozy living room at Meera's house was alive with noise and laughter. The seven friends –Meera, Rahim, Jaspreet, Susan, Shubham, Siddharth, and Noor–had piled onto the sofas and floor, snacks scattered around them, as they fired up the old laptop.

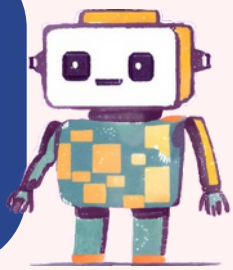
"Let's try this!" Meera said eagerly, her fingers already clicking through different sites and games. "Wait, don't rush! You might click on something weird," warned Rahim, leaning forward with a furrowed brow. "Rahim, don't worry so much–it's fine," teased Shubham, her phone buzzing with notifications as she showed the group a hilarious meme.



"Did you check if that site is safe?" Jaspreet asked, their detective instincts kicking in, as they glanced at the screen. "Also, remember not to share anything personal," Susan added, her tone calm but firm, while scrolling through a new privacy guide she'd bookmarked earlier. Siddharth chuckled. "Okay, everyone, let's breathe! We're just exploring–no need to panic," he said, his easygoing voice helping everyone relax. Noor, meanwhile, was jotting down ideas in her notebook. "What if we started a project about the coolest, safest ways to use the internet? We could even share it with the school!" she suggested, her eyes shining with excitement.

As they navigated through games, videos, and strange pop-ups, the room filled with debates, laughter, and the occasional, "Oops, I didn't mean to click that!" It wasn't just about the internet–it was about doing it together, learning from each other, and making sure their online adventures were safe and fun.

With Amit Bhaiya and Glitch by their side, the friends are about to embark on an exciting journey through the digital world..



They'll learn how to navigate safely, spot hidden risks and unlock incredible possibilties that the internet offers. Every click will bring something new to explore.

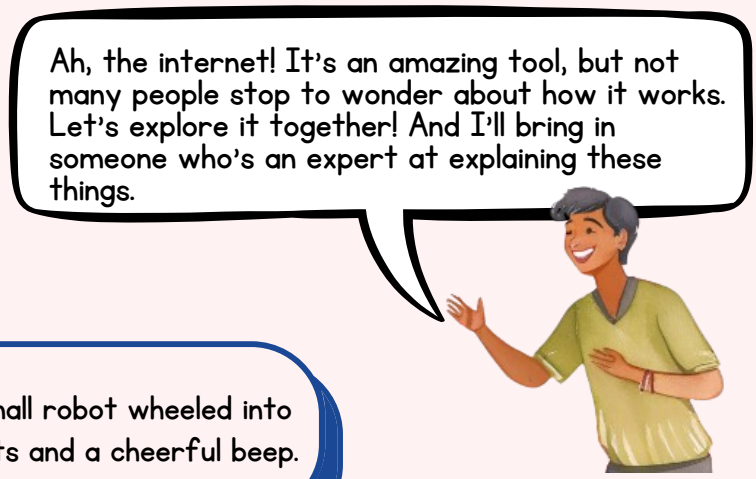
But the journey won't always be smooth. The paths will be filled with surprises and a few obstacles. Yet, with Amit Bhaiya's guidance and Glitch's clever tricks, the children will tackle each challenge with confidence. Will they be ready for the adventure ahead?

Chapter 1: Hello Digital World!

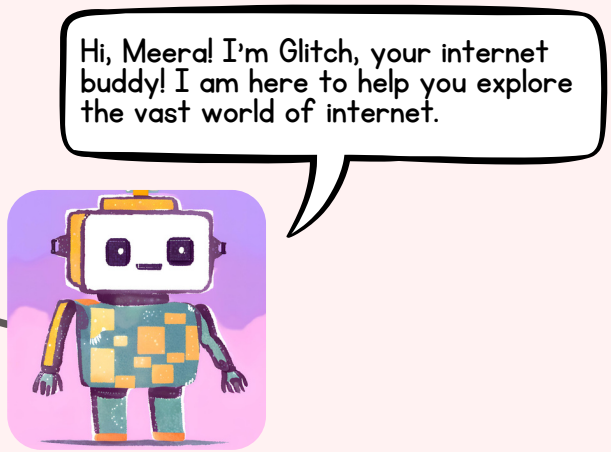
Meera is sitting with her mother's phone near the window. It is glowing with a dozen open tabs. She has recently started exploring the vast world of the internet–watching funny videos, discovering new songs, and searching for the answers to her endless questions. She loves it, but today, she is puzzled.

"How does the internet know so much about everything? and how is everything connected?" thought Meera.

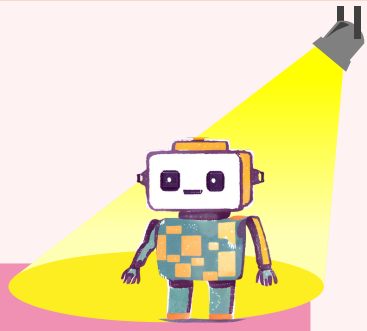
Thankfully, Amit Bhaiya, was around. "Bhaiya!" she called, and soon enough, Amit Bhaiya walked in with his usual calm smile.



With a quick tap on his phone, a small robot wheeled into the room. It had bright blinking lights and a cheerful beep.



WHAT IS THE INTERNET?

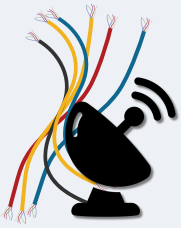


Let's begin with the basics, the internet is like a massive interconnected web that connects billions of computers, phones, and devices around the world. These connections allow devices to exchange information, making it possible for you to browse, watch videos, play games, and even shop online.

The internet is like our railway system, but instead of carrying people and goods, it carries information instantly across the world

Each website has its own address, just like each railway station has its unique name! The only difference is that while trains take hours and days to carry people and goods from one place to another, the internet takes only seconds to carry information.

The Backbone



The internet relies on huge underground cables, satellites, and wireless networks to connect devices globally.

Servers

This is a server, which stores the information you see online. Servers are like giant libraries with millions of websites, videos, and apps.

Your Browser

When you type a question into your browser, your device sends a request to a server. The server finds the answer and sends it back to you in seconds!

HOW DOES THE INTERNET HELP US?

The internet has revolutionized the way we live and learn. Let me show you how it helps us in our everyday lives.

Learning and Education

The internet is your teacher and library in one! Access learning platforms, watch videos in any language, and join virtual classrooms to explore topics you love–all with a click.

Communication

Connect instantly! Whether through emails, social media, messaging apps, or video calls, the internet makes communication fast, easy, and seamless.

Entertainment

The internet is your go-to for fun– watch movies, live cricket matches, play games, or learn new skills like dancing, all from the comfort of home.

Creativity and Sharing

Share your creativity with the world! Write stories, create music, or showcase artwork online, just like many talented young artists do everyday.

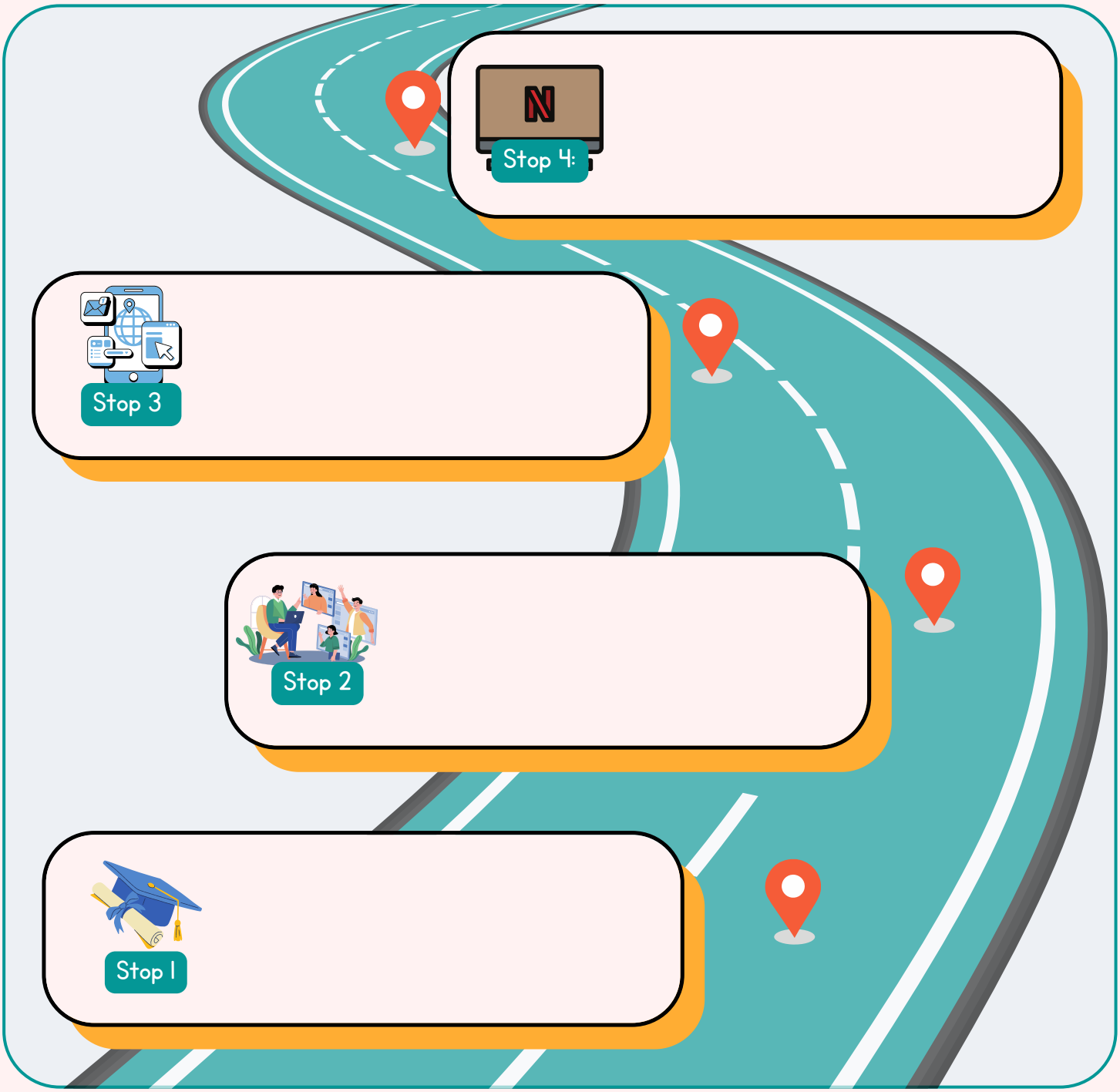
Bhaiya, I started using internet for online classes, and now I love watching funny videos and playing games online to relax after studying as well! But I didn't realise I could learn dancing or music online!

That's great! You're not alone: 88% of young Indians like you watch videos online. Many more use the internet for gaming, searching information and calling friends! So many young people are discovering new things online– isn't that cool?!

Activity

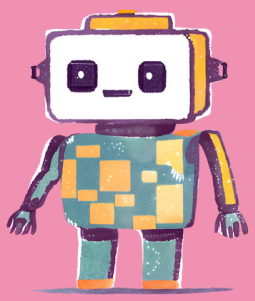
With a new understanding of the internet, Meera felt ready to explore its endless possibilities. If you have ever been on the internet, help her find new things to do by sharing your online adventures. Start from the bottom, and :

- at Stop 1, think about something new you've learned online.
- at Stop 2, share something creative you've made or shared.
- stop 3 is for staying connected–who do you keep in touch with online?
- finally, Stop 4 is all about fun–what's your favorite online activity?



The internet isn't just about the present. It's constantly evolving, and you're a part of its future.

In India, we're already seeing big changes. You or your parents probably use UPI or Unified Payments Interface for payments! UPI allows us to digitally send and receive money, revolutionizing the way we transact. Many new services are available online too-for example, doctors are treating patients through video calls, and students are attending classes from home.



Artificial Intelligence or AI is making the internet smarter, AI allows machines to think and learn like humans. AI tools can answer people's questions, personalize education to suit an individual, make games more challenging, and help humans identify problems- based on the data that has been used to train the AI.

Now there is Virtual Reality or VR in existence, a technology that creates an environment and allows humans to interact with that environment using headsets. Imagine walking through a rainforest, visiting the Taj Mahal, or even exploring space -all while sitting in your room!

Thank you, Bhaiya and Glitch! I never knew the internet was so amazing-and so powerful. I can't wait to explore all these possibilities!

I am excited for you too! But as the internet evolves, you may come across all kinds of experiences-positive and negative-and I want you to be prepared.

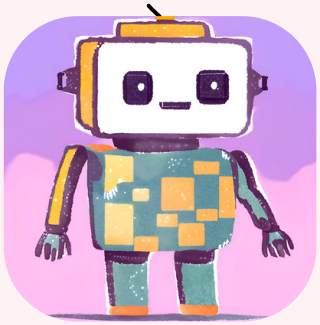
Activity

Meera sat quietly in her room, thinking about what he said. Even though she loved the internet, Amit Bhaiya was right: it is important to be prepared. She started thinking about all the times when the internet has not felt like a nice place to be, and making a list. Have you had any experiences similar to Meera?

I don't like the internet when...

- People share incorrect information to scare others.
- Others try to force me to do something.
- Someone lies or talks rudely to me online.
- Too many notifications make me feel overwhelmed!
- I get unwanted messages or see videos I don't like.
- I feel unsafe because someone is trying to cheat me to get money!

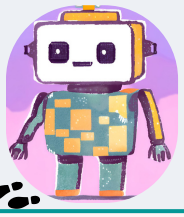
Make your own list here:



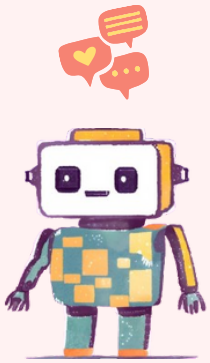
Reflecting on challenging online experiences can be tough but also helpful. Can you explore what happened when you felt this way? Remember, you're not alone – negative emotions like distress, anger, or sadness are normal, both online and offline. Let's work together to identify unsafe situations and learn how to care for yourself online.

The first step towards safe internet use is understanding the internet really well, and staying updated about new developments. Here are a few important things you need to keep in mind online.

First up – your digital footprint. Your digital footprint is like the trail you leave behind whenever you go online. Whether it's a post you share, a picture you upload, or even a search you make, it all adds to your digital identity.



Wait! Does that mean even my search history is part of my digital footprint? What if I use incognito mode? Surely no one can track my digital footprint then!



Every click, like, and share contributes to your online presence. Imagine you're wearing a disguise while walking through your neighborhood. While your friends might not recognize you, people like security guards, shopkeepers, or cameras can still see where you're going and what you're doing. Incognito mode on your browser works a bit like that disguise. It hides some things, like the websites you visit from people who share your computer or phone. But it doesn't make you invisible to everyone. Want to know who can still track your footprints?

Service Provider

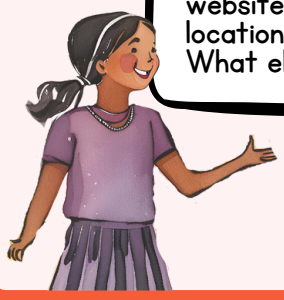
Your Wi-Fi or internet provider (the company that gives you internet) can still track which websites you visit. Think of it like the shopkeeper still knowing you entered their store, even if they can't see your disguise.

Websites

Many websites use tools called cookies or trackers to remember things about you. While incognito mode deletes these after you close the browser, the website can still know you visited if you log in or they recognize your device.

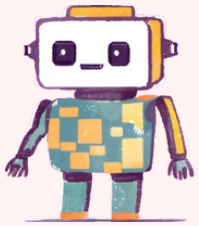
School Wifi

Many a times on school Wi-Fi, they have tools to monitor internet use, even in incognito mode.

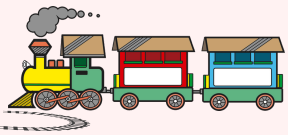


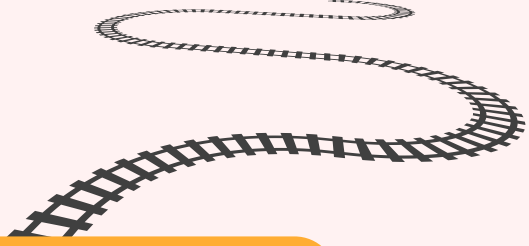
Wow, I didn't realize that everything I do is being recorded somewhere. I've also noticed that all websites ask for my name or phone number or location or e-mail ID before letting me use them! What else do I need to remember?

Two steps ahead of you! Let us understand something fascinating–and a little bit sneaky–about the internet. Have you ever noticed how advertisements pop up for something you searched for, or how your social media feeds always show the videos you like? That's because of algorithms and cookies!

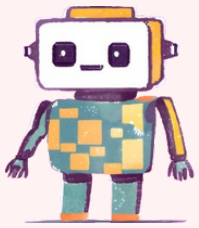


My cousin once searched for shampoos, and the next time she went online, she kept seeing shampoo links. We thought it was just a coincidence! How do algorithms work?





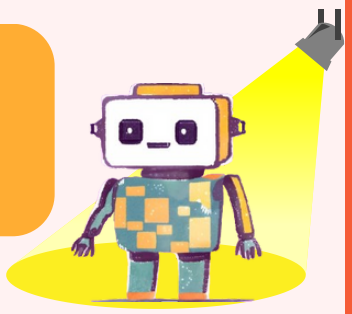
It is a bit like a railway system. Imagine every website you visit is a station, and every action you take like liking a post, searching for something, or adding an item to your cart–is a train leaving that station. Algorithms are like train conductors. They watch where your trains are going and try to predict your next stop based on your previous journeys. If you visit a lot of stations about video games, the algorithm might send you ads or suggest content about gaming, assuming you'll be interested.



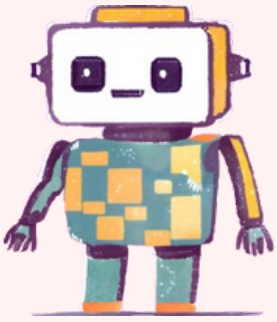
Cookies, on the other hand, are like station tickets that stay on your device so the website knows you've visited before. You can delete them, and throw away the ticket. Remember, every journey leaves a trace!

What if I use a nickname?

That's a great question! Let's talk about anonymity. On the internet, people may not always reveal their real identity.

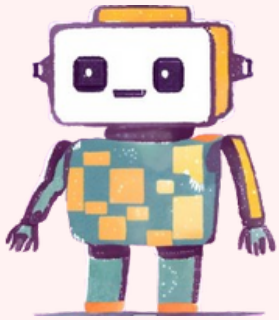


Sometimes, people use usernames and pictures other than their own, to have fun, feel safe or explore their personality. That's alright, but anonymity is limited: someone's online activity can still be traced back to them in some way, because of... you guessed it... your digital footprint! And remember, people might also hide their identity or lie about themselves to harm others. Not everyone is who they say they are.



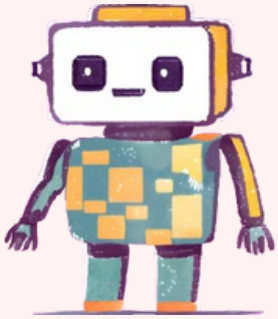
I usually talk to friends I know and trust online! That too using my mother's account.

Ah! Then you should know a few things about different online spaces. Your group chat, for example, is a private space. You are leaving a footprint, but it is not visible to those outside the group. There are other places online where your posts may be visible to everyone-like a tweet from a public account! Always be aware about who can see your messages, posts and likes. Later, we will learn how to change this too!

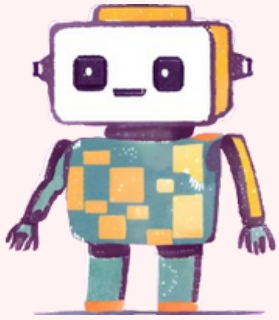


Thanks Glitch! I've learned so much today, but it's making me a bit worried.

In our online and offline lives, we may face both positive and unsafe experiences. By learning about the internet and sharing with friends or trusted adults, you can make smart choices and enjoy its benefits. This is just the beginning!
As you learn more, you'll feel more powerful.

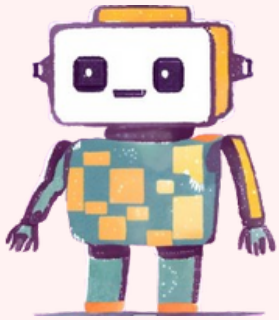


Until then, can you share three wishes about the internet? Let's see if we can make them come true!



Haha okay! I wish to learn more about technology online. I wish the internet would be a safe place for everyone... and I wish... I wish I can keep trying new apps!

Psst, what are your wishes for the internet? Tell me!

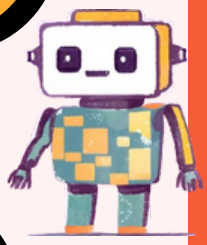


Activity

DID YOU KNOW?

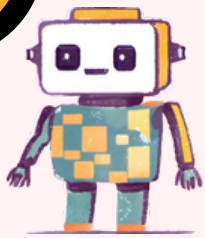
I see so many websites today. I wonder when was the first website created?

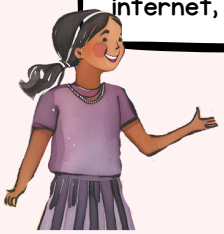
The First Website Was Made in 1989. It was called "info.cern.ch". Imagine trying to use the internet in 1989–it looked very different from the colourful, interactive websites we visit today. Can you guess the name of the scientist who created first website?!



And would you know how many websites are functioning today?

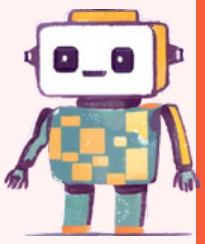
The internet is like a gigantic library with endless books to explore. There Are Over 1.1 Billion Websites! and that number grows every day! But don't worry–most of those websites are like digital museums with valuable knowledge and entertainment.





If so much data is stored on the internet, it must weigh tons, right?

This sounds unbelievable, but the entire internet actually weighs about 60 grams. That's roughly the weight of a strawberry! Can you guess, why? The information has mass, even though we can't see it!



RECAP: HELLO DIGITAL WORLD!

- The internet is like a giant web connecting devices worldwide, allowing us to communicate, learn, and explore.
- Online platforms track your activity through cookies and cache, which can reveal personal habits and information.
- Every action online leaves a digital footprint, always be mindful of what you share.
- Always be cautious with personal data. Information you share can be accessed and stored.

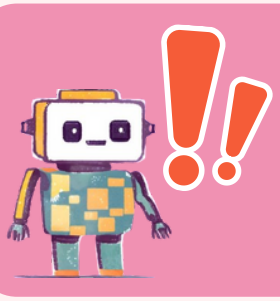
Chapter 2: Scams, Hacks & Cyber Attacks: Stay One Step Ahead!

It's Meera's birthday! Her house is filled with laughter and the aroma of delicious food. Her mother has invited Rahim and his family for dinner. As Rahim's family arrives, the adults settle into the drawing room, exchanging stories and catching up. Meanwhile, Meera excitedly pulls Rahim to her room, clutching her brand-new phone.

Look, Rahim! My parents finally got me my own phone! I can download all the games and apps I've been wanting to use now!

That's awesome, Meera! Before you start downloading, you will need to create an email ID and password first. Let's do that!

Meera quickly types iammeera@gmail.com as her email ID and sets her password to IAMMEERA with a proud grin. Glitch suddenly appears to warn her!



Email ID : iammeera@gmail.com

Password : IAMMEERA

Weak password detected! Security compromised!

Why is this password a problem? It's easy to remember. My mother's phone always had long, complex passwords that were hard to remember, and I had to ask for help every time

Easy to remember but also easy for someone else to guessEasy passwords are risky no? Think about it: if someone knows you and wants to break into your account, they will first try your name or favorite phrase to log in! If a password is a little complex and unique, it'll be like solving a tough puzzle–neither humans nor machines can figure it out easily. Just try again.

That's helpful! Let's try this: M3eRa!sBIrthd@y

Yay! It worked! I'll just use it for all my accounts now

Noooo! Amit Bhaiya had said using the same one for every account is like using the same key for your house, car, and locker. If someone finds it, they can unlock everything. If one app gets hacked–your password could end up in the wrong hands, and all your other accounts would be at risk.

Oh no! I didn't think about that. What should I do?

Better to use a unique one for each!

That sounds like a lot to remember. I guess I'll write them down in my diary

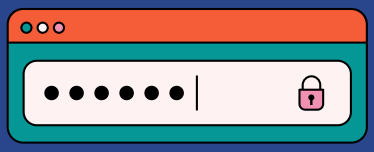
That's what I thought too, but then I started using a password manager. It's a game-changer! Now I just remember one strong master password and I can see all my other passwords. Even if someone cracks my password, I have enabled 2-factor authentication, so they can't get me! It is like having a second lock on your digital door haha!

Oh! I believed that a strong password would be enough, but I guess we need to stay extra safe!

Having many safety layers always helps. Don't forget to check out application locks too! Now, let's get going– isn't it time to cut the cake and I'm so hungry!

Let's learn from Meera's experience and ensure your accounts are secure right from the start. When signing up for a new application or creating an account, follow these essential guidelines to build a strong password:

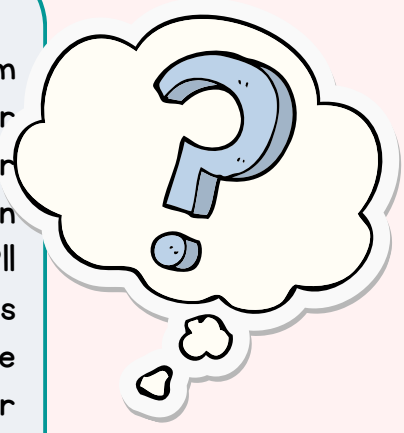
STRONG PASSWORD CHECKLIST



- Use a mix of characters: Combine uppercase (ABC) and lowercase letters (abc), numbers, and special symbols (e.g., @, #, $, !). This makes it significantly harder for hackers to guess your password.
- Make it long: Passwords should be at least 12-16 characters long for optimal security. Longer passwords take much more time to crack, even with advanced tools.
- Avoid common words and phrases: Stay away from easily guessed words like "password," "123456," or any personal information that a lot of people might know, like your name, pet's name, or favorite phrase.
- Avoid obvious personal information: Information like birthdays, anniversaries, or phone numbers is often publicly accessible through social media, making these bad choices for passwords.
- Consider a passphrase: You can use a memorable sentence or phrase and tweak it for complexity. For example, "I love ice cream in summer!" could become "IL0v3!c3Cr34m@2024."

Why does this matter?

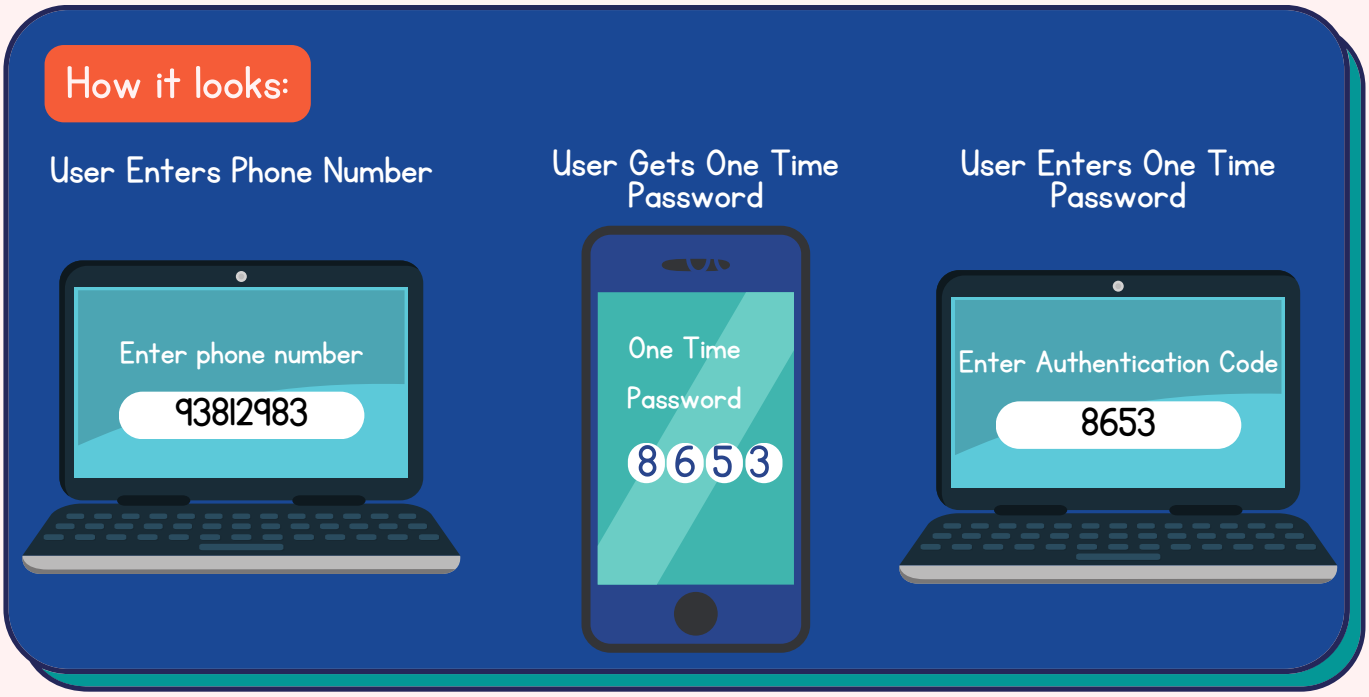
In today's world, many of us manage multiple accounts–from social media to email to banking. A strong password is your first line of defense against someone breaking into your accounts without permission. A weak or reused password can lead to stolen data, financial loss, or even identity theft. We'll explore these threats in more detail later in this chapter. As hackers become increasingly sophisticated, adhering to these guidelines can significantly enhance the security of your accounts.



2 FACTOR AUTHENTICATION

Two-factor authentication is an added layer of security for your account. Many popular platforms recommend its use. When this feature is turned on for your account, additional verification is required after providing your password for logging in; Usually, this is a code sent to your personal mobile number, which acts as a one-time password (OTP). It could also be a passkey, an email, or even a fingerprint scan. This means it is valid only for a few minutes and can be used only once. A new password will be required the next time you log in

How it looks:

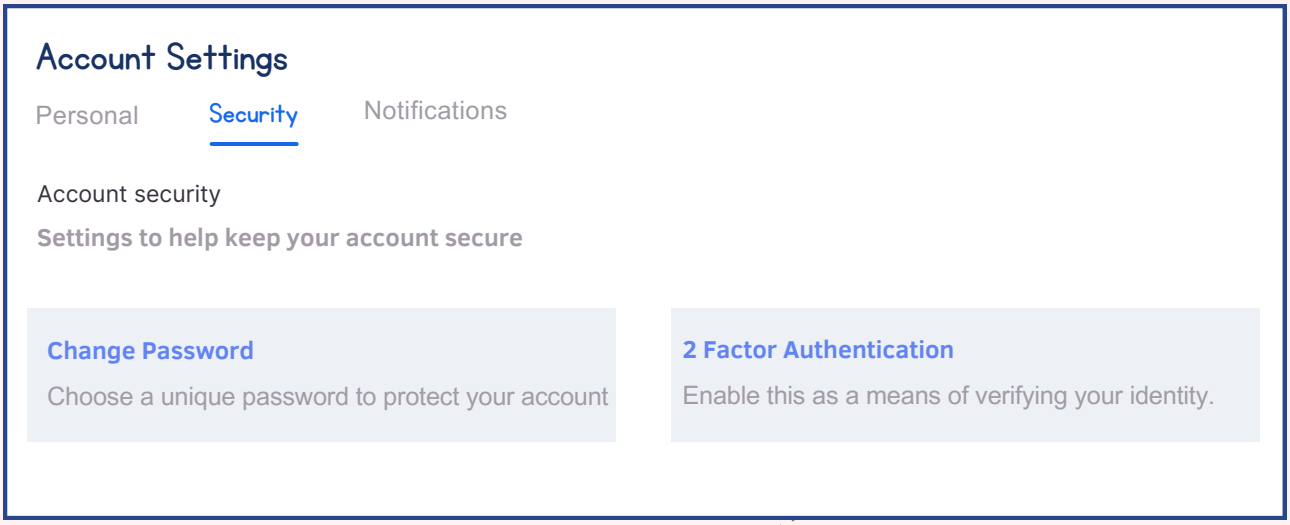


How to set up:

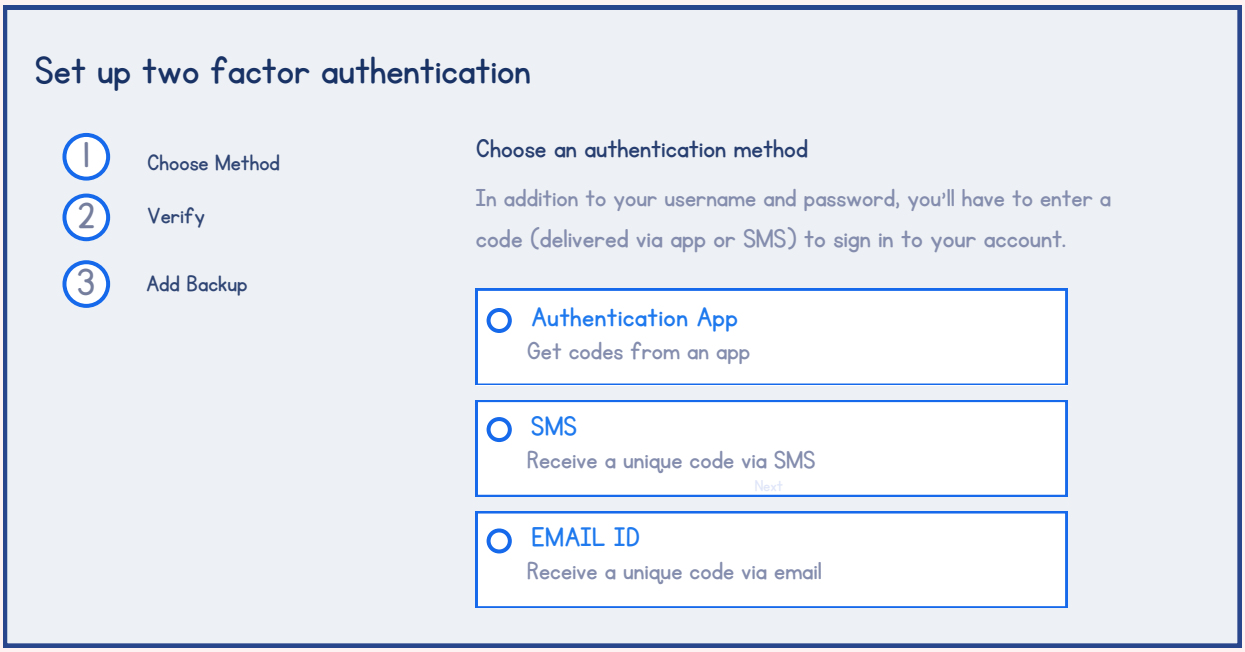
1. Go to the navigation panel. You can look for the following icons:

2. Go to the settings option. It looks something like this usually:

3. Now look for something like 'Security' or 'Privacy.'



4. Enable Two-Factor Authentication. You'll see some options for verification methods. You can pick SMS, an app, or even fingerprints.



PASSWORD MANAGERS

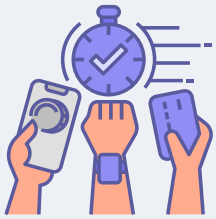
What Do Password Managers Do?

1. Store Passwords Securely: Password managers act as a digital locker, keeping your passwords safe.

2. Generate Strong Passwords: They can also create random, complex passwords for each account, ensuring you don't reuse weak or predictable passwords.

3. Auto-Fill Credentials: Many password managers automatically fill in your login details, saving you time.

Why Use a Password Manager?



With a password manager, you will not need to remember multiple, complex passwords - only the one really strong master password that unlocks your password manager. No more struggling to memorise all your passwords, no more frustration about resetting your passwords!

A password manager ensures that your data is locked away with strong encryption, like a secret code only you can crack using your master password. Without it, hackers don't stand a chance of getting to your passwords!

Some password managers can spot fake websites and other dangers online. They stop you from accidentally entering your credentials on fraudulent pages. Isn't that neat?

APPLICATION LOCKS

Yesterday, Rahim came to me with a unique problem. He loves teaching his friends in the colony how to use smartphones. However, his phone contains sensitive information, such as private notes, photos with friends and family, and personal messages. While he wants to share his phone for educational purposes, he needs to ensure that his privacy and security are not compromised. I told him: use app locks!

App locks enhance phone security by requiring a password, PIN, or biometric access for specific applications. Here's how one can safely share his phone:

Download an App Lock

Setup a secure pin

Select applications to lock

Enable biometric verification

Advantages of App Locks

- Privacy Protection: Rahim's sensitive information stays secure, even if someone else is using his phone.
- Customizable: He can choose exactly which apps to lock.
- Ease of Use: Once set up, app locks are simple and intuitive to use.

Always remember, download only verified apps from official stores to avoid harmful software, and use strong PINs on your app locks. Double and triple lock things on your phone for maximum safety!

Activity

TEST YOUR MEMORY

(I) What is the primary purpose of a password manager?
a) To store and organize all your passwords securely.
b) To automatically log you out after 5 minutes of inactivity.
c) To generate usernames for new accounts.
d) To delete accounts you no longer use.

II) Which of these passwords is the LEAST secure, even though it looks strong?
a) "Password@123!"
b) "xT#4jG!@oLmN$z"
c) "MySecureP@ss2024!"
d) "E!3xy&7#M@n2023"

(III) Which of these is NOT a recommended feature of a strong password?
a) At least 8-12 characters long.
b) Includes your full name or birth year.
c) Contains uppercase, lowercase letters, numbers, and symbols.
d) Avoids predictable sequences like "123456."

(IV) Why should you enable Two-Factor Authentication (2FA)?
a) To make logging in faster.
b) To add an extra layer of security to your account.
c) To automatically update your password every month.
d) To allow anyone to access your account.

ANSWER KEY:

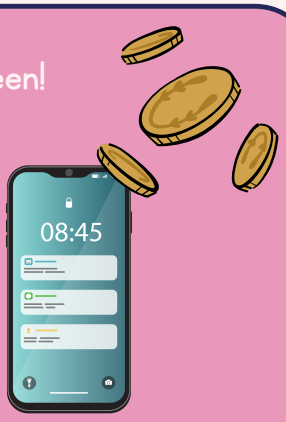
(I) a) To store and organize all your passwords securely.
(II) a) "Password@123!" (Reason: It uses a common word, "Password," and predictable patterns, making it vulnerable to hacking.)
(III) b) Includes your full name or birth year. (Reason: Personal information makes passwords easy to guess.)
(IV) b) To add an extra layer of security to your account.

UNDERSTANDING SECURITY THREATS

It's a sunny afternoon and Rahim is sitting in the neighborhood park. He just finished playing some board games and wants a new challenge! He sees his friend Jaspreet and Amit Bhaiya sitting nearby and joins them. Together, Jaspreet and Rahim open Amit Bhaiya's phone to find some new websites with challenging word puzzles.

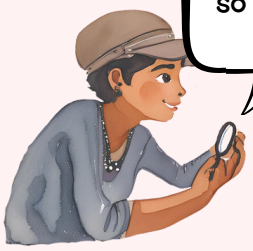
Suddenly, the following message pops up on the screen!

"Congratulations! You've won 1,000 free game coins! Click here and reply to this message with your phone number and OTP to claim your prize."

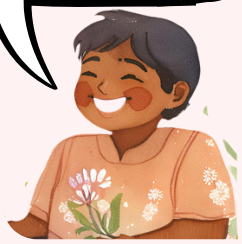


Rahim feels excited to receive so many coins, but he is unsure whether to click the message. Jaspreet also feels suspicious about the message, and together, they decide not to open it.

This message isn't from an official source and its asking for our personal details - I think it might be a scam! Scammers are constantly trying to find new ways to steal our data, money or devices through messages like these. Why don't we revise our understanding of online threats so we can stay safe?[1]



Oh yes! I can't believe despite strong passwords and security measures, I can still be harmed! I want to be fully aware so I can help myself and others too.



Let's start with HACKING then! Hackers try to see your data, like passwords or bank information and find ways to take it without you noticing.

Yeah, my cousin was hacked last year! Everyone in my family uses multiple passwords and locks since then.

Hacking

Hacking is sneaking into someone's phone, computer, or online account without permissions! Hackers use advanced codes to get past passwords and security to steal information or cause harm. Hackers can steal private information, cause damage, or even take over the device. Some hackers do it for illegal reasons, while others (called "ethical hackers") work to find security weaknesses and fix them. Hackers often use malware (a computer software or virus that secretly harms a computer or computer network) to hack devices!

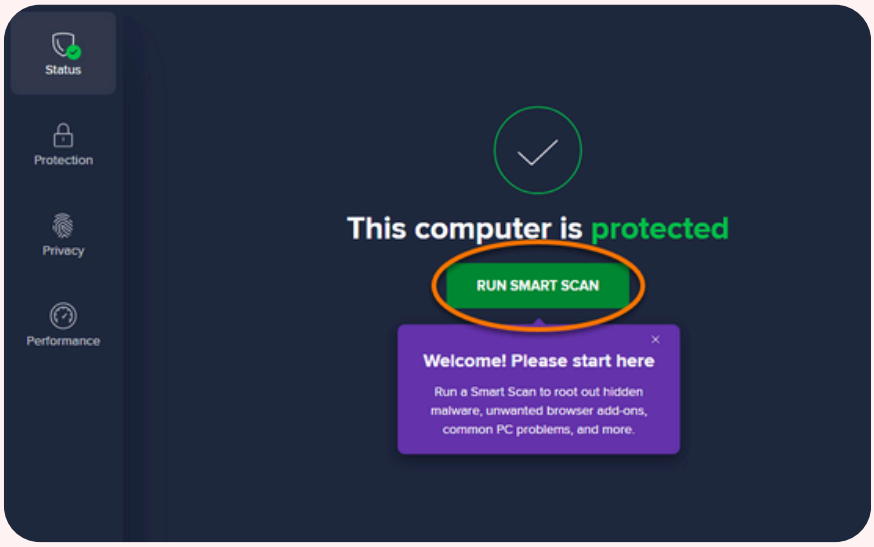
Imagine your friend's diary has a special lock on it, but you figure out the combination by watching closely when they open it. You use the combination to sneak in and read their private thoughts. That's like hacking, but instead of a diary, it happens with computers, phones, or accounts!

TIP: USE AN ANTIVIRUS SOFTWARE AND UPDATE DEVICES

Antivirus software is designed to detect and remove viruses and other kinds of harmful software from your computer. Install an antivirus software, make sure your device's firewall is turned on and regularly update your device to fix bugs or security holes that hackers could use to get in.

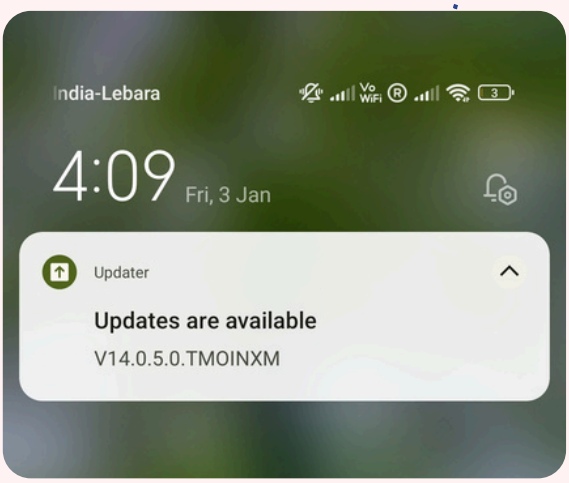
1

This image shows you what the installation and running of a reliable Antivirus software looks like. There are many softwares you can choose from, and asking an adult or doing a simple web search can help you decide!



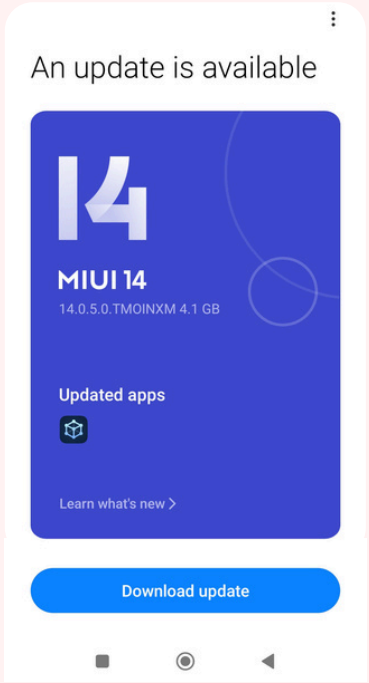
2

When your phone has an update available, it will give you a notification like this:



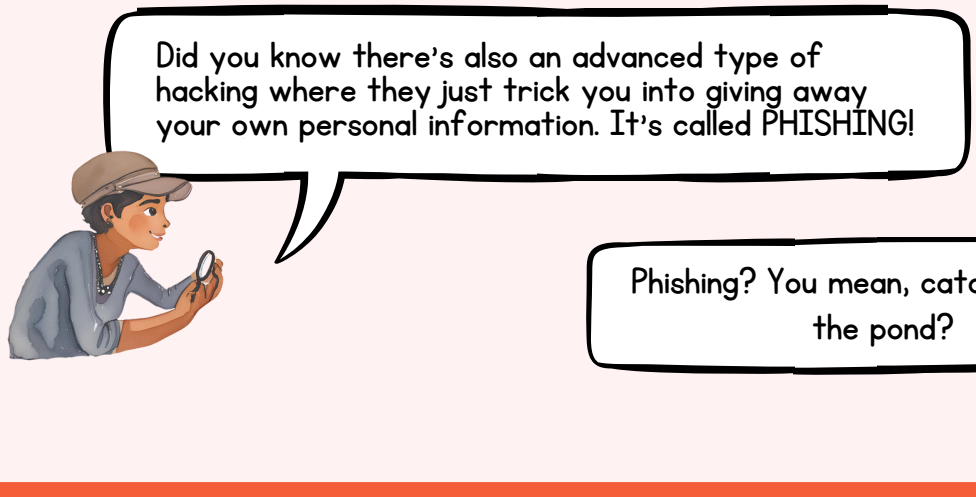
3

After clicking the notification, you will be able to download the update. You should update your phone frequently to protect against hackers!



Activity

When was the last time you updated your devices? Take a moment to think about this, and update them now if you haven't!

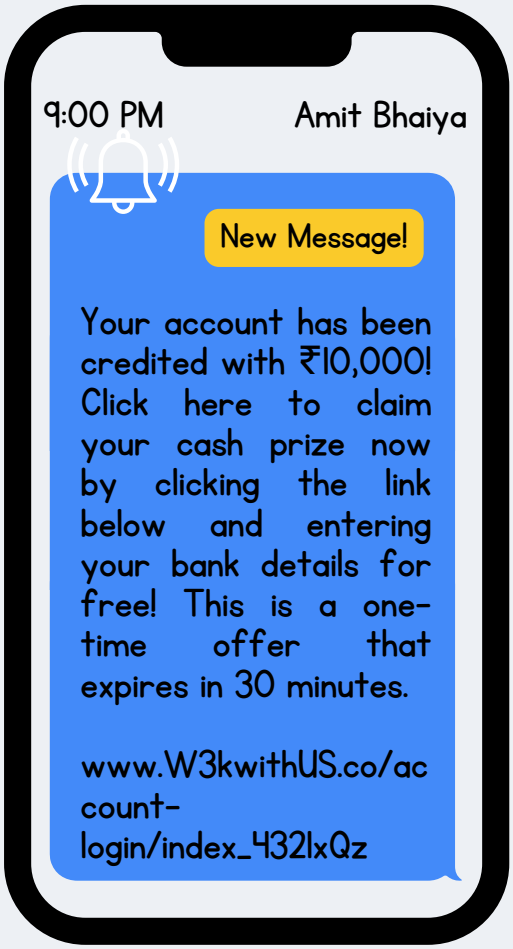


Well, sort of! You can think of it like someone trying to FISH for your information in sneaky ways, sometimes by pretending to be another person or even your bank, school or favorite video game! The message we received earlier is a perfect example of phishing!

Phishing

Phishing is a sneaky trick where scammers send fake messages that look official! The messages usually create a sense of urgency, like "Your account will be deleted unless you verify now!" so that we panic and click the link or enter sensitive information like passwords or credit card numbers. This information then goes straight to the scammer. Let's look at an example of phishing.

Notice the urgency of the message, the fake link at the bottom, and the fact that the message asks for sensitive personal details - these are all RED FLAGS! You should always be wary of messages or calls that ask for banking information.



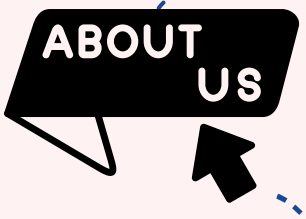
TIP: CHECK THE LINK!!

If you receive a link from an unexpected source, looks inaccurate, or comes with a tempting message, stay away... Sometimes, unknown links can steal your information or download harmful viruses onto your device.

Here are some guidelines that will help you stay away from harmful links and make sure you are on a safe, trustworthy website.

- Check the link of the website where you type on the browser, make sure it begins with "https" The "S" stands for secure and indicates that the site uses encryption to protect data.

- Make sure the link name ends with ".com" ".org" ".gov" ".in" or ".edu.in" - these are standard names



- Check the overall website - especially the About Section - to understand who made it and how it is designed.

- Double-check the URL to ensure it's not a spoofed or fake version of a trusted site. For example, "amaz0n.com" is a fake site trying to imitate "amazon.com."

- Search online for reviews about the platform to ensure it is legitimate and trusted by other users.

AdBlockers, as the name suggests, block pop-ups, advertisements and other unreliable elements on the internet, in case you accidentally click on one. As you can see on the right, some unreliable websites might ask you to disable your ad blocker - that can be unsafe!

Activity

Do you use an AdBlocker?
Try installing a reliable AdBlocker as an extension on your browser!

Phishing sounds really scary! What do hackers and "phishers" even do with all of this information?

They can use all of your information they have gathered to impersonate you online. They can make accounts, withdraw money from your banks, and even take out loans under your name! It's called IDENTITY THEFT.

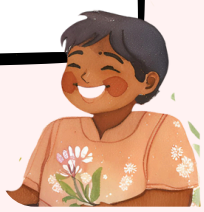
Identity Theft

Identity theft happens when someone pretends to be you by using your personal information like your name, address, or Aadhar card number! They might do this to open accounts, buy things, or do something illegal while making it seem like it's your fault. This can cause big problems, like getting blamed for things you didn't do or losing access to your own accounts. Here are some examples!

Let's say someone finds your lost school ID card and uses your roll number to pretend to be you and collect your exam paper. The teacher believes them because they think it's really you - now they can see your exam score!

Suppose someone finds a lost wallet at a grocery store. Instead of returning it, they use that person's name, age, and address from their ID cards to apply for a credit card. They start buying expensive things, and when the bill comes, it's sent to the owner of the wallet, even though they never spent that money!

So let's say that someone manages to use these methods to steal my identity, information and data... what else can they do with it?

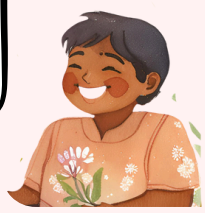


Unfortunately, they might sell your data, misuse it and even use it to target a group of people! This is called DATA THEFT.

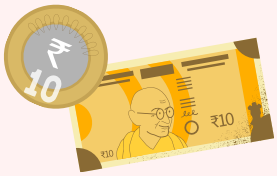
Data Theft

Data theft involves stealing digital information, such as passwords, bank details, or medical records, without permission. This data can be sold or used to commit further crimes! Businesses are often targeted because they store large amounts of customer information, but individuals can also be victims.

I think I am now starting to piece together all of parts of the puzzle! But I still don't understand why someone would steal all of this?



Let's ask Amit Bhaiya to tell us more!



You are both very sharp! All of these activities like hacking, phishing, and data and identity theft should be taken very seriously, because they are often used to commit FINANCIAL FRAUD. This is when someone steals your money or financial information. Fraud can happen online or in person and is often hard to undo. That is why we must be extremely careful. Here is an example of financial fraud to help you protect yourself better - this happened to my sister last week!

Hello, ma'am. I am Suresh from District Electricity Board. This is a very urgent call. According to our records, your last electricity bill payment didn't go through, and your connection is at risk of being cut off in the next 2 hours.

What? I paid my bill last week! There must be some mistake.

I understand your concern, ma'am, but we received no confirmation of payment. To avoid disconnection, I'll need you to quickly settle the outstanding amount of ₹2,500. Don't worry, I can guide you through it right now over the phone.

What do I need to do?

Please open your banking app on your phone and I'll give you the secure link to complete the payment. Make sure you complete this within 5 minutes to avoid any disruption!.

Amit's sister clicks the link, which leads to a fake payment page... and ends up paying her bill all over again, to an unknown person!

Did you both notice some suspicious signs in this conversation? Here are some red flags you can look out for:

Urgency and Fear:
The caller creates panic to pressure the victim into acting without thinking.

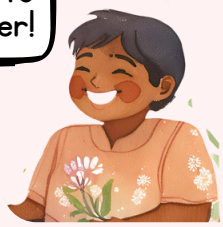
Unverified Identity:
The caller claims to represent an authority but doesn't provide proof.

Unusual Payment Method:
Legitimate companies rarely ask for instant payments over personal accounts or unsecured links.

Fake Link:
The caller sent a malicious link disguised as an official payment page.

My sister later noticed that the payment website had an incorrect layout and URL. What else do you both think my sister could have done to cross-check the scammer and protect herself?

Hmm.... She could have asked the caller for his ID and then called the electricity company to confirm? I think she should also block the number!



Hmm.... she should probably also check with her bank to make sure nothing was withdrawn!

Good job!! All of these tips and safety measures will also be useful for you when you shop online too!

Your Online Shopping Safety Checklist

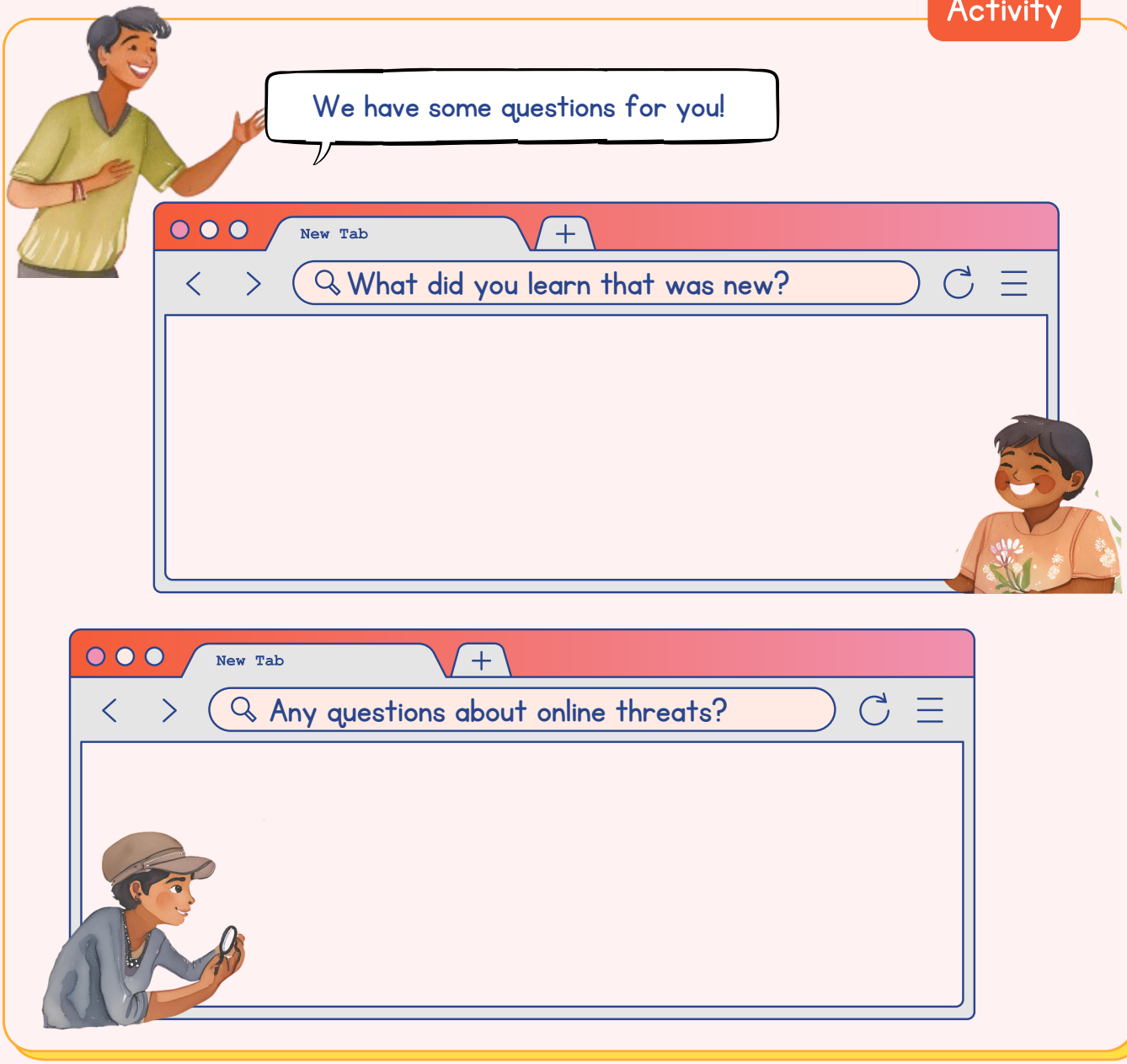
- [ ] Look for reviews and see what other customers are saying about the product. Watch out for fake reviews or suspicious content.
- [ ] Ensure the site is secure, has 'https://' and a lock icon in the address bar.
- [ ] Double-check the size, colour and any special features of the product to make sure it's exactly what you need. Don't just trust the pictures!
- [ ] Did the site ask you for information like passwords or bank details? Genuine shopping sites would never ask this on a call, e-mail or message!
- [ ] Make sure the payment gateway is secure and avoid sharing details like OTP, card details and CVV codes with suspicious websites
- [ ] Ensure messages about the order are genuine - they usually shouldn't include things like: orders you haven't placed, lotteries, sensitive information, or spelling mistakes!
- [ ] Make sure to read the terms and conditions, and refund policy to understand the process if a product doesn't meet your expectations.

Did you know?

On Amazon, you can raise a complaint on phishing attacks, suspicious calls/e-mails/texts or unsafe/suspicious products. Under Amazon's Help...

- Go to "Report Something Suspicious" and select among the options. Submit the report with relevant details. Forward the suspicious e-mail/text on reportascam@amazon.in.
- Report mysterious packages under "Unsolicited Packages Received" by checking the box carefully and submitting details.
- Report sellers or products directly from the product page, by clicking on "Report an issue with this product or seller" and following the instructions.
- Here are some common scams identified by Amazon.

Activity



New Tab

Can you look for these tools online?

Three Reliable Anti-Virus Softwares:

1.
2.
3.

Three Reliable and Free Ad-Blockers:

1.
2.
3.

RECAP: THINGS TO REMEMBER TO PROTECT YOURSELF!

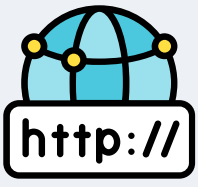
Remember, if something feels suspicious, you should talk to a parent, teacher, or another trusted adult![3]

STRONG PASSWORDS

Create passwords that are hard to guess, with a mix of letters, numbers, and special characters! Avoid using simple things like your name, pet's name, or "12345." If you use shared devices, always make sure to log out of them after each session.

DOUBLE DEFENSE

Use 2 Factor Authentication to set up an extra lock on your accounts! It makes sure that even if someone guesses your password, they'll still need the second code to get in. Go to Settings on any account to find it, under Privacy and Security.



THINK BEFORE YOU CLICK!

Don't click on links in emails or messages unless you're sure they're safe. If something feels suspicious, verify it by checking directly with the company or person. Also look out for spelling mistakes in emails, messages from strangers, or urgent demands for money!

RECAP: THINGS TO REMEMBER TO PROTECT YOURSELF!

ADBLOCKERS

Ad blockers are software tools or browser extensions designed to remove or block advertisements on websites, including pop-ups, banners, and video ads. By preventing ads from loading, they enhance browsing speed, reduce data usage, and help protect against malicious ads that may contain malware.

AVOID PUBLIC WI-FI AND TURN OFF BLUETOOTH

Using public Wi-Fi or keeping Bluetooth on risks exposing data to external actors. It's safer to use a private, secure network and keep Bluetooth off when not in use!

BE CAREFUL WHAT YOU SHARE ONLINE

Avoid sharing personal information like your full name, address, phone number, or school name on social media! Use privacy settings on social media and games to control who can see your profile, posts, and messages. Soon, we will explore how to do so!

USE AN ANTIVIRUS SOFTWARE AND UPDATE DEVICES

Install an antivirus software and make sure your device's firewall is turned on. These tools help detect and block harmful malware and viruses that hackers use to steal your information. You should also regularly update your device to fix bugs or security holes that hackers could use to get in.

BACK UP YOUR DATA

Regularly save copies of important files or photos on an external hard drive or cloud service. If your device is ever hacked or infected with a virus, you won't lose everything.

Chapter 3: Privacy - Your Digital Shield!

Meera, Rahim, and Susan are enjoying a sunny day at the park, laughing and joking as they take selfies. Meera finds a photo of them very cute. She uploads it and tags them along with mentioning the location!

Wait, Meera, you tagged me and added the location? I'm not really okay with that.

Why not? It's just a fun photo. What's the harm in tagging the location?

It just makes me uneasy. Sharing where we are in real time is risky. You should ask first!

Everyone posts photos like this, Rahim. You should relax, nothing is going to happen.

That's not the point! How do I explain it to you ughh....

Rahim, why don't we go to someone who can help Meera understand the issue here? Let's go see Amit Bhaiyya!

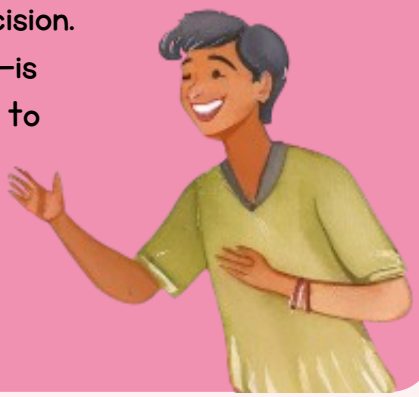
Oh hello all! I'm glad you came to me. All of you are becoming active internet users now. This is a great time to start learning about online privacy, consent and boundaries! So let us begin!

Understanding privacy, consent and boundaries

Privacy means having control over who knows what information about you. Different people are comfortable with different levels of privacy - for example, some people don't like to share their birthdays, while others do! However, just like we are careful not to share our location or personal stories with strangers offline, maintaining and increasing your privacy online can help keep you safe.

In 2017, a landmark case in India, popularly known as the Puttaswamy Judgement, officially recognized privacy as a fundamental right for all citizens. This judgement marked a turning point, emphasizing that every individual has the right to control their personal space, information, and choices.

Think of it this way: You might choose not to share everything about your online activity with your parents or friends, it's entirely your decision. This sense of control over what you share—and with whom—is what privacy is all about. In this chapter, we'll explore how to better understand and express our digital boundaries to protect our privacy.

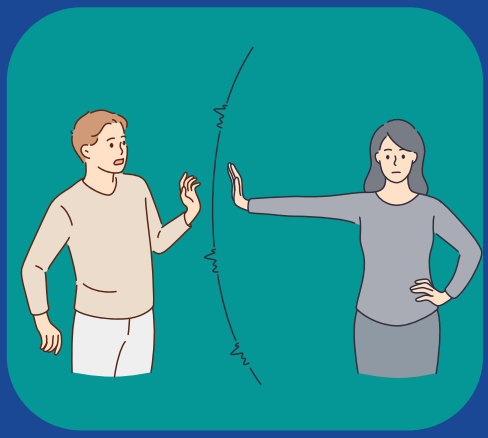


What is Digital Consent?

Digital consent means saying 'yes' or 'no' when someone asks to use, share, or interact with your personal information, photos, or messages online. It involves making a conscious and informed choice about what you're comfortable with, and it applies to sharing things like photos, messages, or even your location. Digital consent can be updated at any time - if you no longer feel comfortable with something after you've said yes, you can still refuse! It's essential to understand that consent must be actively given and cannot be forced or assumed.

Boundaries : A pattern of consenting

Boundaries are invisible lines that define what makes you feel safe and comfortable. In digital spaces, they help you decide what to share, who to trust, and what to expect from others. Once you decide your boundaries, you can use them to give or refuse consent based on what feels right for you. For example, if you prefer being asked before someone posts a photo of you or only sharing your location with close friends, these boundaries guide your choices and help others respect your comfort.



Privacy vs Security

Privacy is about control over your personal information, while security is about protecting your data and devices from external threats. They are interconnected– strong security often supports privacy, and being mindful of privacy helps maintain better security.

Activity

Identify whether the following actions are measures for privacy, security, or both:

- Creating strong, unique passwords for each account.
- Turning off location services for apps you don't use often.
- Logging out of your accounts on shared devices after use.
- Keeping your social media account private.
- Avoiding sharing your social media username.

Activity

Reflecting on Personal Privacy and Boundaries Preferences

Look at each statement on the bingo card and mark the ones that describe what you feel comfortable with online.
If you complete a row, column, or diagonal, shout "Bingo!"

I feel comfortable sharing my birthday online.	I use a private account on social media.	I avoid sharing my real-time location in posts.	I don't like sharing my email address online.
I feel uneasy when someone tags me without asking.	I'm okay with sharing photos, but only with close friends.	I prefer not to share my phone number online.	I feel uneasy when a friend shares my story without asking.
I always review who can see my posts before sharing.	I avoid posting personal details like my school or home address.	I feel comfortable asking someone to remove a post about me.	I always think twice before sharing anything personal on social media.
I prefer sharing only positive or neutral updates about myself.	I feel okay sharing my opinions in online discussions.	I don't mind if someone shares a group photo with me in it.	I don't accept friend requests from strangers

Did you notice any statements that made you pause or think more deeply?
Did you notice any patterns in what you're comfortable with?
Are there any new boundaries you'd like to set for yourself based on this activity?

I got you, buddies! Next time you have to have one such conversation, just remember these points

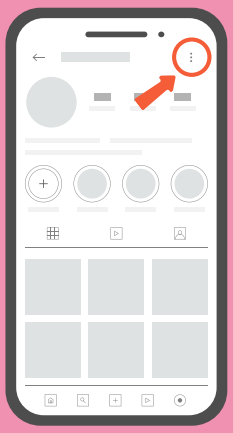
- Your tone matters: Speak in a way that shows you're not angry or upset. You can just say "I just want to share how I feel about this," instead of yelling or sounding annoyed.
- Use emotion words: Share how you feel to explain why the boundary matters. For example, say, "I feel worried about my safety" instead of just saying, "Don't do that."
- Listen and stay open to questions: After you've shared your boundaries, let the other person ask questions or share their thoughts. It's important to have a conversation, not just give rules. This is how we all learn!

Meera & Rahim, let's model it out, shall we?

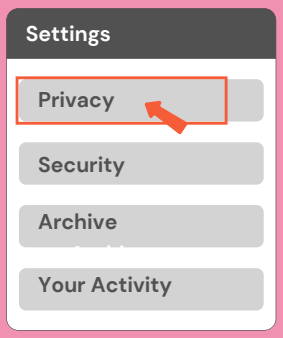
Enhancing privacy settings

Now that we've set personal boundaries, let's look at how to protect your privacy across various platforms. This involves understanding how social media, email accounts, and apps handle your personal information. Knowing what data is collected and how it's used is key to staying in control of your online presence.

Pause here and check if your social media account is public or private. If you don't know how to check, follow these steps

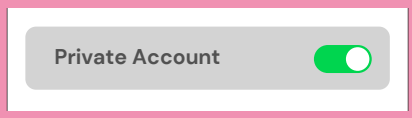


1. Open your social media app and go to your profile settings.

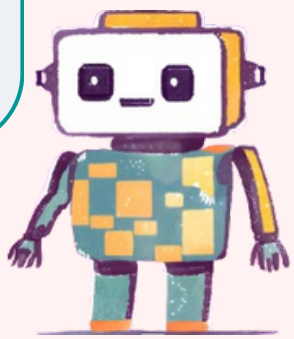


2. Look for an option like Privacy Settings or Account Settings.

3. If your account is public, you can switch it to Private to limit who can see your content.



Remember we talked about Digital Footprint, the trail you leave behind whenever you go online, in the first chapter? Apps, websites, and social media platforms often collect this data to personalize your experience – showing you targeted ads, recommending videos, or even predicting your preferences. While this can feel convenient, it's important to understand how much you're sharing and how to take control of it.



Cache and Cookies: What Are They?

When you visit a website, it sometimes "remembers" your activity. That's because of cache and cookies:

- Cache: Think of it as a backpack your browser carries, storing bits of websites (like images and scripts) so they load faster the next time you visit.
- Cookies: These are tiny crumbs of information stored by the website, like what you clicked on, added to your cart, or even how long you spent on a page.

Cookies also allow websites to track your activity while cache can be used by someone accessing your device to see where you've been online. This can feel like someone peeking over your shoulder as you browse.

Privacy Policies and Tools

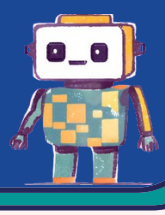
When you sign up for a new game or app, you're often asked to agree to a privacy policy. This document explains how your data is collected, stored, shared, or used. But most people skip reading these because they're too long or complicated.

Some apps and websites may use your data responsibly, but others might share or sell it to third parties. Understanding privacy policies helps you make informed decisions about what you're agreeing to. You can look for tools online that break down privacy policies into simple, easy-to-understand language. Also, some tools can help evaluate websites and apps based on how well they protect your data

App Permissions

- When downloading a new app, it may request permissions for features like the camera, location, or contacts. While some permissions are necessary for functionality, others may be unnecessary, leading to potential data misuse. For example, a photo editing app shouldn't require location access. To stay safe, consider if the app genuinely needs the permission, review and disable unnecessary permissions in device settings, and be cautious with apps that request excessive permissions upon installation.

We have just looked into how apps and websites can affect our privacy. Now, let's turn our attention to how other internet users might impact it, along with tips on how to identify and address these situations.



Online Privacy Violations

Meera, Rahim, and Susan are excited to meet Amit Bhaiya and Glitch to share their experiences from the previous day at the park. Though Meera feels a little shy, she's eager to tell Amit Bhaiya about the valuable lesson she learned–always seeking permission before sharing a picture online that includes others.

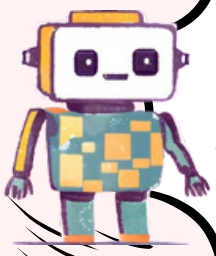
Very good Meera, that is indeed a very important learning, but do you know that such 'non-consensual sharing of images' is quite common?

Really? I guess we all need to have more conversations about why this is important. Can you tell me more?

Non-consensual sharing of images means sharing someone's photo or video without their permission. This can happen in group chats, on social media, or even through private messages. It's a violation of privacy and can have serious consequences.

Why is Non-Consensual Sharing Harmful?

- It invades privacy: Sharing someone's image without their permission violates their right to decide who can view their personal information, including photos.
- It can lead to bullying or harassment: Mean comments or inappropriate sharing can cause emotional harm.
- It may make someone feel anxious, unsafe, or embarrassed: A person might feel upset or unsafe when their image is shared without consent.



When in doubt about someone's comfort, just ask! It's always better to check their boundaries than assume.

Want to protect your and other people's privacy online? Take this quick "True or False" quiz to see if you know if you are on the right track!

-It's okay to share someone's photo without asking if they're your friend. (True/False)

-If someone shares a picture of a friend in a group chat without their permission and makes fun of it, it's okay to ignore it and keep chatting. (True/False)

-If it is a group photo, it is okay to tag people without asking. (True/False)

Let's explore some of the ways people's privacy and safety can be violated online. These might seem scary, but don't worry, if you understand them fully then it is the first step to staying safe.

Bullying

You've probably heard about bullying before–it's often thought of as something physical, like pushing someone around or teasing them face-to-face. But did you know that bullying happens online too? It can be just as harmful, if not more, because it can reach a wider audience and happen anytime, anywhere.

Online bullying, also known as 'cyberbullying', takes many different forms. It's not just about mean words; it can involve actions like revealing someone's private information (doxxing), posting hurtful comments (trolling) and leaving someone out of online groups (exclusion).

Doxxing

Doxxing is when someone publishes your personal information online without your consent, like your address or phone number.

Trolling

Trolling is when someone posts hurtful or annoying comments just to upset others.

Exclusion

Exclusion is when someone is left out of online groups or chats on purpose to make them feel bad.

Step into Their Shoes: Understanding Trolling

Imagine being in the middle of a conversation online when someone suddenly begins targeting you with hurtful words. This isn't just "teasing"; it's trolling–intentional and persistent actions meant to provoke or humiliate. Let's look at an example:

Dear Diary,
Today, the science project discussion turned into something I wasn't expecting.
Aryan typed, "Don't give Sameer anything important. He'll mess it up like last time." Everyone liked it, and I felt humiliated.
Then Kunal posted, "Some of old family pictures." I didn't know how he found that out—it felt like an invasion.
Riya said, "Let's leave Sameer out of the project. He's useless." And they added, "We'll talk more about this in the personal group, not with Sameer here." I felt completely excluded.
Aryan posted again, "Sameer won't even finish his part. He's a waste of space." It felt hew was trying to get a reaction from me.
I just logged off. Why do they treat me like this?
Sameer

Activity

Can you spot the different types of bullying? Match the moments with:

-Exclusion: _____

-Doxxing: _____

-Trolling: _____

What would you have done, if you were also a part of this online group? _____

_____

Now that you all know about online privacy, let's talk about some threats in the online world – the various forms of cyberbullying and harassment. These behaviors are not just "bad manners"; they are illegal and deeply hurtful. But don't worry! You can take control of your online safety by understanding these dangers.

Cyberstalking

Cyberstalking is when someone obsessively tracks you online–checking your posts, commenting excessively, or even sending messages to make you feel unsafe.

Sexual Harassment

Sexual harassment online includes sending inappropriate messages, images, or making someone feel uncomfortable through words.

Sextortion

Sextortion is when someone tricks or forces a person into sharing private images or videos, then threatens to share them publicly unless they're paid or do more things.

Revenge porn

Revenge porn is when someone shares private images or videos of another person to embarrass or hurt them.

Catfishing

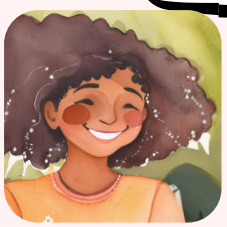
Catfishing is when someone pretends to be someone else online to trick or hurt others. They might use fake photos, names, or details to trick you into trusting them.

Masquerading

Masquerading is when someone pretends to be someone they are not to hurt or manipulate you. This is slightly different from catfishing, as it's often done to bully or harass someone while hiding behind a fake identity.

Deepfake

Deepfake is when someone uses AI (artificial intelligence) to create fake photos or videos that look real but aren't. These can make it look like someone said or did something they didn't.



Oh! These sound so scary, bhaiya! These remind me of my classmate, Sara. She has made an online friend who used to send her gifts and flowers. She really likes this friend and has started meeting him offline also. But he has now started making her uncomfortable with his request to meet alone and come closer. He is 29 years old, and he says this is how old people behave! I don't know what to tell Sara :(

Ah I am so glad you told me this, Susan. What you just described is another common online threat - grooming. But don't worry, we'll understand it together so you can support your friend in the best way possible.

Online Grooming

Online grooming is when an adult builds a relationship with an underage person online by tricking or manipulating them. They might start by being friendly and understanding, but their real goal is to take advantage of the underage person and sexually exploit them.

Stages of Online Grooming

Identification

Before contacting the child, the groomer may target a child and try to learn about their life, identifying their vulnerabilities - what they want, what they are dissatisfied by, what they need and how they feel.

Trust Building

They try to fulfill the child's needs that are not being met in their usual life. Perpetrators utilize tactics such as gift-giving, flattery, gifting money, and meeting other basic needs.

Isolation

They might create situations for them to be alone and reinforce that nobody cares for the child the way they do. The groomer also sexualizes their relationship by taking advantage of the child's curiosity.

Control

This takes the form of sexual abuse, controlling where they go and what they do, who they meet, etc. The groomer can make the child believe they are the only person who can meet their emotional & material needs.

Signs of grooming

Excessive Attention: The individual may shower the young person with compliments, gifts, or special treatment to make them feel special.
Inappropriate Conversations: They might engage in conversations that are not age-appropriate, often introducing topics related to relationships or sexuality prematurely.
Testing Boundaries: The person might gradually test physical or emotional boundaries to see how the young person responds, often escalating their behavior over time.

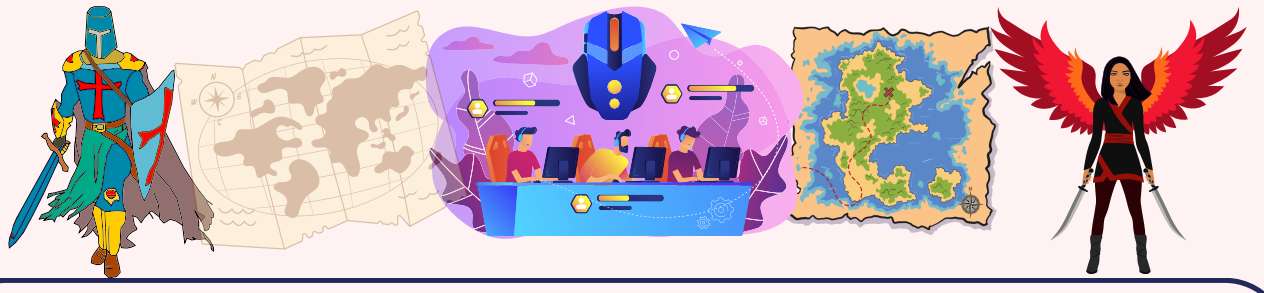
This sounds so much like what is happening with Sara! What should she do now?

Well, you should encourage her to immediately report the situation to the relevant authorities, with the support of a trusted adult. Let me also tell you about some actions you can take in such situations.

What actions to take upon noticing these signs.

Document Everything: Keep a detailed record of all the interactions. This can include screenshots of messages or emails, descriptions of conversations, and any other relevant information.
Communicate Openly: Talk to someone you trust about what's happening. This could be a parent, teacher, school counselor, or another trusted adult.
Involve Trusted Adults: Encourage the young person to share what's happening with a trusted adult, such as a parent, teacher, or school counselor. Having the support of someone they trust can make a significant difference.
Gradually Reduce Contact: Start by decreasing the frequency of interactions. Politely decline invitations and take longer to respond to messages, signaling your need for space.

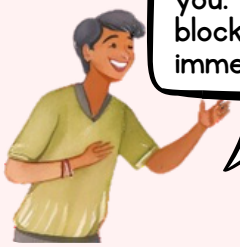
Online Gaming: A World of Fun and Risks



Rahim was enjoying his Saturday afternoon, with his brother's laptop, fully immersed in an intense online game. He had just beaten a tough level and was ready for his next challenge when a notification popped up.

Bhaiya, something creepy happened while I was gaming. This player, 'XxShadowSlayerxX,' kept following me, messaging things like, 'I know where you live.' I got so scared, I closed the game and lost all my progress.

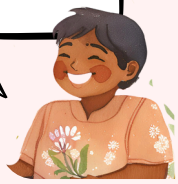
Rahim, that's cyberstalking. It's meant to scare you. You did the right thing by stopping. Now, block and report him on the platform immediately.



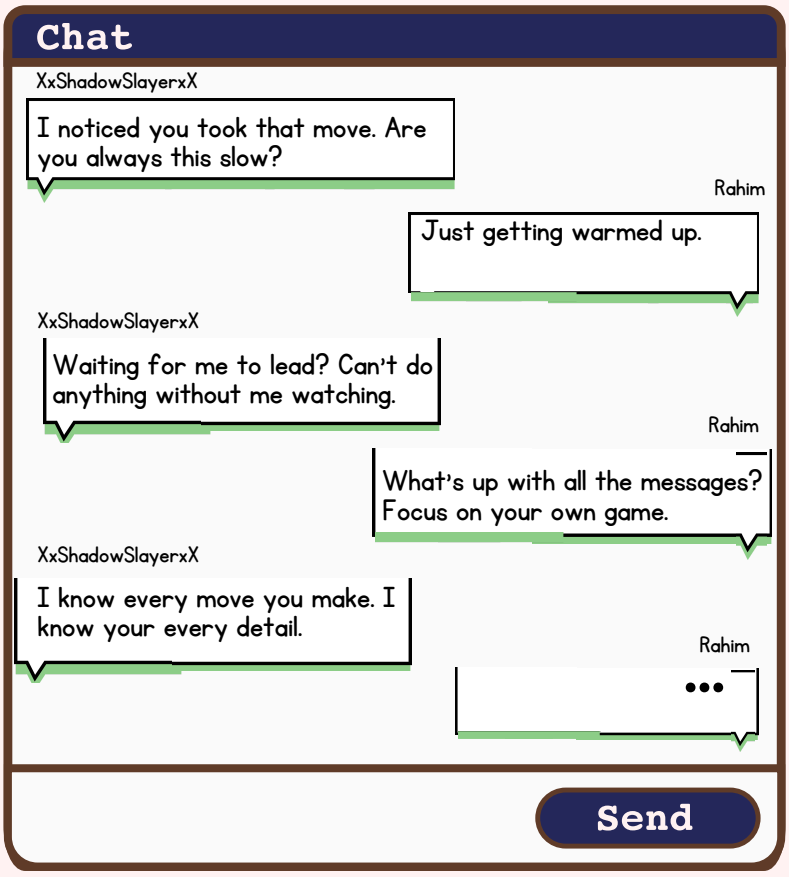
But what if he does more? I feel really unsafe.

You can make your account private if that makes you feel safer. And it is better to avoid sharing personal information with strangers. If anything like this happens again, come to me or another trusted adult right away.

Thanks, Bhaiya. I'll block him and make sure my friends know about this too.



Gaming is fun, but it comes with risks. Watch out for deepfake avatars, where players pretend to be someone they're not to trick you into sharing personal info. Online grooming can happen when someone gains your trust through in-game gifts, then asks for personal details. And be cautious of doxxing, where players might share your personal info to embarrass or threaten you. Always keep your personal details private and report suspicious behavior.



With your help, I'll never feel scared or helpless in such situations again. But Bhaiya, tell me, do these threats only happen during online gaming?

Not at all, Rahim. These threats can happen anywhere online–social media, virtual classes, even family chat groups. Both known and unknown people can violate your boundaries. That's why it's so important to stay alert and protect your privacy no matter where you are online.

Everyday Online Traps: Staying Safe in the Digital World

Often, people come across job ads promising high pay for minimal work. Drawn in by the opportunity, they quickly apply, sharing personal details like their name, email, and qualifications. Shortly after, the website requests a "small deposit" to secure the position. It all seems legitimate–until it's too late. The scammer disappears, leaving them frustrated and unsure how your information might be misused.

Online traps like fake job offers, phishing scams, and grooming are common, and they don't always involve strangers. Sometimes, even people you know can misuse your trust. That's why it's important to stay alert and trust your instincts. Pay attention to how you feel online–do you feel safe, or does something seem off? Listening to your intuition can help you navigate the digital world more safely.

Impact of Privacy Violation on the Victim

After Sara's experience with online grooming, Susan and some of her classmates had discussed online threats. They realised that occurrences of online privacy violations and other attacks are not uncommon. After their discussion, Susan put down some notes on how different people might feel and respond to online attacks and any violation of privacy.

It's not just about the violation itself–privacy violations can really mess with how people feel about being online. Like, they start losing trust in those spaces and get super wary about using them again. But it's more than that. The impact hits differently for different people.

Social and emotional

Some feel it emotionally–like feeling anxious or embarrassed, even though it's not their fault. It leaves them vulnerable, exposed, and just...hurt. Sometimes they even end up isolating themselves because of it.

Physical

For others, it shows up physically. Stress, sleep problems, appetite changes–some even have health issues.

It's not surprising that focus gets harder too. Struggling with school or even regular chores becomes a thing. (Honestly, that tracks!)

And yeah, these feelings might fade after a few days or weeks, but for some people, it sticks around way longer.

What can we do?

Hearing their stories really made me think. They found connection with people who understood what they went through, and that gave them some reassurance–it wasn't all on them. It's sad that privacy violations made them question themselves, but it doesn't mean they're any less capable, trustworthy, or smart. They didn't deserve that, and it's a reminder that no one does.

If there is a privacy violation, remind yourself or your friend that it's not your fault, and talk to someone you trust to process feelings of anxiety, embarrassment, or vulnerability.

Focus on recovery by practicing self-care, giving yourself time to heal, and staying connected with supportive people who can reassure you.

You can take some time off and rebuild trust in online spaces gradually by learning safer habits (like using stronger passwords or being cautious about sharing personal info).

Protecting yourself: What to share online

We've just looked at several types of threats online, but there are things you can do to strengthen your privacy and control over data! Let's now take some time to look at how to protect yourself from threats by understanding what is safe and not safe to share online. Information we are asked for online can generally fall into one of three categories.

Personal Information

Information that can help strangers directly or indirectly identify an individual - like your name! Even seemingly harmless details can be pieced together to form a bigger picture of your identity.

Some examples of personal information are:

- Basic Details: Your full name, date of birth, or age.
- Contact Information: Your phone number, home address, email ID.
- Social Media Activity: Photos with location tags, check-ins at specific places, or posts with identifiable details.

Sharing personal information online increases the risk of identity theft, stalking, or phishing attacks. Always think twice before disclosing personal details, especially on public platforms.

Non-Personal Information

Information that cannot be used to specifically identify an individual - like favourite colour! While it may seem safe, even non-personal data can sometimes contribute to identifying someone when combined with other information.

Some examples of non-personal information are:

- Preferences: Your favorite color, TV shows, or hobbies.
- General Opinions: Your thoughts on a new movie or book.
- Aggregated Data: Trends or survey results that do not reveal individual details.

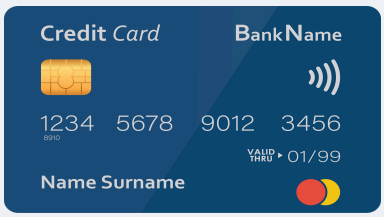
Sharing non-personal information is generally safer. However, be careful: your preferences or habits could still give marketers, algorithms, or even malicious actors insights into your behavior.

Sensitive Personal Information

Sensitive personal - that is, personal information is extra vulnerable to being misused because it locks other important things - like your signature! Misuse of this information can have serious consequences like financial fraud or impersonation.

Some examples of sensitive personal information are:

- Identity-Verification Data: Your signature, government-issued ID numbers (e.g., Aadhaar, passport, Social Security Number).
- Financial Details: Bank account numbers, credit/debit card information, or UPI PINs.
- Authentication Details: Passwords, PINs, security answers, or biometric data like fingerprints or facial recognition.
- Health Information: Medical records, diagnoses, or prescriptions.



Why it matters: Sensitive personal information is a prime target for cybercriminals. It's crucial to keep such data secure and only share it with trusted entities on secure platforms.

ACTIVITY

Help Meera decide what information is safe to share online. Read each situation below and:

- Identify the type of information

Personal | Non-Personal | Sensitive Personal

- Decide Meera's Action

Share freely | Avoid Sharing | Share Cautiously (only if necessary and on trusted platforms)

Scenarios:

- Meera is asked to upload her full name to join an online puzzle-solving competition.
  - Type: _____
  - Action: _____

- A cooking app requests Meera email address to send her recipes.
  - Type: _____
  - Action: _____

- An unverified website asks Meera for her phone number to enter a giveaway.
  - Type: _____
  - Action: _____

- A gaming app wants Meera's date of birth to verify her age.
  - Type: _____
  - Action: _____

- Meera shares her favorite book title on a discussion forum.
  - Type: _____
  - Action: _____

- A shopping website asks Meera to provide his address for a product delivery.
  - Type: _____
  - Action: _____

- Meera is asked to upload his signature to verify her identity for an online banking service.
  - Type: _____
  - Action: _____

RECAP: HOW TO STAY SAFE WHEN SHARING INFORMATION ONLINE

Think Before You Share: Always question whether the information is truly necessary to share online.

Limit Visibility: Use privacy settings on social media to control who can see your posts.

Be Cautious on Public Wi-Fi: Avoid sharing sensitive information when connected to public or unsecured networks.

Use Secure Channels: Share sensitive details (e.g., bank information) only on encrypted platforms.

Regularly Monitor Accounts: Keep an eye on your online accounts for unusual activity to catch any misuse early.

Chapter 4: Click Wisely: Dodging Misinformation Like a Pro

Shubham was scrolling on her phone when she came across what seemed to be important news. Urgently, she shared it on her social media to spread the word.

Hey Shubham, I think this is fake news!

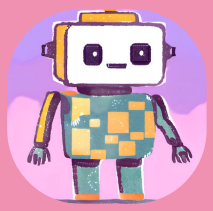
This was debunked yesterday, be careful!

Not true, Shubham. Just saw an article clarifying this!

Soon, Shubham sees many comments on her shared post.

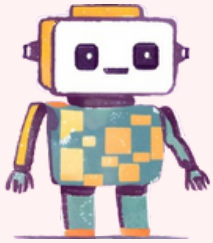
What? No! This can't be fake, it looked so real! Siddharth, Look at this -I shared this news on my profile, and now people are saying it's fake! I don't know what to do, people will make fun of me for this!

Don't worry, this isn't just you Shubham! Some of my other friends faced the same issue recently. It looks like you've fallen into the trap of misinformation. I don't know everything, but maybe we can figure out how to navigate information online together?



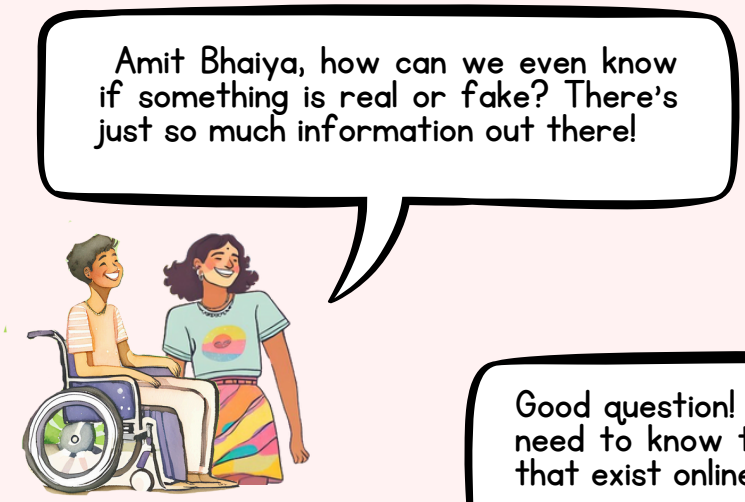
Welcome to Mission NIO: Navigate Information Online. It's time to become a News Navigator!

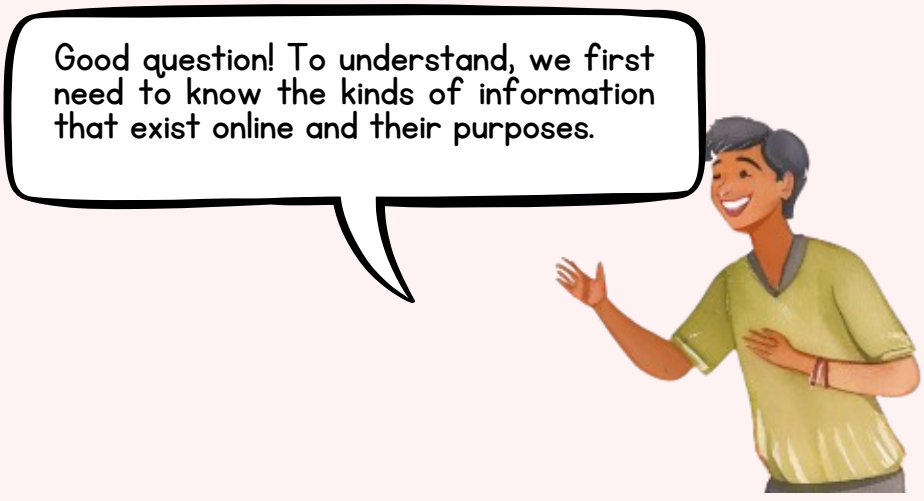
Activity



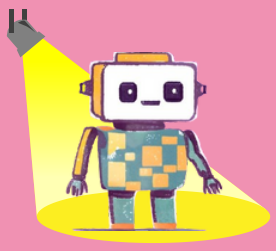
Have you ever shared something online, thinking it was true, only to find out later it wasn't? How did you find out? What would you do differently next time?

Reflect for a moment and jot down your thoughts in the space below.

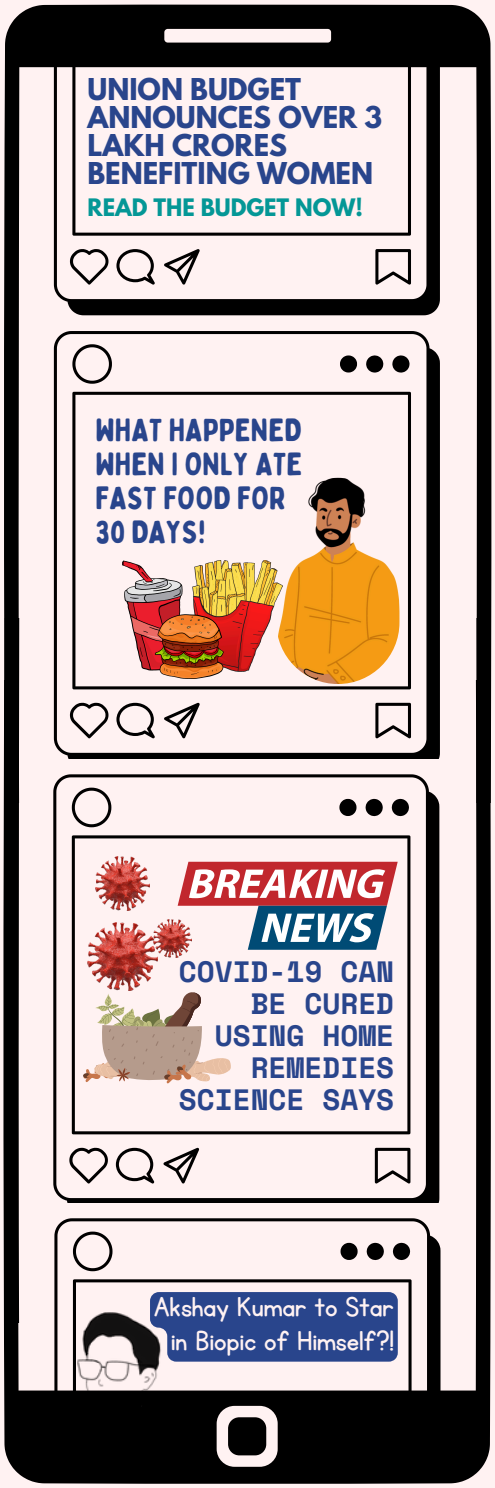




TYPES OF ONLINE INFORMATION



Let me break it down for you! Let's look at your social media newsfeed together, Shubham. Quickly, you'll notice that information online usually belongs to the following categories:



Verified and Credible Information

Some information or news comes from well-known news outlets, research organizations, or government websites. They're usually fact-checked and trustworthy!

Opinion and Personal Content

Such content reflects an individual's perspective - for example, blogs, posts or personal video journals might show someone's daily life, emotions and opinions that may or may not be based on facts.

Misinformation, Disinformation and Fake News

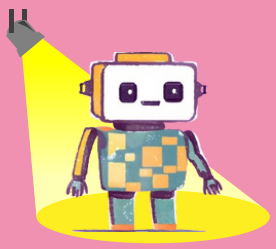
Misinformation, disinformation and fake news are forms of false information. They often contain sensational headlines, emotional language, unclear sources, and a sense of urgency!

Humour and Entertainment

The internet is full of jokes and memes that can be mistaken for news - especially when they comment on real events or issues!

Ohhh... so not everything on the internet is meant to be true or even serious! I think I understand now!

Correct! When you practice, distinguishing between the types, you can navigate the internet smartly!



Let's see a few more posts from Shubham's newsfeed and messages she has received this week. Can you identify what kind of information each is?

Hey Shubham! I just read that scientists have made a advancements in Alzheimer's treatment! Wanted to share since you've been researching for your grandmother.

Inhaled xenon modulates microglia to treat Alzheimer's disease in mice: https://www.science.org/doi/10.1126/scitranslmed.adk3690

>> *Forwarded many times*

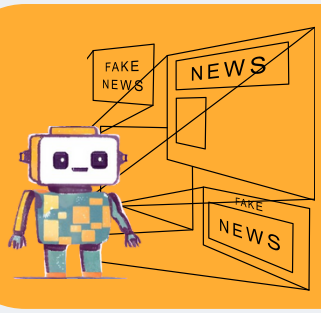
FLIGHT ATTENDANT INSULTS SUNDAR PICHAI IN FIRST-CLASS - THE TRUTH WILL SHOCK YOU!

Read More...

IDENTIFYING MISINFORMATION

Bhaiyya, there's still one problem! In funny posts it is easy to identify false information, but when posts are serious, how do I tell if they're true?

That's a great question. Glitch is an expert at spotting false information, and can show you its types and signs.



SCANNING WORLD WIDE WEB... Information moves through countless channels online–social media, news sites, private messages–and each stop can distort it. Not all false information looks the same, but there are three main types...

1. MISINFORMATION

Unintentionally shared false or misleading information – that is, the sender may not know that the information is wrong.

Just like I shared that fake announcement about exam postponement, by mistake!

The person who made the message could have been trying to mislead students, Shubham!

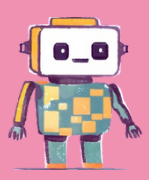
2. DISINFORMATION

Information that is intended to mislead people – usually, for political, financial or social gains.

It looked like it was on a news site – that's why I believed it...

3. FAKE NEWS

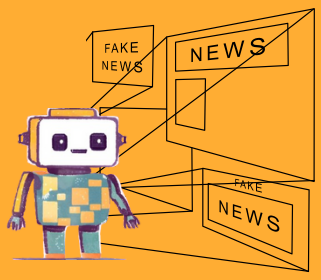
When false information is shared in the form of a news piece – making it look and feel legitimate.



...sometimes the same piece of information can circulate as all three types!

Activity

Write down an example of fake news, disinformation or misinformation that you have come across before. How did you realise it was false? What you already know can be really helpful!



You can verify information/news using a variety of methods. A simple, easy to remember one is the SUCS method, which stands for source, ubiquity, context and second opinion. It will show you what to look out for to make sure that you are trusting only credible information online! Let's look at each step closely and try to verify these two news pieces:

https://economictimes.indiatimes.com/news/budget-2025

Home | Latest News | Market | Economy | Politics | Elections | News Blogs

The Economic Times

Latest Updates to Healthy Ministry Funding

By Dr. Sohini Kumar I Last Updated on 22nd February 2022

NATIONAL HEALTH MISSION
राष्ट्रीय स्वास्थ्य मिशन
Ministry of Health & Family Welfare

New Delhi: As the ruling party gets ready for the up-coming state elections, the health ministry has seen significant funding cuts to its National Health Mission that could turn the tide in 50% of states facing supply shortages in hospitals. The opposition has....

About the author:

Dr. Sohini Kumar is a professor at the School of Economics and Business and has studied Indian Health Systems and politics for over a decade.

Sounds good, let's do it!

What do you think? Do these look true?

http://economicsmadeeeazyl23.biz/india-to-pay-foreign-

EconomicsMadeEasy

INDIA TO PAY-OFF FOREIGN LOANS BY DIPPING HANDS INTO PRIVATE CITIZEN BANK ACCOUNTS!!

India is being pushed into crippling debt by foreign nations and the national treasury is being rapidly depleted. States are low on funds and the only way to recover these costs is to pull directly from citizen bank accounts! Private banks have already announced their withdrawal from this program, but no accounts in state banks are safe from misuse anymore... (Read More)

Image: Foreign Secretary of India shaking hands with New Private Bank owner

SOURCE

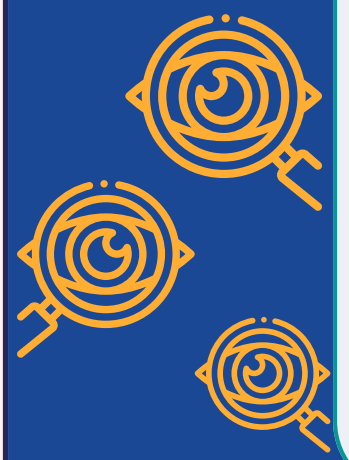
The first step is to check the source of the information or news. Is it credible? Can you trust the source?

Means I should check who posted it? I get news forwarded from trusted friends usually...

I think it's also about the original source - news outlets, research studies or statements. We have to check those too, but how?

Use this checklist. If you tick most of them, the information is likely trustworthy. If you have doubts, don't forward the news!

Always look closely.



CHECKLIST

- ☐ Is the website a well-established news outlet, peer-reviewed journal or a reputed organisation?
- ☐ Is the website known for publishing properly checked accurate information?
- ☐ Is the URL secure (i.e. starts with 'https') and safe, rather than being flagged as unsafe by your browser?
- ☐ Is the webpage clear and well-designed, rather than being full of risky pop-up advertisements, grammatical errors and design inconsistencies?
- ☐ Is the author qualified and/or reliable? Have they studied this topic before and been honest in the past?

LET'S CHECK!

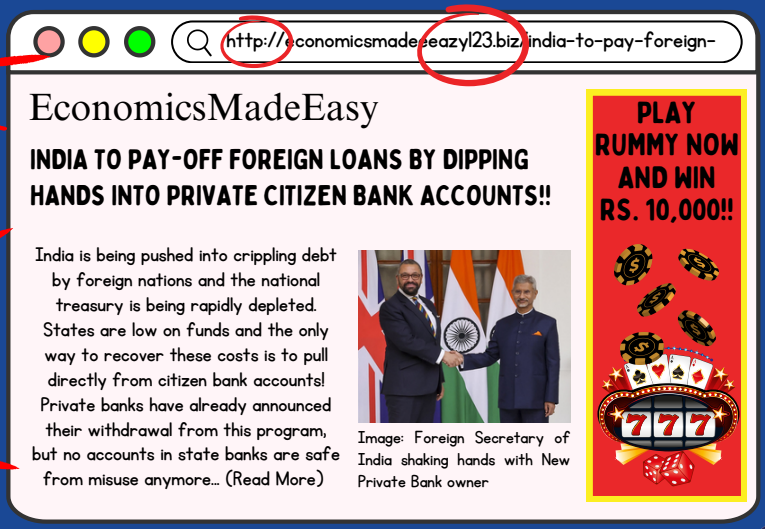
Let's go back to our articles. Are their sources reliable?

The website uses a safe URL starting with https

The Economic Times is a well established news site, known for publishing checked and accurate information

The author is qualified to write about this topic

Overall, the web-page is clear and well-designed, without ads, pop-ups, or grammatical errors



The website URL is unsafe! It starts with http (without an "s"), and has spelling errors and inconsistencies. It ends with .biz too

The website is unreliable and unofficial, and we don't know if it is reliable or accurate!

There is no author!

The website has big pop-ups and ads, and has formatting and grammar issues and inconsistencies!

TIP: TABLOIDS, FLYERS, MESSAGE BOARDS, SOCIAL MEDIA POSTS, BLOGS, AND WEBSITES NOT MANY PEOPLE HAVE HEARD OF ARE UNRELIABLE SOURCES!

Activity

Write down 3 examples of reliable sites, and 3 examples of unreliable sites you have come across.

This is a great tip because now I will pay attention to where I get my news from!

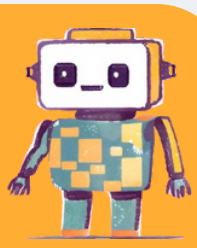
You're on your way to becoming a responsible netizen - but sources are not the end!

UBIQUITY

Ubiquity means something is commonplace or appears everywhere. Is the information unique or can it be verified from different sources? Have multiple credible sources reported it and checked it?

Wait, I don't get this one. Why is this important? Doesn't fake news spread faster sometimes?

It's true: just because many websites have made a claim, doesn't mean it is automatically true. But in some cases - especially, of disinformation - the news is designed to make people panic. Imagine reading these headlines online or in a text:

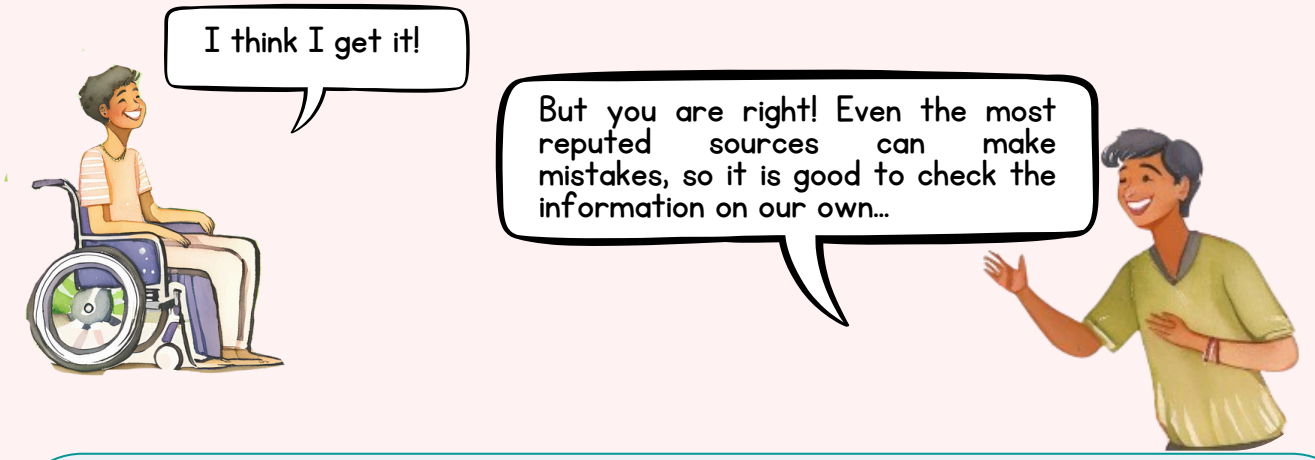


DANGER: 5G Networks Are Responsible for Spreading the COVID-19 Virus Across the Globe!

DEADLY CYANIDE FOUND IN SALT: Stores across India sell poison to homes

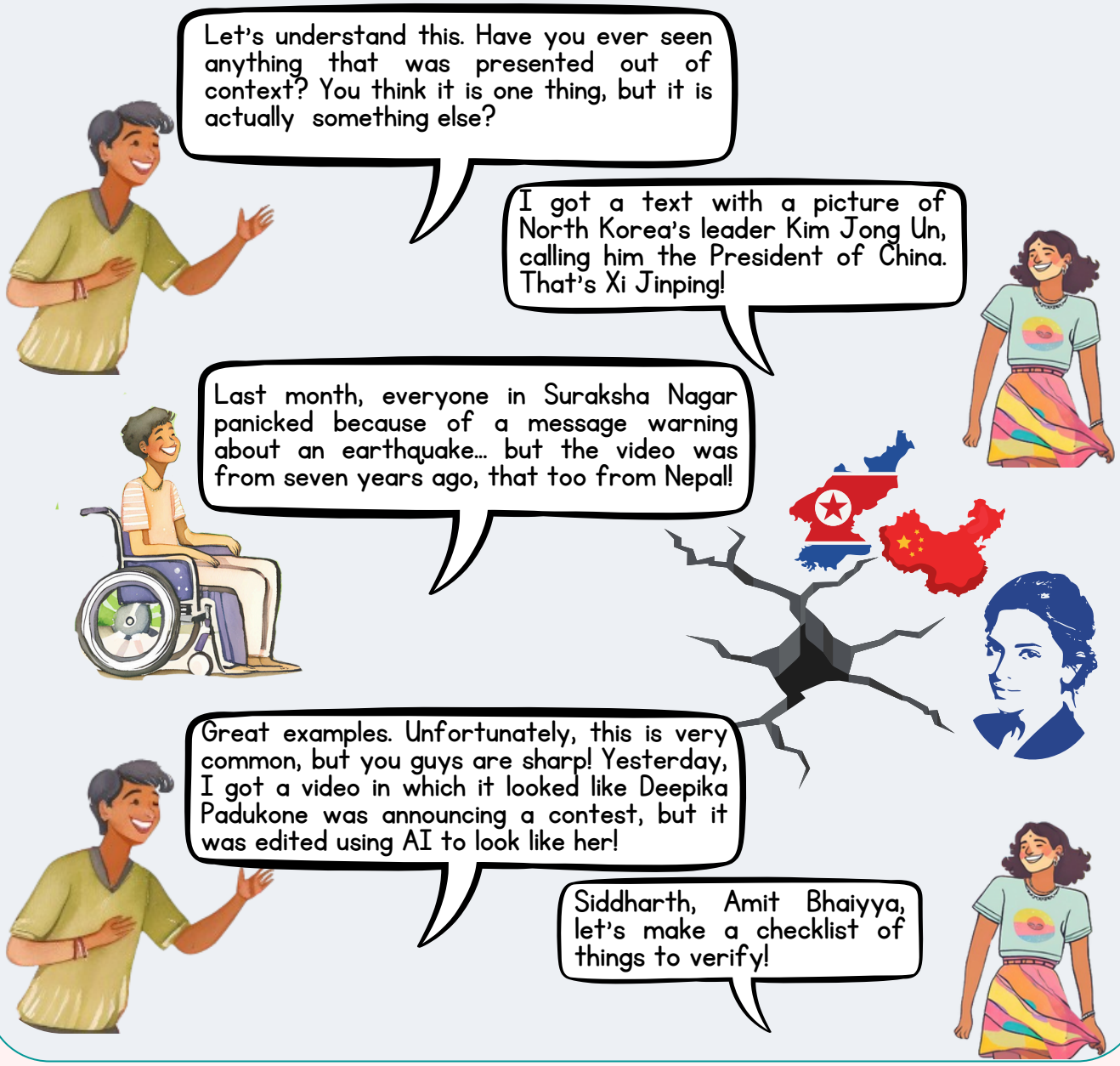
Think about it: if something so dangerous was happening in the entire country, more news sites would cover it. National and international organisations would immediately be investigating this, complaints would be recorded, and official statements would be made...

And if none of this is available, and this piece of news only exists in a few unrecognized places online, it is reasonable to conclude that it might be untrue.



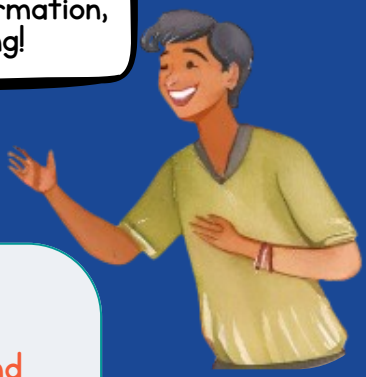
CONTEXT

Independently check whether the context of the information matches the context in which it is being presented.



Good idea!

Let's not forget another important point: we should make sure that the whole story is told, without omitting information, changing the tone or misrepresenting!



CHECKLIST

- [ ] Are the names, places and dates specified and accurate, rather than trying to portray one thing as another?
- [ ] Is the information up-to-date?
- [ ] Is the full context explained, with proof, rather than omitting important information?
- [ ] Are the images and videos of the same people, places or events mentioned in the information?
- [ ] Are images and videos presented accurately, without cropping, editing or altering them to mislead?
- [ ] Does it miss perspectives that can help us understand the situation better?

TIP: EXIT THE SITE YOU ARE ON TO CHECK THE CONTEXT FROM OTHER SOURCES - PREFERABLY, GO TO THE ORIGINAL SOURCE! READ ABOUT THE BROADER TOPIC!

While looking at context, make sure to check if the article, post or message you are looking at provides evidence or proof using links to studies, reports, recordings or documents. Does it show you how the information is known? Is the evidence credible and reliable?

LET'S CHECK!

Let's go back to our articles. Is the information, and the way it is presented, true to its context?

The articles clearly mentions the location and date of the article, providing up to date information

The article has provided context to the issue with with proof, and is also supported by similar information on other sites.

The image matched the text referencing the National Health Mission and the image is an official one without editing or altering

There is no date, place or author!

There is no context about which countries or banks this loan is related to! No other news sites have published this story despite it being such big news!

The image is not used in the correct context or with the right caption! This is a picture of the British Foreign Secretary meeting the Indian External Affairs Minister to start a scheme for young professionals!

https://economictimes.indiatimes.com/news/budget-2025

Home | Latest News | Market | Economy | Politics | Elections | News Blogs

The Economic Times

Latest Updates to Healthy Ministry Funding

By Dr. Sohini Kumar | Last Updated on 22nd February 2022

NATIONAL HEALTH MISSION
राष्ट्रीय स्वास्थ्य मिशन
Ministry of Health & Family Welfare

New Delhi: As the ruling party gets ready for the up-coming state elections, the health ministry has seen significant funding cuts to its National Health Mission that could turn the tide in 50% of states facing supply shortages in hospitals. The opposition has....

About the author:

Dr. Sohini Kumar is a professor at the School of Economics and Business and has studied Indian Health Systems and politics for over a decade.

http://economicsmadeeeazyl23.biz/india-to-pay-foreign-

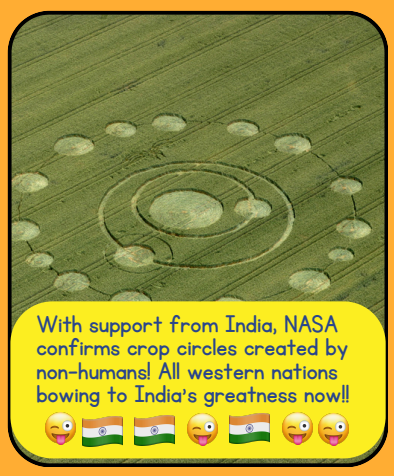
EconomicsMadeEasy

INDIA TO PAY-OFF FOREIGN LOANS BY DIPPING HANDS INTO PRIVATE CITIZEN BANK ACCOUNTS!!

India is being pushed into crippling debt by foreign nations and the national treasury is being rapidly depleted. States are low on funds and the only way to recover these costs is to pull directly from citizen bank accounts! Private banks have already announced their withdrawal from this program, but no accounts in state banks are safe from misuse anymore... (Read More)

Image: Foreign Secretary of India shaking hands with New Private Bank owner

HERE'S MORE NEWS: CAN YOU IDENTIFY WHY THESE ARE MISLEADING?



@citizensforum

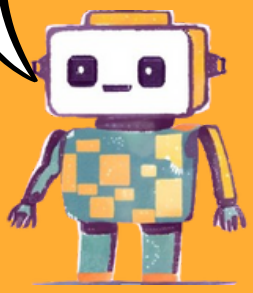
Last 50 COVID-19 vaccines of the day being handed out now at Central Hospital. Experts say no more vaccines to arrive for another week!

SECOND OPINION

If you are still not fully sure you can trust the information, it can always help to get a second opinion - from an expert or an online resource like a fact-checking website.

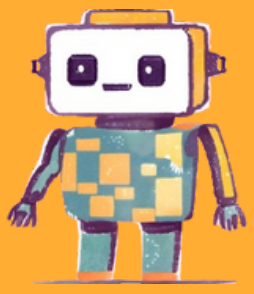
Fact-checking website? What is that?!

Fact-checking websites are dedicated to identifying fake news and misinformation floating around on the internet.



But how do they find out it is fake?

Great question! Each site has its own technique, which they explain on the website. Usually, it involves advanced web search to trace the origin of information...



They also read and watch original sources, and contact local authorities or people featured in the news story to verify... in fact, you can also reach out to experts for a second opinion!

LET'S CHECK!

Let's go back to our articles. What can be some sources of a second opinion for them? Who can you reach out to?

https://economictimes.indiatimes.com/news/budget-2025

Home | Latest News | Market | Economy | Politics | Elections | News Blogs

The Economic Times

Latest Updates to Healthy Ministry Funding

By Dr. Sohini Kumar I Last Updated on 22nd February 2022

New Delhi: As the ruling party gets ready for the up-coming state elections, the health ministry has seen significant funding cuts to its National Health Mission that could turn the tide in 50% of states facing supply shortages in hospitals. The opposition has....

About the author:

Dr. Sohini Kumar is a professor at the School of Economics and Business and has studied Indian Health Systems and politics for over a decade.

Health Ministry Website

Times of India

School Teacher

http://economicsmadeeeazyl23.biz/india-to-pay-foreign-

EconomicsMadeEasy

INDIA TO PAY-OFF FOREIGN LOANS BY DIPPING HANDS INTO PRIVATE CITIZEN BANK ACCOUNTS!!

India is being pushed into crippling debt by foreign nations and the national treasury is being rapidly depleted. States are low on funds and the only way to recover these costs is to pull directly from citizen bank accounts! Private banks have already announced their withdrawal from this program, but no accounts in state banks are safe from misuse anymore... (Read More)

Image: Foreign Secretary of India shaking hands with New Private Bank owner

LOOK FOR 3 TRUSTWORTHY FACT-CHECKING WEBSITES. SHARE THEIR NAMES, URLS AND VERIFICATION PROCESS:

Remember, misinformation can have a heavy cost: it can impact people's physical safety, mental health, relationships between people or communities and dignity.

The SUCS method is so helpful... but I feel so stupid and guilty for believing and spreading false information. I can't get over my mistake...

No one is always successful at identifying misinformation, that's why it is so prevalent! The point is to keep improving our ability to check information, and change our mind when we find out the truth!

Amit Bhaiyya, I am so anxious though! I get so many messages. How will I keep up and fact check everything? That will take all day!

Hmmm... it's good to be aware of what we feel on the internet. I am also really overwhelmed online, most days...

Here are some ways I try to be a responsible consumer of information, without feeling lost!

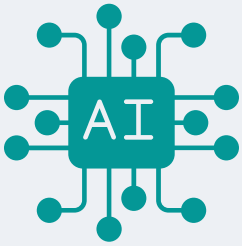
- Setting fixed times to read news from reliable sources
- Remembering that over time, verification will come more naturally!
- Getting a fact-checking buddy so you can keep practising together and correcting each other!
- Taking time to process information and making up your mind, but don't forward until you're sure of its accuracy!

HOW DO MISINFORMATION AND DISINFORMATION SPREAD?

It is also important to understand the reasons behind the easy spread of misinformation. The problem is bigger than all of us!

CLICKBAIT AND SENSATIONALISM

Content may be designed to tempt us to click – it may be written in a dramatic, exaggerated way, to make you afraid, excited or curious.



DEEPFAKES AND DOCTORED CONTENT

Photos and videos are heavily edited to look real and deceive people – sometimes, they lead to fraud or set unrealistic expectations about how people should look.

CONFIRMATION BIAS

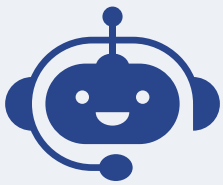
We tend to believe information that fits in with our existing opinions more easily than information that clashes with our current views. So, we may forward fake news if we agree with the opinion presented in it!

INCREASING POLARIZATION

Internet arguments can be very heated, because there is a growing divide between disagreeing parties. People may feel encouraged to create or share false information in such an environment.

CREDIBILITY BIAS

We trust the information shared by people we trust – for example, a teacher, relative or friend we agree with – more easily than information shared by people we do not trust. It can land us in trouble because we check the person rather than the news!



SOCIAL PROOFING, BOTS AND FAKE PROFILES

Social proofing means that we tend to believe information that is popular, that others around us also trust. Increasingly, bots and fake profiles are used to make posts appear popular – so that we trust them!

BEING RESPONSIBLE AND CRITICAL ONLINE

WHAT DO YOU THINK WE CAN DO TO CREATE A MISINFORMATION-FREE INTERNET?

Amit Bhaiyya, I had no idea the world of misinformation was so complex!

Yeah! I also end up reading so much and learning new things on the internet while verifying information...

That's so amazing! It feels like now we finally get to be less lost and discover what we think, what our opinions are...

Remember, critical thinking is not just about staying away from what's wrong. It's also being able to differentiate between facts and opinions, making up our minds carefully... Glitch will explain!

Often, information you gather online is a mix of facts and opinions. Distinguishing between the two parts in any piece of information can be helpful in your critical thinking journey!

Facts

It is raining outside!

- Can be verified
- Based on observation or research
- Cannot be disputed

VS

Opinions

Rain makes everything sad!

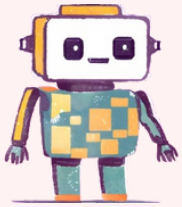
- A belief/view, can't be verified, can be discussed
- May contain biases and ideas about good/bad
- Shares how someone feels about a fact

Opinions are a way of interpreting the world and how you feel in it. They may be supported by facts. Opinions can be discussed, debated and explored. However, if they go against facts, they lose validity.

So along with making sure the sources are credible and the facts are straight, we need to pay attention to how the facts and opinions are connected, right?

I think that sums it up nicely! Thanks, Bhaiyya!

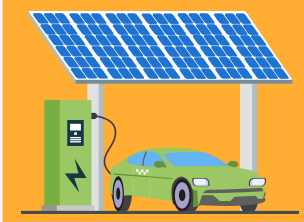
Activity



Can you circle the facts and underline the opinions in the following pieces of information? While doing so, reflect on whether the opinions are based on facts, and whether you agree with them. You can also read more about the topic and see if you change your mind!

Strawberries are a fruit that contains vitamin C, and they are the tastiest fruit of all.

The Qutub Minar is located in New Delhi but it's not as beautiful as other monuments in the city.



Electric cars produce fewer emissions than gas-powered vehicles, making them the obvious choice for everyone who cares about the environment.

Spending money on space exploration may be wasteful, but it has led to incredible technological advances!

Fast food contains high levels of sugar and fat, which is why it's a leading cause of obesity worldwide.

Reading every day can help improve focus and vocabulary, though some believe audiobooks are just as effective. Personally, nothing beats the feeling of holding a real book in your hands

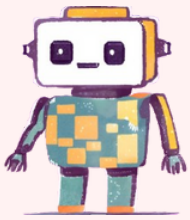
Social media algorithms prioritize content that keeps users engaged, which shows they are designed to manipulate our behavior

WHAT ARE ALGORITHMS?

It was a hot and humid day after heavy rains, and Shubham was sitting under a tree, enjoying her ice cream. Shubham takes out her phone to read through the news, feeling more confident about identifying fake news. As she scrolls, she notices something odd.

Hmm, this is strange. I know there was a big thunderstorm yesterday, but I don't see anything about it online. My newsfeed is filled with recommendations about cafes instead!

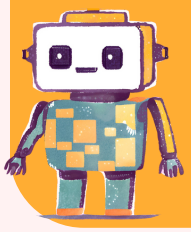
That's because algorithms show you what they think you like based on your activity. If you have recently searched for cafes around you, the algorithm will show you more of that!



Remember how we compared the internet to a railway system in "Hello Digital World"? Algorithms work just like station managers on trains! Imagine you're taking a train, and every time you get to a station, the station master notices where you go. If you keep taking the same train to places like Orissa or Bengal, the station master will start to think you like exploring East Indian tourism. Next time, they will suggest more trains to those same places because they think that's where you enjoy traveling.

Similarly, when you use the internet, algorithms watch what you do - like what videos you watch, the pages you visit, or the things you search for. If you keep searching for videos about cooking, the algorithm assumes you love cooking and recommends recipes and food tips.

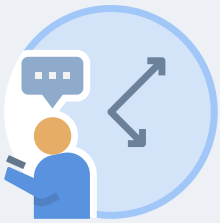
Algorithms monitor your online actions, such as what you like, comment on, or share. These interactions signal your interests and help platforms tailor your feed. If you like posts about gaming, the algorithm will show more gaming content, ads, and pages.

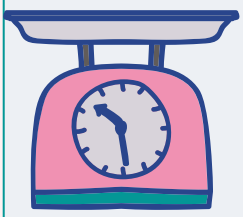


The type of content you consume–whether videos, articles, or pictures–also influences recommendations. Algorithms prioritize the formats you engage with most often.

HOW DO ALGORITHMS WORK?

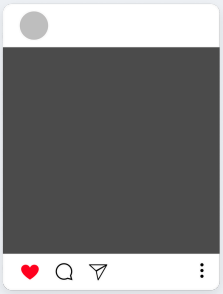
The time you spend on certain topics tells algorithms what you find most engaging. The longer you engage with specific content, the more similar posts you'll see.





Another important component of algorithms is content weighting, which assigns a score to different types of posts and activities. Videos uploaded directly to platforms are given higher priority than links to external sites like. Links from high-quality sources are also weighted more favorably.

Posts lose prominence as they age. Newer posts and recent interactions with a page increase the chances of its content appearing in your feed. If you haven't engaged with a page for a while, its posts might show up less frequently, even if they're new.

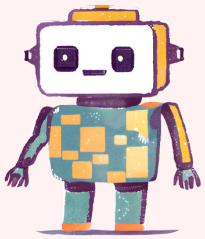


Remember! Algorithms prioritize what grabs attention, not what's truly important. They often promote popular content, like flashy headlines or viral videos, even if it's not always accurate or reliable. This means the most engaging content isn't necessarily the most trustworthy.

While algorithms personalize your online experience, they can also trap you in a Filter Bubble–a space where you only see content that aligns with your existing interests. This limits your exposure to new ideas and perspectives. To break out of the bubble, explore different topics and engage with diverse content–you never know what exciting discoveries you might find!

HOW DO ALGORITHMS WORK?

Algorithms don't just shape the content you see, they also decide which ads pop up while you're browsing. Advertisers use your online behavior such as search history, clicks, and even your location to deliver ads designed specifically for you. Let's break it down step by step:



Ad Targeting

Once advertisers collect your data, they analyze it to understand what you might like. Advertisers use demographic data like age, location, and preferences to show ads relevant to specific groups.

Ad Personalization

Using the data they've collected, companies create a profile of your interests and habits. They predict what kinds of ads you'll click on and show you ads they think are most relevant. This is why, after looking at new phones online, you might suddenly see ads for phone cases, chargers, or earphones.

You can take steps to reduce the amount of data advertisers collect and regain control over your online experience. Here's how you can decide what to share and what to keep private!

Review Privacy Settings

Adjust settings to disable location tracking or personalized ads.

Clear Cookies and Cache

Regularly delete cookies to reset the data advertisers use.

Use Ad Blockers

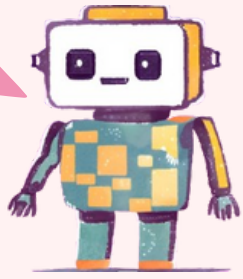
Block ads and prevent trackers from collecting your data.

Opt-Out of Personalized Ads

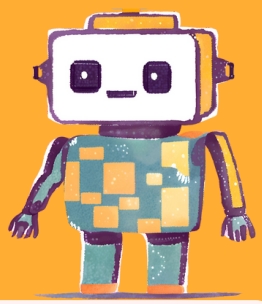
Opt-out of ads based on your activity. You'll still see ads, but they won't be tailored to your browsing history.

Wow algorithms are cool but kind of scary! No wonder my video suggestions keep changing. Do they also decide ads? I looked for shoes once, now that's all I see!

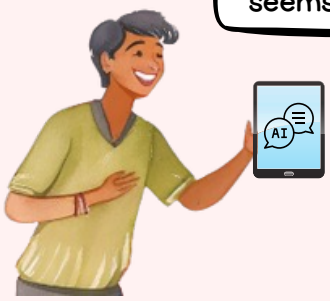
Correct! That's targeted advertising, another way algorithms use your data!



Write down three types of content you see most often on your newsfeed. Are these topics truly what you're interested in, or do you think algorithms have created a bubble for you? Share your thoughts with a friend or classmate.



WHAT IS ARTIFICIAL INTELLIGENCE?



Hey, folks! Have you heard about this AI chatbot? It seems to know everything!

Oh, yes! We learned about it together when were reading about technology and our lives online. AI, or Artificial Intelligence, refers to computer systems which can mimic human intelligence. For instance, chatbots can answer questions, search engines recommend websites, and image recognition tools identify objects in photos.

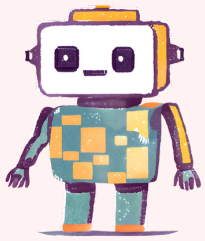
That's fascinating! Did you understand how it works?

Yes! AI processes big amounts of information to identify patterns and make predictions. For example, if I asked an AI chatbot a question, it will understand my question, analyse it, search its database for the most relevant information, and provides an answer–all in seconds, like a super-smart assistant!

But remember, AI doesn't actually think like humans. It simply follows its training data. It can be incredibly helpful, but it's important to understand its strengths and weaknesses. Glitch can help you with that!

HOW DOES AI WORK?

Artificial Intelligence, is like having an assistant that can help you complete tasks faster, solve problems, and even make learning more enjoyable. While it doesn't think or feel like a human, AI can still be very helpful in many areas of your daily life. Let's look at some of the ways AI can assist you:



Fast Access to Data

AI can analyze large amounts of information in just seconds. This makes AI especially useful for research and learning.

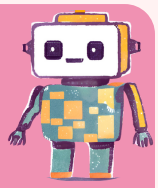
Brainstorming Ideas

Ever felt stuck when you're trying to come up with ideas? AI can help by suggesting creative options for projects. It's like having a study partner!

Language Translation

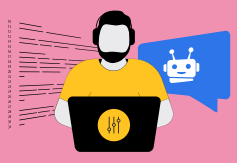
AI tools can break language barriers, making it easier to communicate with people from around the world or understand content in other languages.

While AI can be incredibly helpful, it's not perfect. There are some challenges to be aware of when using it:



Bias in AI

AI learns from data, and if the data it's trained on is unfair or incomplete, the AI might give biased results. This means it could make mistakes or favor certain opinions.



EXAMPLE

If an AI tool is trained mostly on Western media, it might struggle to understand cultural references from other parts of the world, including India.

False Information

AI can often make up information that sounds real but isn't true. Sometimes it predicts answers based on patterns, not actual facts.

EXAMPLE

You ask an AI tool about a historical figure, and it confidently gives you a fake quote or event that never happened.

Privacy Concerns

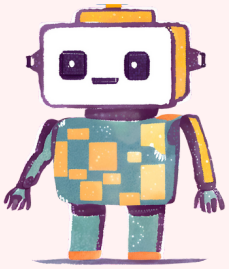
Many AI tools collect and analyze data to learn and improve. While this helps make AI smarter, it raises privacy concerns over personal information.

EXAMPLE

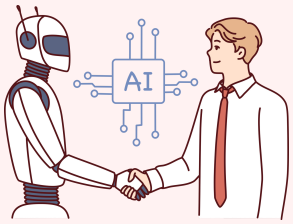
If an app asks for your location, it's important to think about why it needs that information and whether you want to share it.

GLITCH'S GUIDE TO USING AI

Feeling overwhelmed? I understand! It's a lot and can be confusing. Here are some simple tips to help you use AI responsibly



Partner with AI, Don't Depend on It



AI can be a great assistant, but it's not a replacement for your own ideas, creativity and critical thinking. It can be a tool brainstorm or get suggestions, but it can't replace your own thinking and creativity.

Always Fact-Check

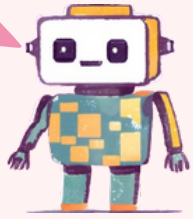
AI isn't perfect and can often give incorrect information. Always verify what it tells you by checking reliable sources like books, trusted websites, or even asking a teacher.

Understand Its Limits

AI is very smart but doesn't think exactly like humans. It can't understand emotions or cultural contexts the way people do. Treat it as a tool, not an expert!

So I should use AI as a starting point, not the final answer?

Exactly! Think of it as an assistant that makes your work easier but doesn't replace your critical thinking.



Activity

If you have access to the internet

Split up into pairs. Now, one of you should use the AI tool and the other person can use the traditional research methods. Research any topic of your liking. Afterwards, compare the results for accuracy, completeness, and reliability!

If you do not have access to the internet

Rewrite an AI-generated response. Add more context, examples, and your own ideas to make the answer generated richer and more accurate.

CHAPTER RECAP!

-  Online information can often be catagorised as: verified and credible information, opinion and personal content, misinformation, disinformation and fake news, or humour and entertainment!
-  Misinformation is usually unintentionally shared misleading or false information, while disinformation is intended to mislead people.
-  You can verify information using a simple method - SUCS (source, ubiquity, context, second opinion)
    - Source: is the website reliable and well-known? Is the URL secure? Is the page design good, or is it full of popups?
    - Ubiquity: is the information commonplace and verifiable from other sources?
    - Context: are the names, dates and places accurate? Is it up to date with full context? Do the images match the information?
    - Be careful between facts and opinions when sharing information!
-  Remember: algorithms prioritise and promote what grabs attention, not necessarily what is accurate or important!
-  Review privacy settings, clear cookies and cache, use ad blockers and disable personalised ads to reduce the information shared with ad agencies!
- 

AI is extremely helpful, but can also promote fake information, carry encoded biases, and has privacy concerns! Remember to fact check AI, understand its limits and use it to support, not complete, your work!

Chapter 5: Not Today, Scammers! Spotting and Stopping Online Threats

Its a sunny day, and Jaspreet and Noor are at Jaspreet's house, planting some new seeds together!

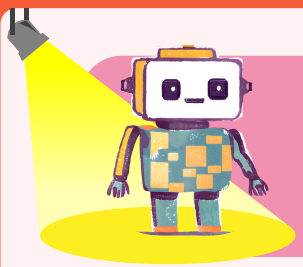
Yesterday I was spending some time with Shubham, and she was telling me about algorithms, AI and a bunch of other cool stuff that she figured out with Siddharth and Amit Bhaiya! It sounded interesting, but it did make me think about how much is out there that we don't know about...

That's true! The internet is fascinating, but it can also be daunting to navigate when we don't know if it's safe or reliable.

I think it would be really helpful for all of us if we had a go-to place to quickly learn how to deal with scary and unwanted interactions on the internet. What do you think?

That's a brilliant idea. I think Glitch could help us with something like this!

I absolutely can! Let's go on an adventure! Welcome to Glitch's Guide to Internet Safety!



GLITCH'S GUIDE TO ~~THE GALAXY!~~ INTERNET SAFETY!

How do you identify threats sent to you on personal channels of communication? Here is a checklist of red flags to look out for!

- Did they ask for personal information or sensitive information (eg: age, address, phone number, school, bank account).
- Did they demand private photos/videos, especially in a casual, friendly conversation?
- Did they ask you to keep your conversations or actions a secret from others?
- Did they try to become your close friends very quickly, offering compliments or gifts?
- Did they send abusive/hurtful messages that made you feel unsafe or guilty?
- Did they make grand promises or offers (eg: lottery, job opportunity)?

Some safety measures to prevent threats and unsafe situations!

- Create strong passwords with a mix of letters, numbers, and special characters.
- Enable 2-factor authentication
- Make sure your profile's visibility is set to your preference - public or private!
- Avoid sharing personal information like your full name, address, phone number, or school name on public platforms.
- Only share sensitive details (e.g., bank information) on encrypted platforms.
- Install an antivirus software and make sure your device's firewall is turned on
- Always check URLs carefully. Scammers may use links like 'amazOn.com' instead of 'amazon.com' to trick you.
- Don't click on unknown links in emails or messages
- Regularly monitor your accounts to check for unusual activity
- Avoid allowing any app access to too much information. Disable unnecessary permissions and be cautious with apps that request excessive permissions
- Use ad blockers to prevent pop-ups, banners, and video ads and protect against malware
- Avoid using public wifi and keep your Bluetooth off when not in use
- Save copies of important files or photos on an external hard drive!

CASE STUDY: THE BLUE WHALE CHALLENGE

In 2016, an online trend called the Blue Whale Challenge spread across social media and private messaging platforms. It was not a typical game–it was a form of online manipulation that targeted teenagers, tricking them into performing harmful tasks over 50 days. It is now recognized as an example of how online threats, harassment, and scams can lead to real-world harm.

At first, the challenge spread as invitations from strangers - message recipients were told they had been "chosen" for an elite game, creating curiosity and excitement. In order to continue, they had to follow instructions from an anonymous "curator" or "game master" who assigned daily tasks. Initially, most of the tasks seemed harmless–drawing a whale, watching a scary movie, or waking up at odd hours. But over time, participants were asked to take dangerous risks or isolate themselves from family and friends! Some of the means used to pressure and control participants included:

- Privacy Invasion & Blackmail - The game tricked participants into sharing personal information, like their full name, address, or private photos. Later, it used this information to threaten them. Messages like "We know where you live" or "If you leave, we will harm your family" were used to scare participants into staying in the challenge. Fake promises were also made.
- Online Harassment & Bullying - When a participant expressed the desire to quit, they received multiple aggressive messages, calling them weak or a failure. Players were also added to fake online communities where participants felt pressured to impress or prove their bravery.
- Hacking & Tracking - Some players believed their devices had been hacked, with their screens flashing warnings that they were being watched, making players feel trapped.

The Blue Whale Challenge is no longer as widespread, but new online threats continue to emerge. Staying informed, recognizing manipulation tactics, and reaching out for help can keep you and others safe in the digital world.

Activity

List down 3 tangible things someone could do to prevent becoming a victim of a threat or scam like the Blue Whale Challenge:

1. Never share personal information with strangers online. No real game or challenge should require private details.
2. Watch out for red flags like secrecy, threats, or pressure. If someone online asks you to keep something a secret, isolate yourself, or do anything that feels wrong–block and report them.
3. If something online makes you uncomfortable, talk to someone you trust. No challenge, trend, or game is worth your safety! You are never truly alone, and help is always available!

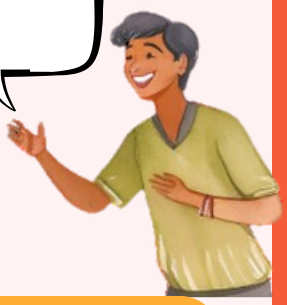
REPORTING HARMFUL CONTENT ON ONLINE PLATFORMS

This is a great reference for anyone who wants a quick guide to protecting themselves against threats! Good Job, Jaspreet and Noor!

Thank you Amit Bhaiya!
I still have a question. Let's say we follow all of these steps carefully, but we still receive messages or content that seem unsafe. What can we do in that situation?

Oh, I was watching a video on this yesterday! I found out that most apps and platforms have reporting and blocking features that we can use.

That's right, Jaspreet! Most online platforms and messaging apps have built-in tools to report harmful content like harassment, threats, impersonation, and misinformation. Reporting is important, because it helps keep you and others around you safe!



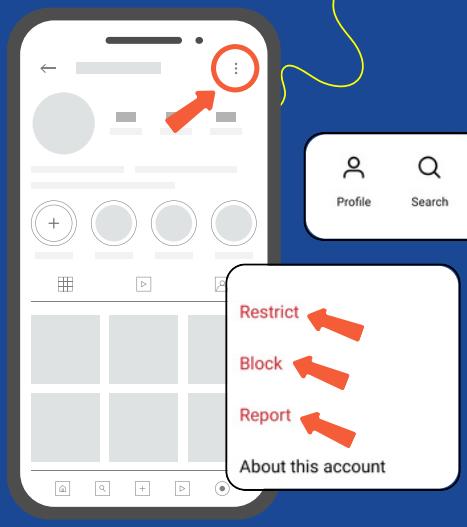
Reporting such content or messages helps platforms take action against offenders, protects yourself and others from online abuse, and prevents harmful content from spreading. Reporting doesn't always result in immediate action, but repeated reports from multiple users can increase the chances of a platform addressing the issue.

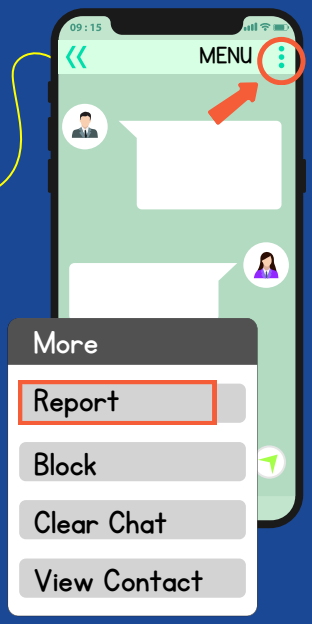
How to Report and Block Harmful Content on Online Platforms

On most platforms, it's pretty easy to report harmful content or chats. Here are some simple steps you can follow (remember these might vary based on the platform you are using, so ask a trusted adult or friend if you are unsure):

1. Take a screenshot of the chat or content before reporting, in case further action is needed. Press a combination of the power/home button and volume button to take a screenshot on your phone (this changes based on model)

2. Click on the menu option.
Select "Report", "More" or "Find support" from the menu.
Choose the most relevant category (e.g., harassment, false information, impersonation, hate speech etc.).





Many messaging platforms also have an option to "BLOCK & REPORT", rather than just reporting. This will prevent the person from contacting you again!

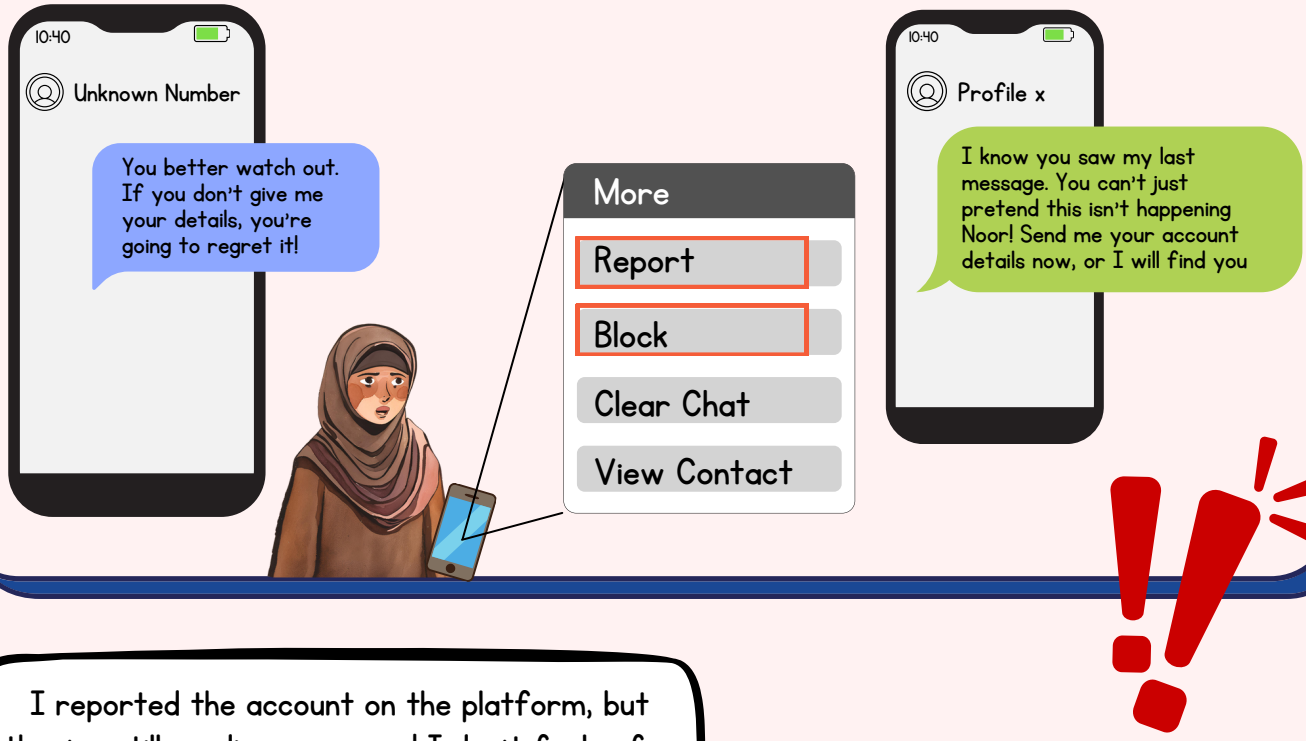
If you want to report a fake account or profile (someone who is impersonating you or someone else you know), you can similarly find the menu or more information button, and click "report profile".

If you want to report a specific chat or message, you should press and hold the message or check the conversation settings to find the report option (it might be under "more" settings)

3. Submit the report and follow any additional instructions.
After you report content or a chat, the platform might decide to remove it, restrict the account, or issue warnings. Some platforms will give you updates on your report, while others may not.

REPORTING CYBER CRIMES

Noor receives a threatening message on her phone. She feels scared and reports and blocks the message on the platform! But within 5 minutes, she receives another message from the same profile through a different platform

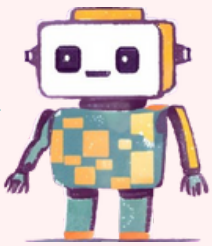


I reported the account on the platform, but they're still sending messages! I don't feel safe... What else can I do?

If it's serious, I think we should report it to the Cyber Crime Cell. I've heard they handle online threats, harassment, and digital fraud. Right, Amit Bhaiya?

That's right! Glitch, can you walk us through some important helplines?

Sure Amit Bhaiya!
You can report cybercrimes at cybercrime.gov.in or call 1930 for immediate help. And if the threat is gender-based, you can also contact the National Commission for Women (NCW) helpline at 7827-170-170. They provide support for cases of online harassment, blackmail, and abuse.



Government Helplines to Report a Cyber Crime

If you or someone you know is facing online abuse, threats, blackmail, or harassment, take action by reporting it.

Cyber Crime Cell (National Cyber Crime Reporting Portal)

- Website: cybercrime.gov.in
- Helpline: 1930
- Reports cyberstalking, online threats, identity theft, hacking, and more.

National Commission for Women (NCW)

- Website: ncw.nic.in
- Helpline: 7827-170-170
- Focuses on crimes targeting women, including online harassment and abuse.

Local Police Station

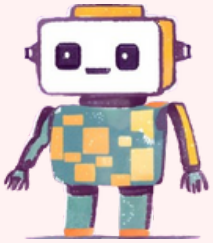
- Phone Number: 100
- Cybercrime cases can also be reported at your nearest police station.
- You can also file a First Information Report (FIR).

Childline India (For Cyber Safety of Children)

- Website: childlineindia.org
- Helpline: 1098
- Handles online threats, cyberbullying, and other digital crimes against children.

This is a really helpful list to have on me, thanks Glitch! Let's say that I call one of these numbers or go to their website. How would I file the complaint and what information would I need to have?

There are a couple of things to keep in mind. Let's take a look!



Step 1: Collect Evidence

- Take screenshots of the threats/messages or save the URL
- Note down their timestamps and the number or ID that sent the messages to you

Step 2: File a Complaint

- Go to cybercrime.gov.in and submit a report. This can be anonymous if you prefer
- In case you are unable to submit the report or call the helpline, visit your nearest police station to file an FIR

Step 3: Follow Up

Keep track of your complaint status and if necessary, seek help from NGOs, legal experts, or support organizations.

Activity: Let's See What You Remember!

1. When reporting a cybercrime in India, what type of evidence is most helpful to authorities?
a) Physical copies of any documents related to the crime
b) Screenshots, email exchanges, and digital copies of the fraudulent content
c) A verbal description of the incident during a phone call
d) A signed affidavit from the victim's relatives confirming the crime

2. True or False: To report a cybercrime in India, it's necessary to physically visit the police station.
a) True
b) False

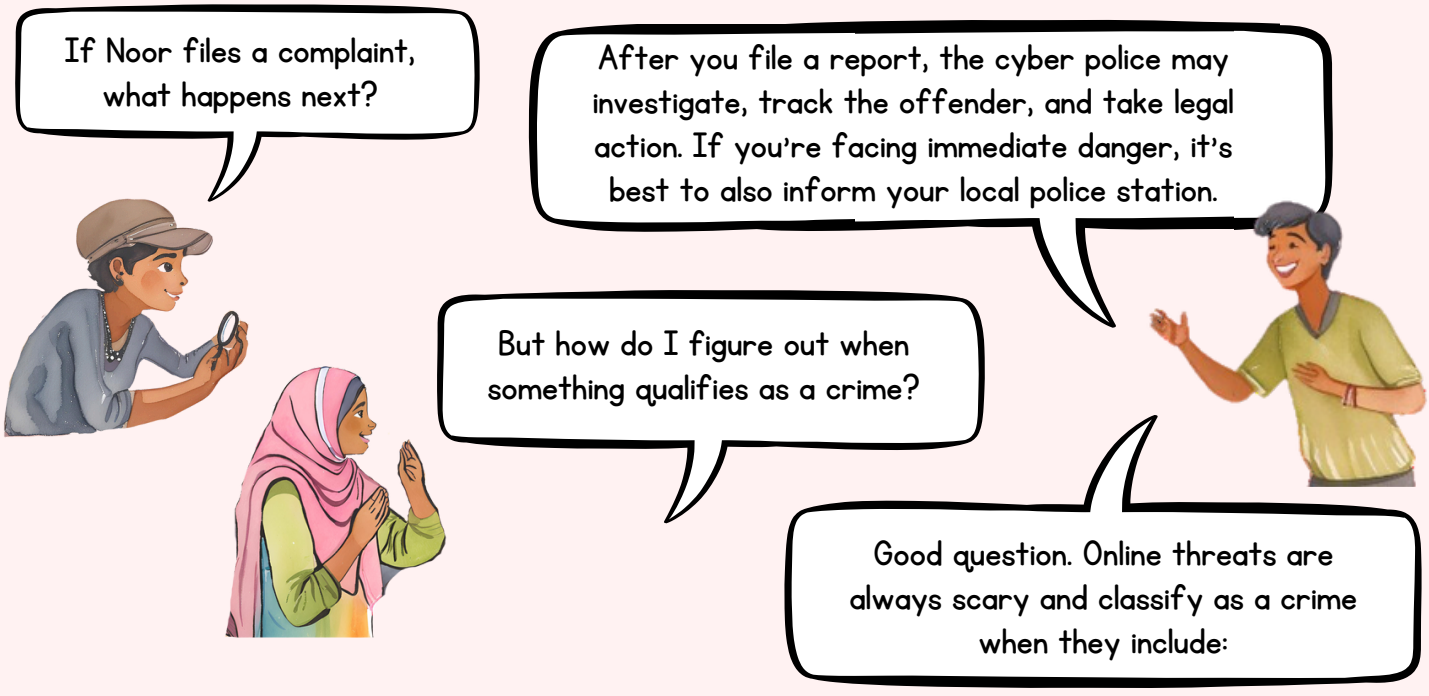
3. What is the helpline number for reporting cybercrimes in India?
a) 100
b) 112
c) 1930
d) 1098

Activity, Continued

4. Your friend tells you they are being cyber-stalked by an unknown person who keeps messaging them and tracking their online activity. What should they do first?
a) Block and report the stalker on the app
b) Reply to the stalker and demand that they stop
c) Deactivate social media accounts immediately and turn off location
d) Ignore the situation so that the stalker loses interest

5. Which of the following actions poses the greatest risk to your cybersecurity?
a) Using the same strong password across multiple important accounts
b) Connecting to public Wi-Fi and logging into sensitive accounts
c) Enabling two-factor authentication (2FA) on important accounts
d) Keeping Bluetooth and location services enabled only when actively using them

6. When is it okay to reach out for help from an adult?
a) You feel uncomfortable or unsafe because of an online message
b) You have been asked to keep your conversations and actions a secret from others
c) You receive an offer for a huge cash prize from a new friend online
d) All of the above



- Threats of violence or harm
- Sexual harassment or stalking
- Sharing private images without consent
- Impersonation, fraud, or identity theft

LAWS FOR OUR PROTECTION

The internet is a powerful space where we connect, learn, and share, but just like in the real world, there are laws to protect us from harm. If someone steals from you, threatens you, or invades your privacy, they can be punished under Indian law. even if the crime happens online!

Information Technology (IT) Act, 2000

The IT Act is India's main cyber law, protecting people from hacking, identity theft, online harassment, and privacy violations.

Data Theft (Section 43)

If someone hacks into your device or steals your data without permission, they can be fined up to ₹1 crore.

Identity Theft (Section 66C)

Creating a fake social media profile using someone else's name or photos is illegal with a penalty up to 3 years in jail + ₹1 lakh fine.

Violation of Privacy (Section 66E)

Sharing private pictures or videos without consent is a crime., with a penalty of up to 3 years in jail + ₹2 lakh fine.

Hacking (Section 66)

Illegally accessing, damaging, or locking someone's computer or social media is punishable with up to 3 years in jail + ₹5 lakh fine.

Indian Penal Code (IPC), 1860

Cyber Extortion (Section 384)

If someone threatens to leak your private chats or photos unless you pay them, they can be punished under cyber extortion laws.

Online Stalking & Harassment (Section 354D)

Repeatedly messaging, tracking, or harassing someone online, even after being blocked, is illegal.

Anonymous Threats (Section 507)

If someone sends threats while hiding their identity, whether through fake social media accounts, anonymous emails, or messaging apps, they can be punished under this law.

LAWS FOR OUR PROTECTION

Consumer Protection Act, 2019

This law protects consumers from online fraud, scams, and unfair business practices. If an online shopping website refuses to refund a defective product, you can file a complaint under this act.

Activity: Match the Laws!

Below are five different online crimes and five laws designed to protect against them. Match each crime to the correct law!

A private photo is leaked without consent	Hacking
Someone hacks into your computer and deletes files	Consumer Protection Act
A company refuses to refund you for a faulty product	Identity Theft
A stranger keeps sending threats from fake accounts	Violation of Privacy
Someone creates a fake profile pretending to be you	Anonymous Threats

I had no idea there were so many laws protecting us online! But what if I don't know which law applies to a situation?

That makes sense. So, if someone is stalking me online, I don't need to memorize Section 354D–I just need to report it and seek help?

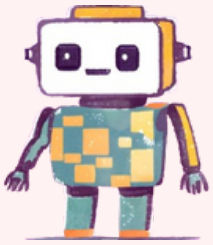
That's okay! The important thing is knowing when something feels wrong and reporting it to a trusted adult or the authorities. You don't have to know every law, but being aware of your rights helps!

Exactly! And if you ever feel unsure, you can always look up these laws or ask for guidance. Help is always available!

FINDING HELP & SUPPORTING OTHERS ONLINE

The internet can be a great place to connect, learn, and have fun–but what happens when things go wrong? If you ever feel unsafe, overwhelmed, or simply need someone to talk to, help is just a call away.

There are trusted helplines, counselors, and organizations ready to support you, whether you're dealing with online harassment, bullying, distress, or mental health struggles. Knowing where to seek help and how to support others is an essential part of staying safe online.



Childline India Foundation
Focused on: Bullying, harassment, emotional support
1098 (Toll-Free)

NCPCR (National Commission for Protection of Child Rights)
Focused on: Child rights violations, bullying, harassment
1800-121-2830 (Toll-Free)

Women Helpline WHL (Nirbhaya Fund, Ministry of Women and Child Development
Focused on: Online harassment, safety concerns
181 (Toll-Free)

NCW (National Commission for Women)
Focused on: Online sexual harassment, women's rights
011-26942369 / 26944754

AASRA Helpline
Focused on: Suicide prevention, emotional distress support
91-9820466726

iCALL
Focused on: Confidential emotional counseling, mental health support
022-25521111 (Monday to Saturday, 8 AM - 10 PM)

MANAS Foundation
Focused on: Mental health support, counseling for distress and bullying
+91 97117 00069

Bachpan Bachao Andolan
Focused on: Missing children, child labor, trafficking, abuse
1800-102-7222 (Toll-Free, 24/7)

EMOTIONAL FIRST AID: CALMING YOURSELF IN DISTRESS

These helplines are really useful! But Noor, what if I start feeling panicked in the moment? Do you have any tips to help me calm down? I think I get so caught up in trying to fix things that I forget how I'm feeling matters.

I get what you mean! When something stressful happens online, like bullying or even an argument, it's easy to react without thinking. But taking a second to pause and manage your emotions first can really help. Let me show you a few simple tricks that might make a difference!

Quick Ways to Calm Yourself: Try these techniques when you feel overwhelmed!

5-4-3-2-1 Grounding Exercise

Look around you. Identify:

- 5 things you can see
- 4 things you can touch
- 3 things you can hear
- 2 things you can smell
- 1 thing you can taste

Journaling Your Thoughts

Write down what happened, how it made you feel, and what steps you can take next.

Putting your thoughts on paper helps you process emotions, gain clarity, and make informed decisions before reacting.

Visualization & Deep Breathing

First, close your eyes and picture a calm, safe place—a space where you feel completely at ease. It could be a quiet park, a cozy room, or the peaceful mountains. Your safe place is anywhere that makes you feel secure, relaxed, and in control.

Now, Take slow, deep breaths, focusing on the sights, sounds, and feelings of that space. Let yourself fully experience this moment.

Activity: Design Your Personal Calm Plan

What is one calming activity you want to try next time you feel overwhelmed?

Where is your safe space (real or imagined) that helps you feel relaxed?

Write an affirmation you can repeat to yourself in difficult moments.
("I am strong. this moment will pass.")

Wow! This is so helpful - Thank you Noor! I will definitely be filling in one for myself.

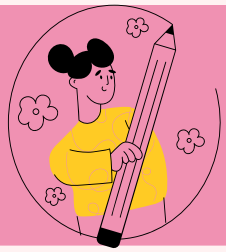
Do you have any suggestions for how to help a friend who might be in a similar situation? Just asking them to report or take action immediately can feel insensitive sometimes and I want to learn how to best support them!

You're right - a friend might be struggling emotionally and mentally because of online bullying, harassment, or negativity but they might not always ask for help! It is also possible that they have already reported the crime but are still feeling unsettled. I think knowing how to support our friends is really important and can make a huge difference.

SOCIAL FIRST AID: HOW TO BE A GOOD SUPPORT SYSTEM FOR A FRIEND IN DISTRESS

Active Listening - When a friend opens up about their struggles, resist the urge to immediately offer solutions. Instead, give them space to talk without interruptions. Let them express their emotions freely and acknowledge their feelings. Sometimes, knowing someone is listening without judgment can be more comforting than advice.

Check In & Follow Up - A small message like "Hey, how are you doing? What have you been up to?" can make a big difference. Even if they say they're fine, following up and checking in later shows that you genuinely care. If they've been dealing with online stress, bullying, or harassment, casual conversations can help them feel supported without pressure.



Help Set Boundaries - If they're facing online harassment or negativity, remind them that they have control over their space. Encourage them to block and report harmful users and adjust their privacy settings. If they're unsure how, offer to guide them through the process.!

You can even recommend this guidebook to help them better understand internet safety, privacy settings, and managing their time online. Having the right information can empower you and those around you to create a safer and healthier digital experience

Activity: Your Personal Safety Checklist

Being prepared can make a big difference in how you handle stressful or unsafe situations online. Complete the checklist below to ensure you have the right tools and support system in place.

- [ ] Choose at least one helpline from the list and save it in your phone or write it down somewhere easily accessible. In a crisis, knowing where to get help quickly can be very helpful.
- [ ] Think of two people you can turn to for support–this could be a family member, a teacher, a close friend. Write their names down so you remember during a crisis!
- [ ] Pick one calming strategy, like deep breathing, journaling, or grounding exercises. Practice using it when you feel overwhelmed!
- [ ] Practice one social first-aid strategy to help a friend in distress.

CHAPTER RECAP!

- [ ]  Be very careful of messages that ask for personal information, offer gifts or promises, demand pictures, or ask you to keep your conversation a secret!
- [ ] 

All messaging and social media platforms have mechanisms to report and block messages and profiles - you should always use these when in doubt!
- [ ]  If reporting and blocking online does not feel like enough, you can also report the crime to the Cyber Crime cell (ph. 1930 or cybercrime.gov.in, or 100 for your local police station)
- [ ]  Online threats can include: threats of violence or harm, sexual harassment or stalking, sharing private images without consent, impersonation, fraud, or identity theft
- [ ]  There are several laws under the IT Act 2000, Indian Penal Code 1860, and Consumer Protection Act 2019 that guarantee our rights as digital citizens!
- [ ]  Most importantly, remember that you are not alone! You have many loved ones and friends to support you, so reach out for help.

Chapter 6: Click, Scroll, Breathe: Mental Wellbeing in the Digital World

The internet is an incredible space–full of opportunities to learn, connect, and express ourselves. But just like any place in life, it can pose some its unique set of challenges. It is important to recognise those challenges, build healthy online habits, and make the most of our digital world while staying safe and in control.

Meera is scrolling through her phone late at night. She sees exciting updates from friends and funny videos. But she also sees negative news and comments that make her feel uneasy. She wakes up feeling exhausted the next morning.

Why do I feel so drained even though I've just been scrolling? Is it the content or just... too much of everything?

Looks like you've been scrolling for a while. Sometimes, being online can feel like a rollercoaster–one moment you're entertained, the next you're hit with things that weigh you down. It's okay to pause and check in with how it's making you feel.

Yeah, it's weird. Some things make me laugh, but then I see something upsetting, and suddenly I feel off.

Think about the last time you were online–not just on social media, but using any app or website. Whether it's news, shopping, or banking apps, how we interact with the internet can affect how we feel.

- Did browsing the news leave you feeling informed yet anxious?
- Did shopping provide a brief thrill but later lead to guilt?
- What time of day did you engage with the app or website?

Analysing these elements can help you can gain insight into the emotions that drive your internet usage and how the internet impacts your mood in return.

Activity

Internet Well-Being Scorecard

Instructions:

- Answer the following 10 questions honestly.
- For each statement, give yourself 1 point if you do it frequently.

Your Social Media Habits

1. I check my phone (social media, news, shopping apps) first thing in the morning.
2. I find it hard to stop scrolling, even when I have other things to do.
3. I feel stressed or anxious after reading news or seeing updates online.
4. I compare my life to what I see online—whether it's people, trends, or lifestyles.
5. I shop online even when I don't need anything, just to feel better.
6. I use the internet when I'm feeling sad, bored, or overwhelmed.
7. I've stayed up late, sacrificing sleep, just to keep browsing or scrolling.
8. I feel pressured to reply immediately to messages, comments, or notifications.
9. I've avoided real-life activities (hobbies, schoolwork, family time) because of being online.
10. I feel upset when my posts don't get enough likes, comments, or engagement.

Score Analysis

- 0–3 points – Great! You have a healthy relationship with social media.
- 4–6 points – Balanced! You're doing okay, but you might want to be mindful of a few habits.
- 7–10 points – Your social media use may be affecting your well-being. Time for a reset!

Reflection & Action

- Did anything surprise you about your score?
- What's one small change you can make to improve your digital well-being?

Think about which statements you checked and why. Were they related to a specific platform, app, or mood? Sometimes, certain triggers—like late-night boredom or stress—lead us to overuse the internet. Later in this chapter, we'll explore ways to make healthier choices.

Siddharth completed the Digital Champions Program two years ago, becoming a go-to guide for his friends on online safety. From spotting scams to setting privacy controls, he knew how to navigate the digital world responsibly. But lately, his parents seemed uneasy – news of digital crimes was everywhere, and their concern was growing.
One evening, over dinner, Siddharth finally asked,

Mom, Dad, do you ever worry about how much time I spend online?

We trust you and know that you've been using the internet with caution all these years. But lately, we've been seeing worrying trends in the news. We don't want to alarm you, but we do want to make sure you stay safe and vigilant–just like we would in a crowded place. We were also talking about this with Meera's parents the other day.

Should I not use internet at all then? Or use it only when I'm around you?

Absolutely not–taking away access isn't the solution. Let's work together to set some simple, practical ground rules that keep you safe while respecting your independence. We can set some limits and see how you feel.

Why Are We Always Told to Use The Internet Less Frequently?

It's a question many of us have– Why do adults keep saying, "Put that phone down?" It's not just about screen time; it's about what's happening behind the screen. Imagine social media as an ocean–vast, exciting, and full of opportunities to explore. Some areas have crystal-clear waters where you can learn, connect, and grow. But one may get lost in the hidden currents of doomscrolling sometimes. The internet is built to keep you engaged–content and notifications all modified and personalised especially for you. But we can choose to be mindful of how much time we spend online and what we're engaging with. The goal isn't to disconnect entirely but to stay in control–using the internet in ways that add value to our lives rather than distracting us from it.

Checklist: When Social Media Feels Like Too Much

Like Siddharth, we should all establish some basic guidelines regarding our internet usage. However, the first step is to identify what feels safe and what doesn't. Here are some ways to self-assess. If you notice yourself experiencing any of the following feelings, it may be time to take a moment to pause and reflect.

Feeling Anxious or Insecure
- Physical signs: heaviness in your chest, restlessness, or mood swings.

Constant Comparison
- You find yourself measuring your life against others' highlights.

Getting Angry or Sad from Interactions
- Conversations or comments leave you more stressed than before.

Losing Sleep
- You stay up late scrolling or refreshing your feed.

Feeling Disconnected
- You feel more isolated, even though you're "connected."

Overthinking Likes and Comments
- You keep replaying reactions in your head.

Emotional Drainage
- You feel exhausted or depleted after being online.

Remember, even your phone needs to recharge—so do you! If social media is making you feel more meh than yay, let's find ways to reset and feel better.

Everyone's journey online looks different—what works for one person may not work for another. Social media is great for connecting and learning, but we need to balance our digital life with our physical one. Real-life experiences are essential for growth, connection, and overall well-being and they ground us in their own unique ways.

Based on my experiences and research, here are some things that help create a healthier relationship with social media.

Building a Healthier Relationship with Social Media

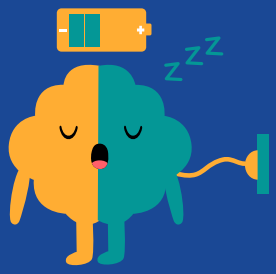
1. Follow positive and inspiring content.
2. Practice digital kindness by engaging in uplifting conversations.
3. Set daily limits for how long you spend on certain apps- using app timers.
4. Turn off notifications for apps that don't need your immediate attention.
5. Use the 'Do Not Disturb' feature when you need a break or time to focus.
6. Limit social media usage to avoid late-night scrolling and set up screen free zones at home
7. Use the "One-Night Rule" wherein you wait a day before posting anything.
8. When others' actions make social media stressful
   - Limit interaction with negative content.
   - Mute, unfollow, or block if necessary.
   - Talk to someone–friend, parent, teacher.
9. Use social media for learning and advocacy.

Happiness Menu

Remember, there's a whole world outside your screen! When the internet feels too heavy, take a step back–your life isn't just pixels and notifications. There's fresh air to breathe, real people to meet, and experiences waiting beyond the scroll. Your best moments aren't just online. Here's a Happiness Menu –a list of serotonin-boosting activities you can pick from to lift your mood and remind yourself that joy exists offline too!

- ○ Dance to your favorite song
- ○ Go for a walk in nature
- ○ Call a friend for a chat
- ○ Journal your thoughts
- ○ Play a sport
- ○ Paint, doodling or do art
- ○ Listen to uplifting music
- ○ Deep breathing or meditation
- ○ Cook or bake something
- ○ Do a random act of kindness
- ○ Watch the sunset
- ○ Visiti a place you love
- ○ Create a goal list
- ○ Take a relaxing bath
- ○ Reading a book or poetry
- ○ Letter to your future self
- ○ Declutter your space
- ○ Volunteer for a cause

The activities listed above are just a few examples. The key is to listen to your own needs and identify what works best for your mood and mental well-being. Start by asking yourself:



What makes me feel good and energised?
What helps me calm down when I'm overwhelmed?
What activities bring me joy or make me feel accomplished?

Once you identify these activities, incorporate them into your routine. Over time, these habits will help you create a balance between your online and offline life, ensuring that you remain in control rather than letting social media control you.

Taking care of your mental well-being means recognising that ups and downs are a natural part of life–including online life. Social media can be a space for learning, connection, and inspiration, but it can also bring moments of self-doubt or comparison. It's easy to feel like you're falling behind when you're constantly scrolling through highlight reels–but remember, what you see online is often a carefully crafted version of reality, not the full picture.

Think back to what we studied about disinformation and misinformation–just as false news can spread, so can unrealistic digital personas, people often share only the best parts of their lives, making things seem more perfect than they really are. But behind every post is a real person with struggles, insecurities, and challenges just like yours.

It's important to remind yourself that what you see isn't always the full story. Instead of comparing your reality to someone's highlight reel, focus on what truly brings you joy and fulfillment.

Your happiness is more important than likes and comments on your posts or the number of followers you have!

Over time, I've learned that it's important to be intentional about how I use the internet. I used to think that I had to be online all the time to stay up to date, but I've realised that that's not sustainable. Now, I try to be more mindful about my time online and set boundaries so that I don't get sucked in. I also make sure to schedule in time for things that help me recharge, like spending time with friends and family, being in nature, or simply taking some time to myself. It's not always easy, but I've found that it's worth it in the long run.

RECAP: CLICK, SCROLL, BREATHE!

PAY ATTENTION TO HOW YOU FEEL ONLINE.

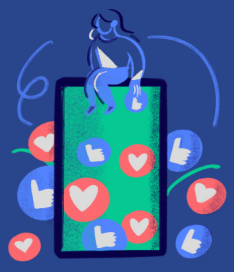
The internet can be fun, but it's important to notice how it affects your emotions. If you feel anxious, sad, or exhausted after being online, it's a sign to pause and take a break.

FIND A HEALTHY BALANCE BETWEEN ONLINE AND OFFLINE LIFE.

Spending too much time online can affect your sleep, mood, and focus. Make space for real-life activities like hobbies, spending time with friends, and enjoying the world beyond your screen.

SET CLEAR BOUNDARIES TO PROTECT YOUR WELL-BEING.

Small actions like turning off unnecessary notifications, setting time limits for social media, and avoiding late night scrolling can help you stay in control of your digital habits.



REMEMBER, SOCIAL MEDIA ISN'T THE FULL PICTURE.

What you see online is a highlight reel and not real life. Avoid comparing yourself to others and focus on what makes you happy and fulfilled in your own life.

REACH OUT IF SOMETHING FEELS WRONG.

If the internet ever feels overwhelming or unsafe, talk to someone you trust. You're not alone, and there's always help available when you need it.

Chapter 7: Trending for Change: Using the Internet for Good

Noor had always thought of the internet as just a place for learning and entertainment, but her perspective had started to shift. Now, as she worked on her civics project, she couldn't stop thinking about the role of young people online–and how she could do more with what she had learned.

Amit Bhaiya, I've been reflecting on how we use the internet. It's so awesome how people coming together online can make such a big impact, and it's really cool to see voices that don't usually get heard.

Absolutely! The internet is really a community space and each one of contribute to shaping the shared expereince- we can make it joyful and useful- if we put in the work!

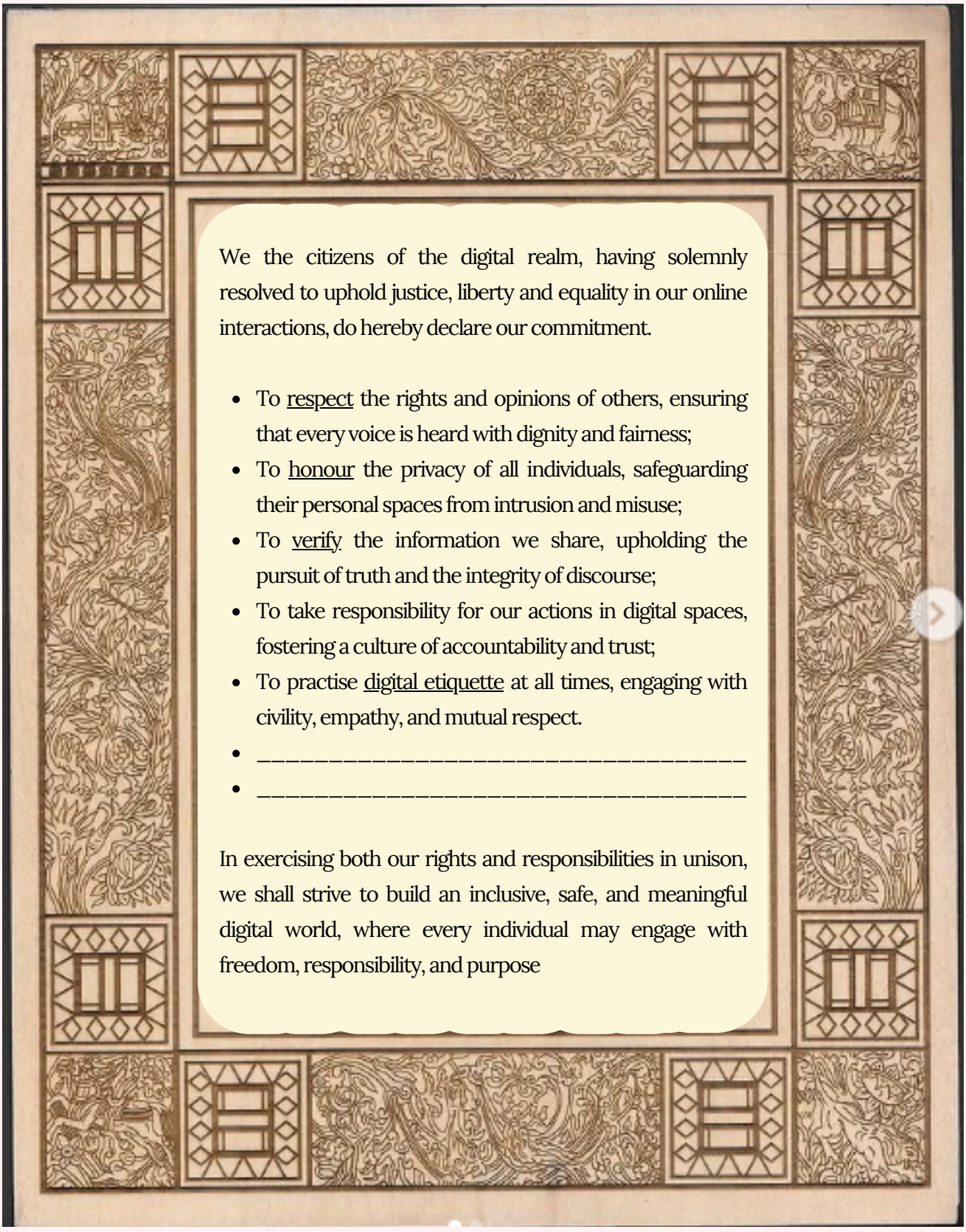
I like thinking of the internet as a community space! In fact, aren't we as much digital citizens as we are citizens of India?

Yes! with similar rights and responsibilities!

You're right! I wonder what the preamble would look like if we made one for digital citizens

RESPONSIBILITIES AS A DIGITAL CITIZEN

Noor created a Preamble which included some non negotiable points that she felt all digital citizens must abide by. Discuss with your friends and add two responsibilities that you think should be included here!



We the citizens of the digital realm, having solemnly resolved to uphold justice, liberty and equality in our online interactions, do hereby declare our commitment.

- To respect the rights and opinions of others, ensuring that every voice is heard with dignity and fairness;
- To honour the privacy of all individuals, safeguarding their personal spaces from intrusion and misuse;
- To verify the information we share, upholding the pursuit of truth and the integrity of discourse;
- To take responsibility for our actions in digital spaces, fostering a culture of accountability and trust;
- To practise digital etiquette at all times, engaging with civility, empathy, and mutual respect.
- _____
- _____

In exercising both our rights and responsibilities in unison, we shall strive to build an inclusive, safe, and meaningful digital world, where every individual may engage with freedom, responsibility, and purpose

CHANGEMAKERS

Noor! The preamble you created for digital citizens has gone viral! Everyone in school has been talking about it!

We had a discussion in our civics class about rights and responsibilities, and a bunch of people brought up digital citizenship too!

Thank you friends!

It's amazing! I love how you are sparking conversations beyond just our group.

Like Maliha Abidi? I've been inspired by them, and was thinking of how I can start something that makes an impact as well!

Well, I'm sure you can! But who is Maliha Abidi and what do they do?

Maliha Abidi is a 23-year-old artist and writer. She is from Karachi, currently studying Neuroscience at the University of Sussex while also continuing her passion for art and spirit for women empowerment through various projects, one of them being her upcoming book "Pakistan for Women".

Yes! Resources online have been helpful in building better understanding of causes I care about!

That's amazing! So people are using the internet to do so much good!

Learning and Growing

- Many platforms offer learning support to students. These come in various combinations of study material for school subjects, preparation for board and competitive exams, tutoring, homework help, etc.
- Leveraging resources online, we can also learn about issues and causes that we are passionate about- by looking at research and hearing different perspectives from people involved.

Just last week Siddharth had raised funds for a friend's medical expenses using crowdfunding. We can show up for each other and orgainse!

Peer and Community Advocacy

- Social Media Mobilisation - Activists use popular social media and messaging platforms to spread messages rapidly, launch viral campaigns, and engage broad audiences. Hashtags, live videos, and digital petitions help amplify causes, making it easier to rally supporters and drive public discourse.
- Community Coordination and Direct Action - Organisers leverage online forums, mailing lists, and messaging apps to plan logistics, share resources, and keep participants engaged. Crowdsourcing platforms and digital sign-ups facilitate collective action, enabling people to pledge support and contribute funds!

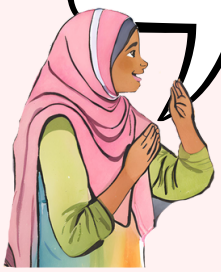
CHANGEMAKERS

It's amazing how much we can learn and do online, but that also means we have a responsibility to make it a better space, right?

Yeah, exactly! It's not just about using the internet, but also about how we interact with others and make sure it stays a positive place

Maybe we could make a checklist of things to think about before we post or reply to someone?

Good idea! You know, one of the coolest things about the internet is getting to hear from people we don't usually see in the news or on TV



Yeah, but I've also started noticing how some people get way more hate online. I feel like we should do something– whether it's reporting, speaking up, or just showing support.

Kinder Conversations

- ☐ Is it kind? (Will this make someone feel good or bad?)
- ☐ Is it necessary? (Do I really need to say this?)
- ☐ Is it respectful? (Would I be okay if someone said this to me?)
- ☐ Is it accurate? (Have I fact-checked this information?)
- ☐ Does it respect privacy? (Am I sharing someone's personal details without permission?)

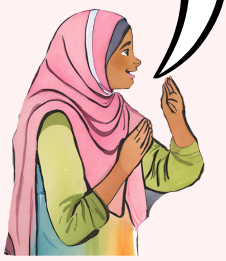
Showing Support

- Call it out – If it's safe, reply with facts or a calm response to challenge harmful content.
- Report & block – Use platform tools to report hate speech and prevent further harm.
- Encourage kindness – Shift the conversation by promoting respectful and inclusive discussions.

CONVERSATIONS AND ACTIONS

Makes sense!! We can be can online just like we are in real life? But beyond just being careful with what we say, is there more we can actually do to make the internet a better space

Yeah! I mean, we're all part of different groups–our families, schools, even online communities. There must be ways to bring what we've learned into those spaces too, right



Exactly! There are things we can do at different levels–at home, in our schools, in our friend groups, and even in the larger online space. It all adds up!

ACTION

Change begins at home!

- Teach younger siblings or family members about privacy settings and digital well-being.
- Help parents identify fake news or online scams.
- Start a conversation about healthy screen time habits.

A friend indeed

- Call out harmful jokes, cyberbullying, or inappropriate content.
- Support friends who feel unsafe or overwhelmed online.
- Encourage responsible sharing–remind them to fact-check

Ambassadors at School

- Organize a Digital Kindness Campaign–where students post positive messages for each other.
- Start an awareness club to discuss online safety and digital rights.
- Work with teachers to host workshops on responsible internet use and identify student ambassadors.

Conversations With Community

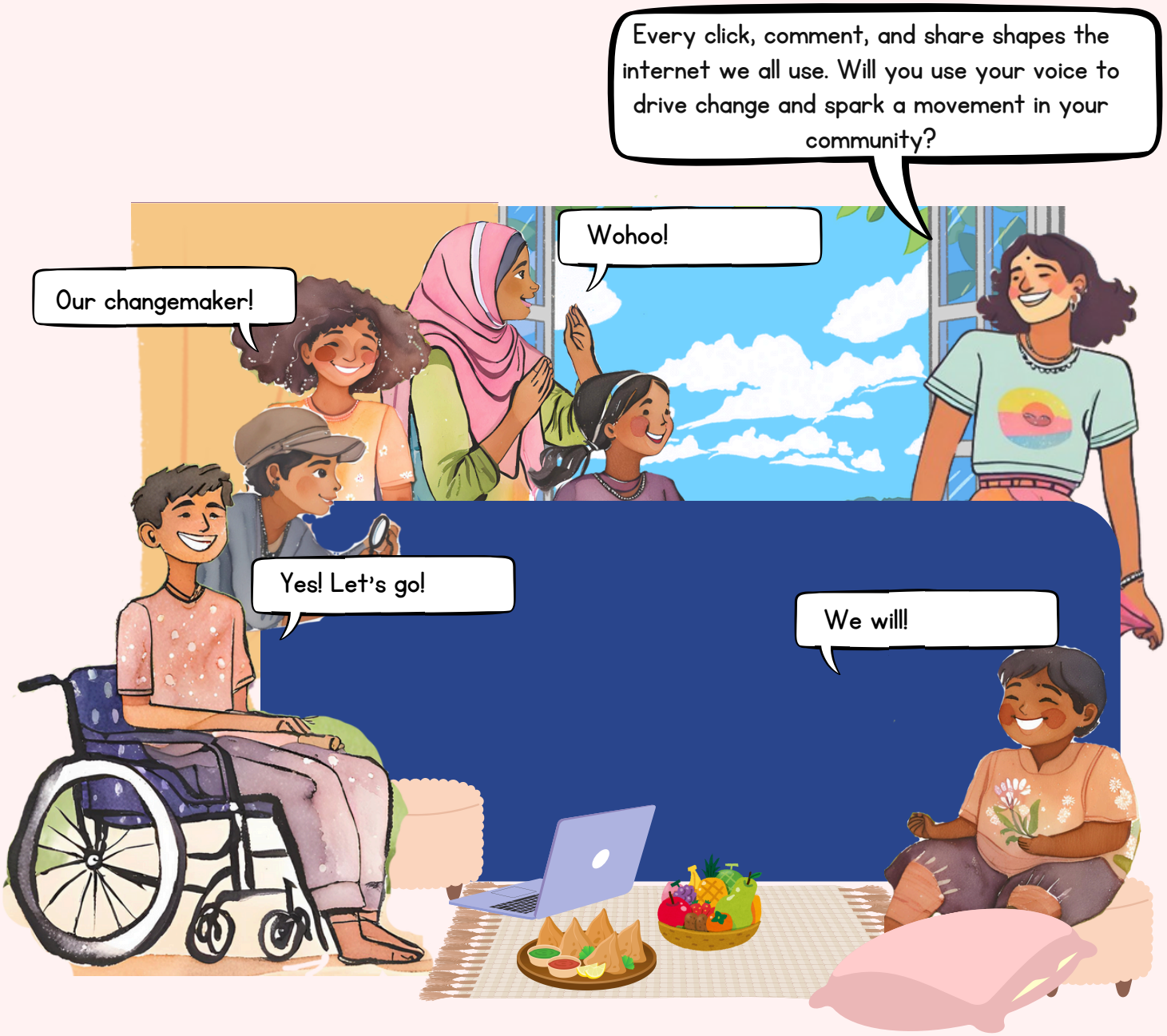
- Spread awareness about online scams and misinformation with local groups.
- Advocate for stronger cyber safety policies in schools and youth spaces.
- Share verified resources on mental health, online harassment, and support networks.

These are amazing ideas, Shubham. Our online futures are shaped by us, just as much as the internet shapes our online experiences.

You are right! I actually have an idea about something I now want to try- Noor, I'll need some help!!

Ofcourse! I'll let everyone know we're meeting tomorrow afternoon!

Once again, the friends were back together. This time around it wasn't just a chill afternoon of lazing around. Shubham had a mission for the team, and everyone was waiting to hear more.

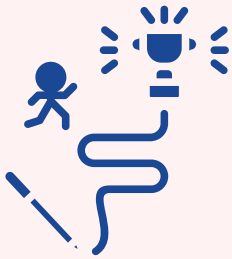


Shubham handed out worksheets and pens to everyone, along with a mission statement to guide their thinking. Scroll down to see the mission statement and what they came up with in 30 minutes! Keep scrolling to check out their final action plan.

Agents of Suraksha Nagar,

Your community needs you. The growing threat of garbage and pollution is compromising our streets, our air, and our future. This is a call to action—assemble your allies, spread the word, and deploy solutions. From awareness campaigns to cleanup drives, every action counts. The mission is clear: restore Suraksha Nagar's safety and cleanliness.

Will you rise to the challenge? If you're ready to make a difference, create your plan of action now!



Goal: Restore Suraksha Nagar's safety and cleanliness through community action and digital advocacy

1 month for awareness + 2 weekly cleanup drives + ongoing social media engagement.

Shubham – The Creative Designer

- Learn to design posters using Canva.
- Create eye-catching visuals with the campaign hashtag to share online and around the community.

Rahim – The Reel Maker

- Film and edits short reels highlighting the pollution problem and community efforts.
- Post videos on social media to spread awareness.

Susan – The Community Connector

- Manage the Suraksha Nagar messaging group.
- Invite neighbors, share updates, and remind everyone about cleanup events.

Meera – The Social Media Captain

- Create and run a dedicated campaign page (e.g., @CleanSuraksha).
- Regularly post progress updates, success stories, and ways for people to contribute.

Siddharth – The Researcher & Informer

- Gather facts about pollution, waste management, and eco-friendly practices.
- Write informative posts and share tips for reducing waste in daily life.

Noor – The Event Organiser

- Plan and coordinate cleanup drives and awareness events.
- Make digital sign-up forms and schedules for volunteers.

Jaspreet – The Hashtag Hero

- Monitor the #CleanSuraksha hashtag.
- Encourage people to use the hashtag when sharing their own cleanup actions, building a sense of collective effort.

Define your own mission and design a plan of action to tackle a cause that you care about!

Mission:

Goal:

Timeline:

Activities:

Roles and responsibilities:

CHAPTER RECAP!

- [ ]  As digital citizens we have both, rights as well as responsibilities like respecting the rights, opinions and privacy of others
- [ ] 

The internet can be used as a powerful force for good! We can use it to advocate for changes we want to see in the world!
- [ ]  The internet can also be used to learn and grow, to build community and peer groups, and to show support to others!
- [ ]  Always ask yourself, are my actions and words kind? Are they respectful?
- [ ]  Change begins at home! You can start conversations with your family and friends, become an ambassador at school, and call out harmful behaviour around you

BIBLIOGRAPHY

Chapter 1

- 88% of kids watch online videos- Global kids online report MICA
- World's First Website.
- How many websites are there?
- The weight of the internet.
- Number of People using Google.
- The first emoji ever created.

Chapter 2

- Cyber Security - Awareness for Citizens. Cyber Crime Portal.
- Don't fall prey to these scams! 10 common ways in which scamsters can fraud you.
- 3. Minding the data: Protecting learners' privacy and security.

Chapter 3

- Different types of Bullying
- What are cyber crimes?
- Respecting Privacy
- Cache and cookies:

Chapter 4

- Rest assured, salt is not poisoning you.
- Evaluating Resources and Misinformation.
- How do algorithms work?
- How does AI work? Basics to know.

Chapter 5

- National Cyber Crime Reporting Portal
- Online Hate and free speech
- IT Laws India
- Blue Whale Challenge

BIBLIOGRAPHY

Chapter 6

- Mental health resources
- A commitment planner to balance your time use.
- How to identify and help a friend struggling with mental health issues

Chapter 7

- Safetinterview with Maliha Abidi
- Using internet based tools to promote community health and development
- Digital Safety and Citizenship Curriculum