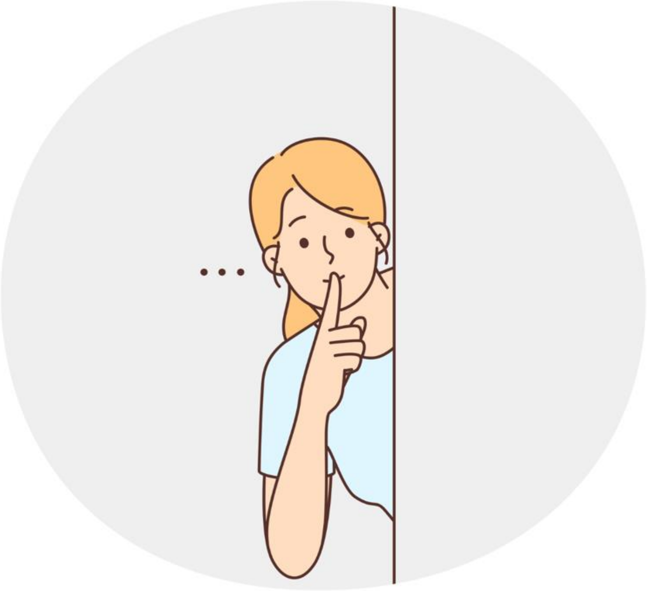
CYBERSAFETY

EMPOWERING A CYBER-SAFE SOCIETY

How To Stay Safe Online

What’s in this document?

You will find out everything you need to know to stay safe and private online. We explain how to use social media safely and how to manage cookies and general privacy tips.

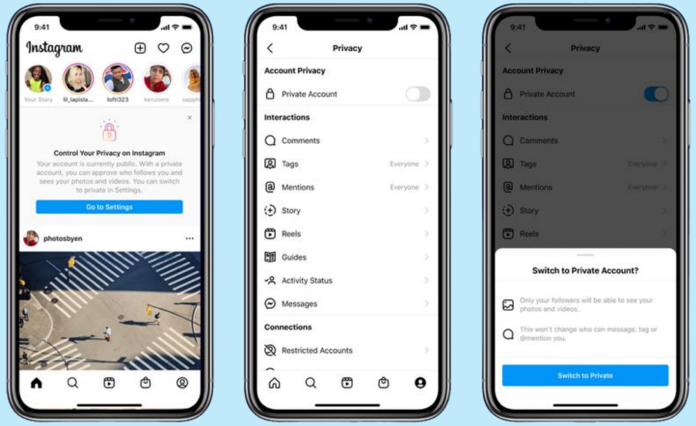


What Does “Staying Private” Mean?

When you are online, it’s important to **keep your information safe**.

This means:

- Only sharing things with people you trust
- Making your social media profile **private**
- Keeping your passwords secret



Control Your Privacy on Instagram

Your account is currently public. With a private account, you can approve who follows you and sees your photos and videos. You can switch to private in Settings.

Switch to Private Account?

Only your followers will be able to see your photos and videos.

This won't change who can message, tag or @mention you.

Public vs. Private Profiles

- Your **profile** is your page on apps like Facebook or Instagram.

There are two types of profiles:

- **Public**: Anyone can see your posts and pictures
- **Private**: Only people you choose can see what you share

✅ **It’s safer to have a private profile.**

To stay private on social media, you can:

- Ask someone you trust to help you change your settings
- Only accept friend requests from people you know

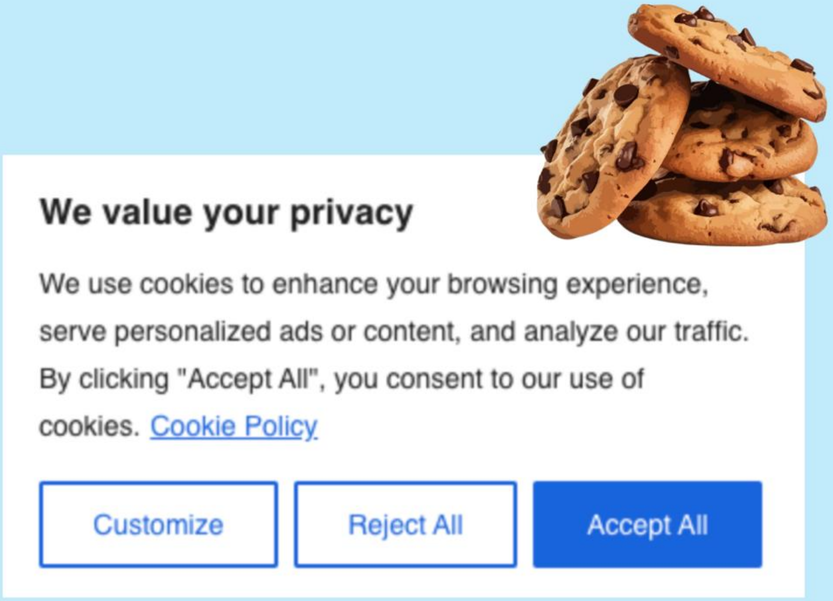
Sharing Information Online

It’s easy to share too much information online, but some things should stay **private**.

Don’t share:

- Your home address or phone number
- Your email or password
- Where you are right now

Cookies!

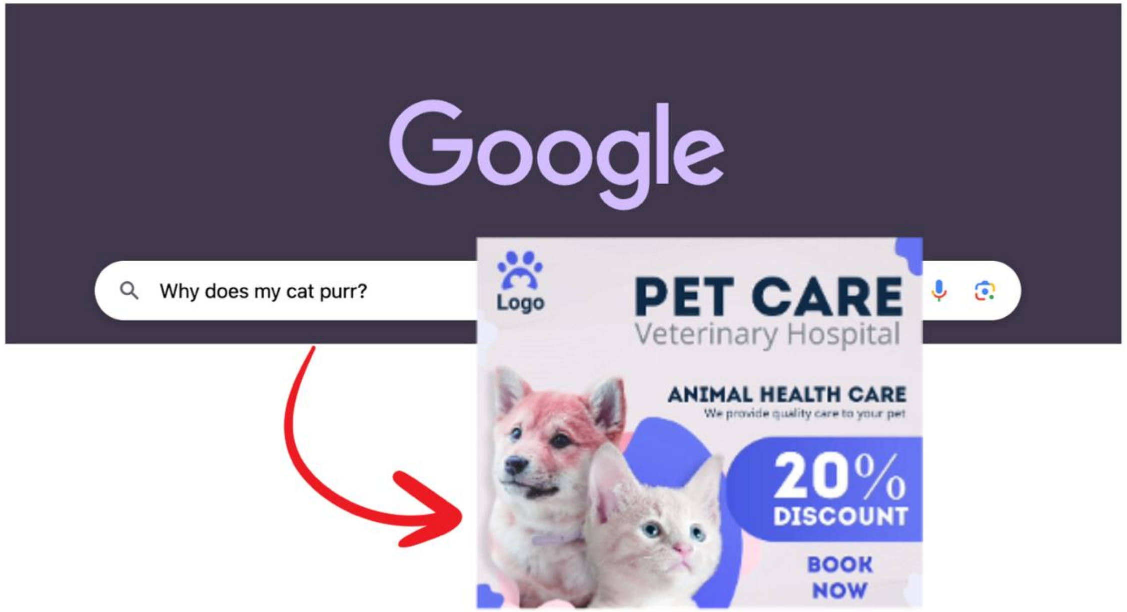


We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies. Cookie Policy

What Are Cookies? (Not the food kind!)

- **Cookies** are small files that websites use to **remember you**.



For example:

- You look up “Why does my cat purr?” on Google
- Later, you see ads online about cats or vets
- This happens because of **cookies**

Types of Cookies

There are two kinds:

- **Necessary Cookies** (okay to accept)
- **3rd Party Cookies** (You can say NO to these)

✅ Necessary cookies (Okay to accept):

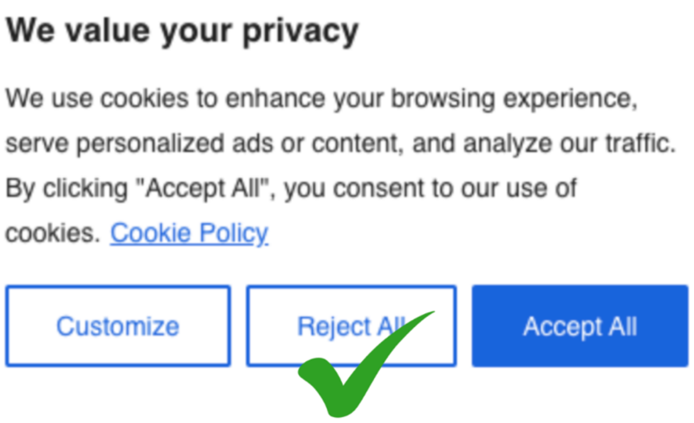
- Help websites remember your password
- Keep items in your shopping basket

🛑 3rd party cookies (You can say NO):

- Track what websites you visit
- Show you ads

You don’t need to say yes to 3rd party cookies.

You can **reject them** and still use the website.



We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies. Cookie Policy

What to Do With Cookie Messages

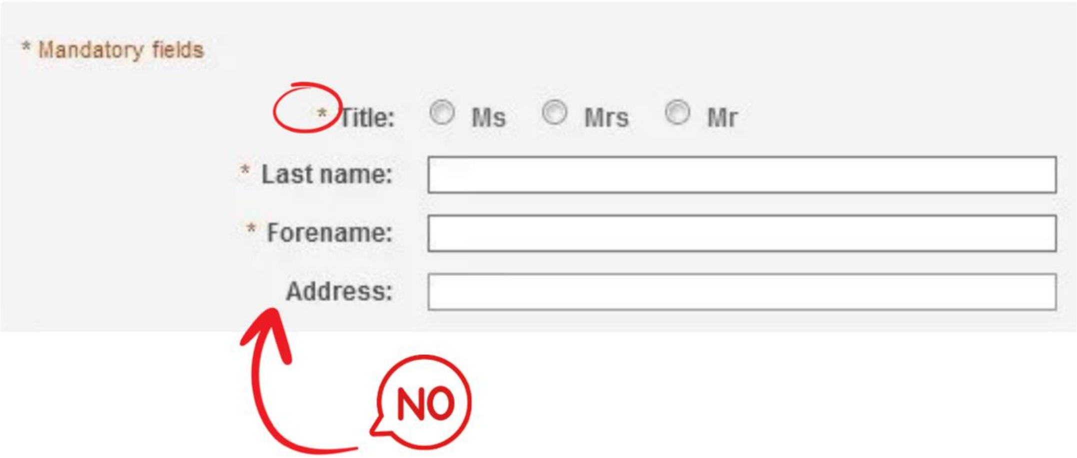
Sometimes, a box pops up asking about cookies.

You can choose:

- **Accept All** – says yes to every cookie
- **Reject All** – says no to the ones you don’t need

✅ **Try this: Next time, click “Reject All”.**

How To Stay More Private Online



* Mandatory fields

* Title: ○ Ms ○ Mrs ○ Mr

* Last name:

* Forename:

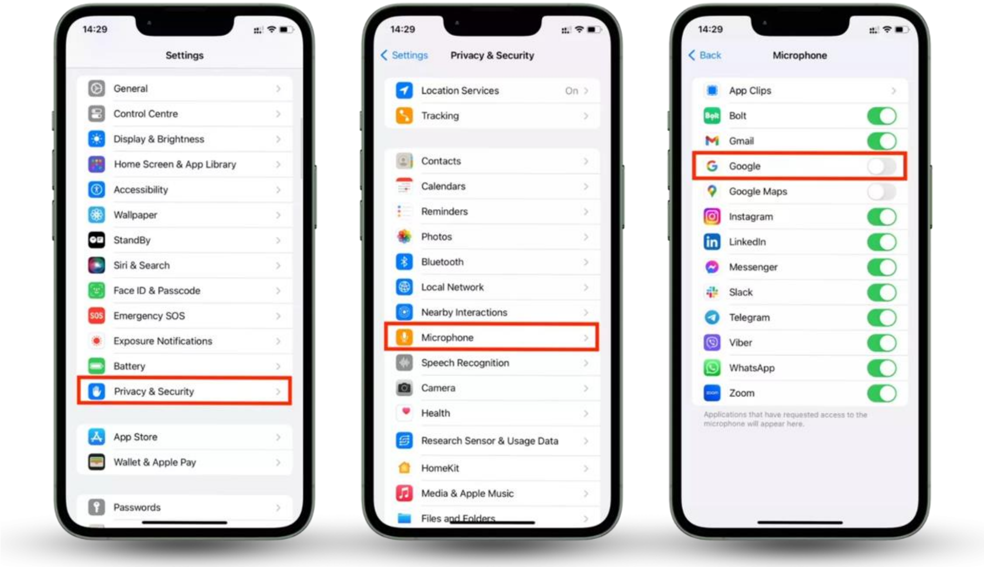
Address:

If you're filling out a form online, check:

- **Does this form really need that information?**
- If there is a * star symbol, then you have to fill it in.
- Ask someone you trust if you’re not sure.

Cover your camera

- Put a **sticker** or **tape** on your computer or phone camera when you’re not using it.
- This helps keep your space private.



App Clips

Bolt ●

Gmail ●

Google ○

Google Maps ○

Instagram ●

LinkedIn ●

Messenger ●

Slack ●

Telegram ●

Viber ●

WhatsApp ●

Zoom ●

Applications that have requested access to the microphone will appear here.

Turn off your microphone

- Some apps **don’t need your microphone**.

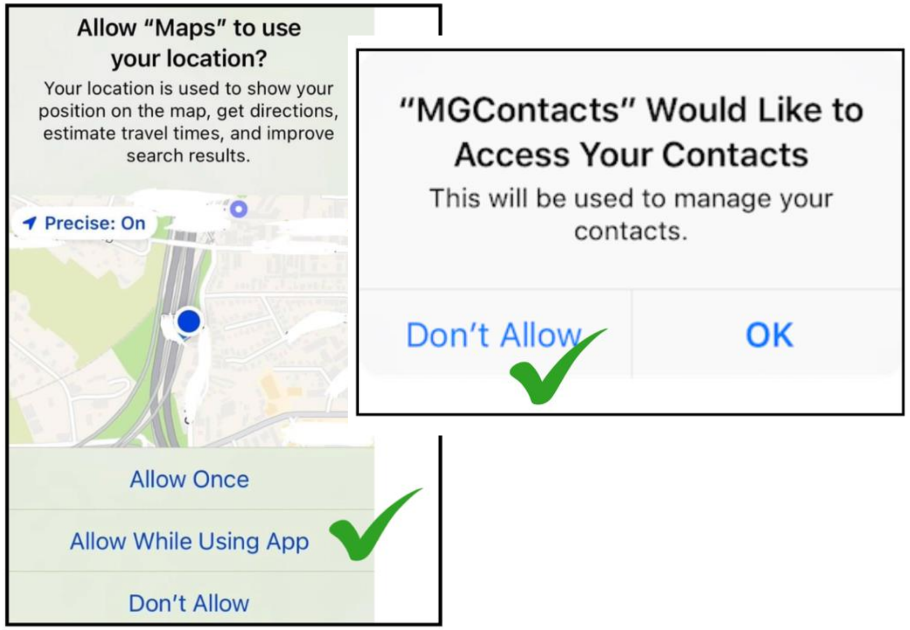
  Turning it off keeps your privacy safer.

- Ask someone to help you turn off the microphone

Apps that need microphones:

- WhatsApp
- Voice command apps like Siri, Alexa, or Google Assistant

These apps need a microphone so you can send voice messages or talk to the app.



Allow "Maps" to use your location?

Your location is used to show your position on the map, get directions, estimate travel times, and improve search results.

"MGContacts" Would Like to Access Your Contacts

This will be used to manage your contacts.

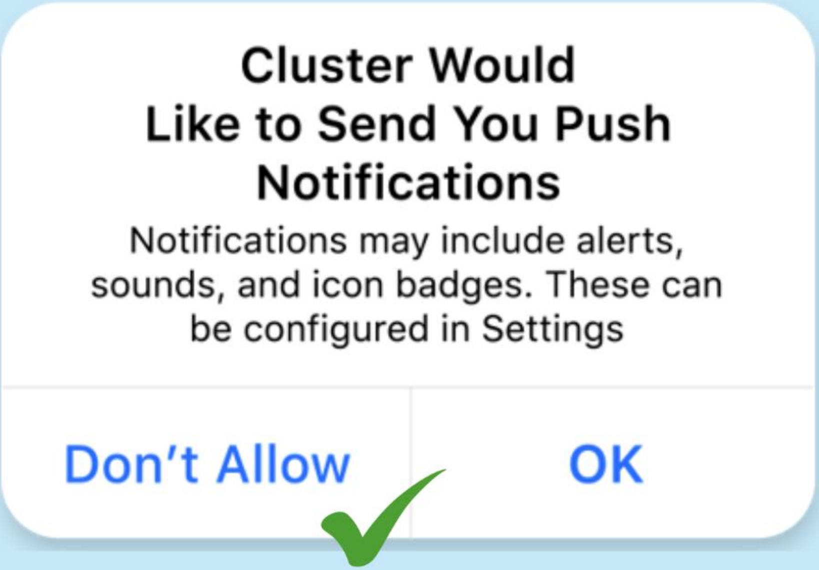
📍 Be careful with location and contacts

Some apps or websites will ask:

- "Can we use your location?"
- "Can we see your contacts?"

🛑 **Say "No"** unless the app really needs it.

✅ OK examples: Google Maps, food delivery apps like Just Eat.



Cluster Would Like to Send You Push Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings

🔔 Say "No" to notifications

If a website asks, **"Can we send you updates?"**

- 🛑 Click **"No"** or **"Don't allow."**

This helps stop spam or pop-ups that you don't want.

Social Media

What Is a Social Media Profile?

A social media profile is your page or account on apps like:

- Facebook
- Instagram
- TikTok
- Snapchat
- WhatsApp

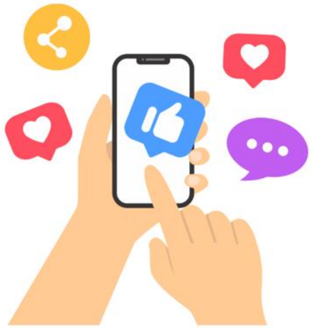
📷 Be careful with photos

Only post photos you'd be happy with:

- Family
- Your boss
- Your support worker to see.

If you post photos of friends:

- **Ask first** if they are OK with it



Don’t share too much

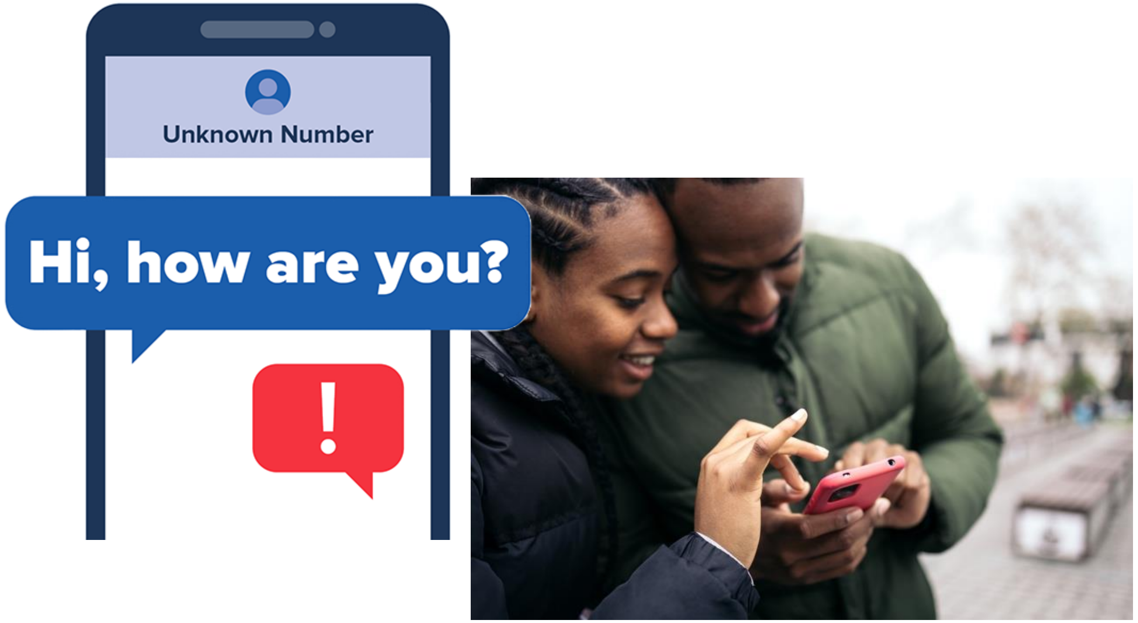
Don’t post:

- Where you live
- Where you are right now (like at a concert)

Tip: Post about the event **after** it ends.

👥 Friend requests

- Only accept friend requests from people you **know in real life**.
- If you're not sure, **ask someone you trust**.



🚫 **If someone strange messages you:**

- **Do not reply**
- **Show someone you trust**

They can help you decide what to do

💬 **Think before you post**

Ask yourself:

- "Is this kind?"
- "Would I want someone to post this about me?"
- **Do not share or forward** mean messages.

Post things that are friendly and respectful. If you're not sure, ask for help before posting.

Cyberbullying

👎 What Is Cyberbullying?

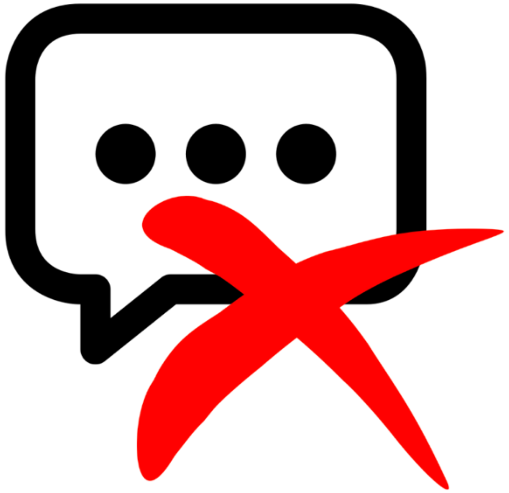
Cyberbullying is when someone is **mean or hurtful online**.

This can happen on:

- Social media (like Facebook or TikTok)
- In text messages
- On games or apps

Cyberbullying can include:

- Mean messages
- Threats
- Lies about you
- Sharing private photos or videos without asking



What Not to Do.

Don’t reply to mean messages.

- If someone says something **mean or upsetting, do not answer** them.
- Answering back can make it **worse**.

What You Should Do - Tell someone you trust.

Talk to:

- A parent
- A teacher
- A carer or support worker
- A friend you trust

It’s not your fault. You are not alone.

Save the messages.

Keep proof of the bullying:

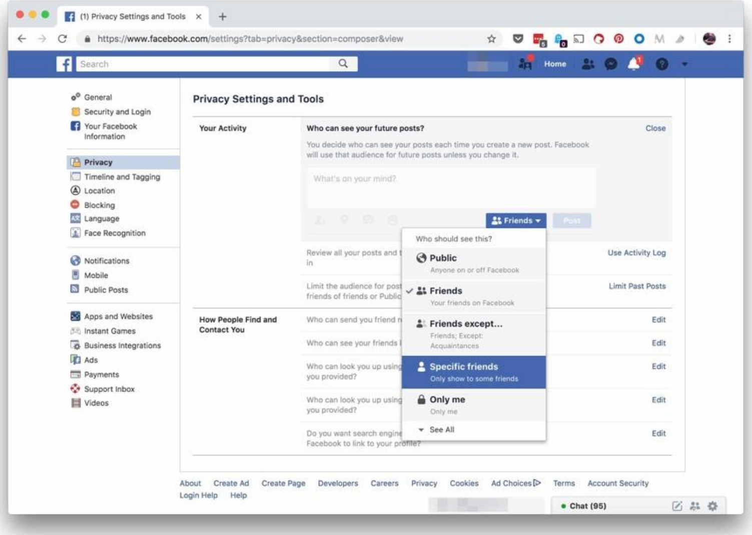
- Take screenshots
- Save messages, pictures, or videos

Someone you trust can help you save them.

Block and report the bully

You can:

- **Block** the person so they can’t contact you again
- Use the **“Report” button** on the app or website
- Ask for help if you don’t know how to do this.



Privacy Settings and Tools

Your Activity

Who can see your future posts? Close

You decide who can see your posts each time you create a new post. Facebook will use that audience for future posts unless you change it.

What's on your mind?

Friends ▾ Post

Who should see this?

- Public — Anyone on or off Facebook
- ✓ Friends — Your friends on Facebook
- Friends except... — Friends; Except: Acquaintances
- Specific friends — Only show to some friends
- Only me — Only me
- See All

Review all your posts and t in — Use Activity Log

Limit the audience for post friends of friends or Public — Limit Past Posts

How People Find and Contact You

Who can send you friend r — Edit

Who can see your friends l — Edit

Who can look you up using you provided? — Edit

Who can look you up using you provided? — Edit

Do you want search engine Facebook to link to your profile? — Edit

Use Privacy Settings

Make your accounts **private**.

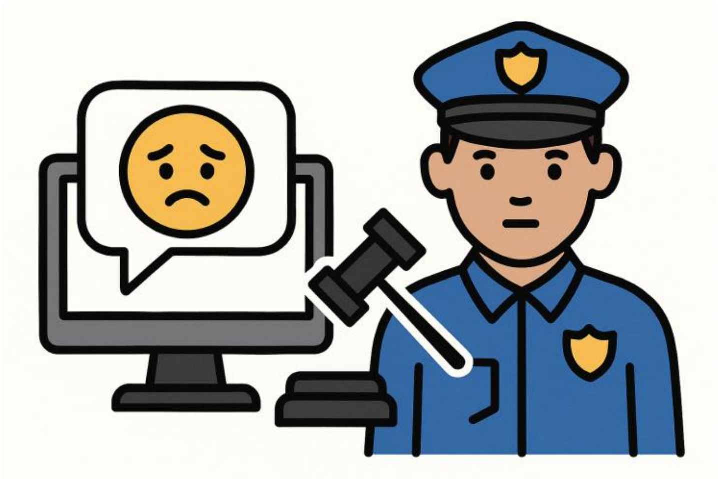
- Only people you know and trust should see your posts.
- You can ask someone to help you change your settings.

Be careful who you talk to

If someone you **don’t know** sends a message or friend request:

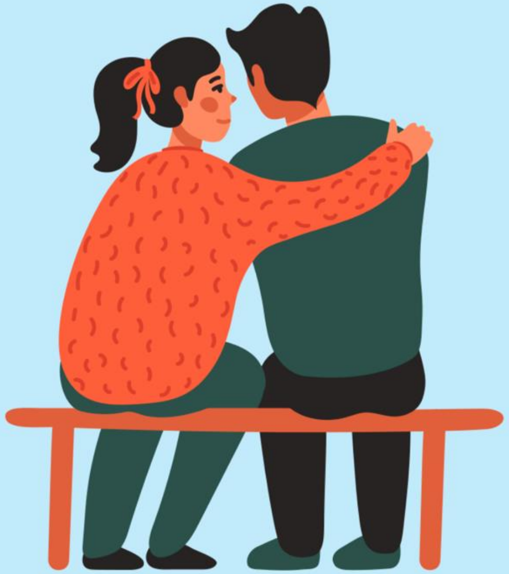
- Don’t accept it
- Don’t talk to them

They may pretend to be nice but later be mean.



Is Cyberbullying Against the Law?

- In many places, being mean or threatening online is **against the law**.
- People who bully may be **reported to the police**.



If you are bullied:

- You have done **nothing wrong**
- You can get help

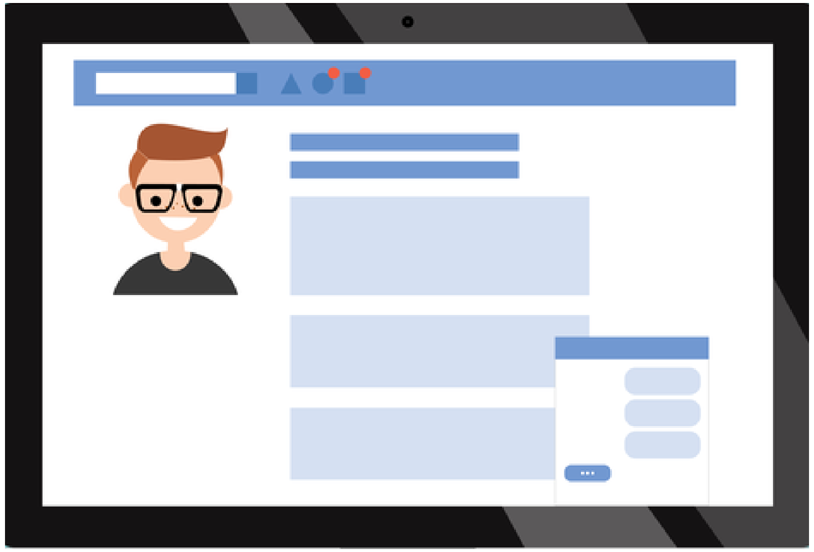
It's OK to take a break

If the internet is upsetting you:

- Log off
- Take a break
- Talk to someone about how you feel

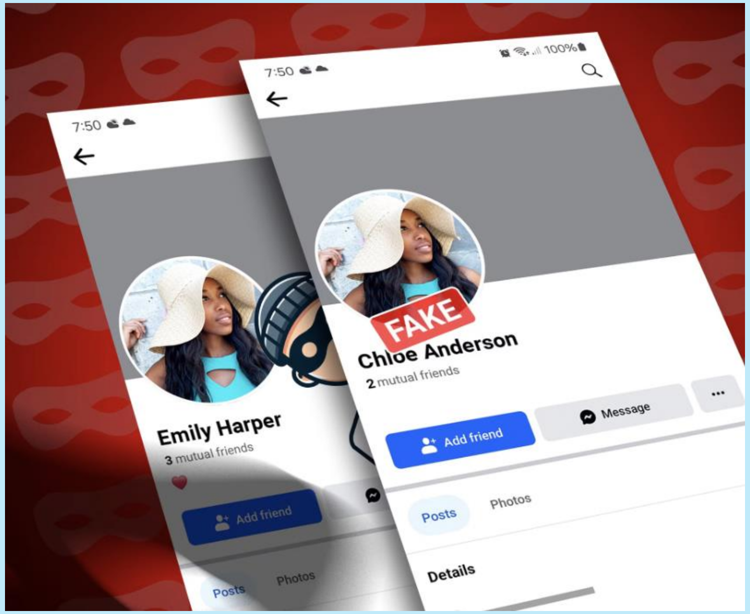
You don't have to stay in a place that makes you feel bad.

Fake Or Real?



A Social Media Profile usually has:

- Your name
- A photo
- Posts or videos
- Friends or followers



What Is a Fake Profile?

A fake profile is when someone:

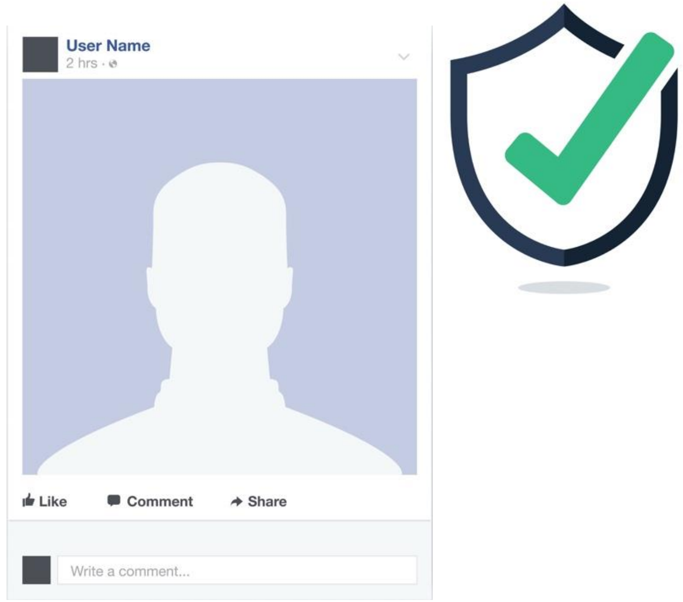
- Pretends to be someone else
- Uses a fake name or fake photo
- Lies about who they are, where they live, or what they want

People use fake profiles to:

- Trick people into talking to them
- Steal money or private information
- Spread lies or fake news

How To Spot a Fake Profile - Watch out for these signs:

- Strange or perfect-looking photos
- No friends or very few followers
- They ask for money, gifts, or private info
- Their posts don’t make sense or are copied
- They ask to move the chat to WhatsApp or Snapchat quickly
- They refuse to video call or meet in real life



What Is a Trusted Profile?

A trusted profile:

- Belongs to a real person or company
- Has a clear name and photo
- Has regular posts that make sense
- Doesn’t ask for personal details or money

What Is Fake News?

Fake news is when someone shares wrong information on purpose:

- They may use AI, fake photos, or made-up stories
- It might try to make people angry or scared
- It may be used to sell things or win support

How To Stay Safe Online

✅ DO:

- Check if the profile looks real (photos, posts, friends)
- Ask someone you trust if something seems strange
- Block and report people who ask for money or private info
- Use your privacy settings to protect yourself

❌ DON'T:

- Talk to strangers who make you feel uncomfortable
- Share your password, private photos, or bank info
- Send money to people you only know online
- Click on links from people you don't know

What To Do If You're Not Sure

- Stop and check before replying or clicking
- Ask someone you trust — like a friend, carer, or support worker
- Report fake or suspicious profiles on the app

Catfishing

What is Catfishing?

- Catfishing is when someone pretends to be someone else online
- They may use a fake name, fake photos, or lie about their age, job, or identity

Why Do People Catfish?

People catfish for different reasons:

- To trick or scam others out of money
- To get attention or feel better about themselves
- Because they are lonely or want to escape real life
- To bully, control or abuse someone emotionally

They might catfish on:

- Social media (like Facebook or Instagram)
- Dating apps
- Chatrooms or online games

Here are some ways to spot a catfish:

- They won’t video chat or meet in person
- They ask for money, gifts, or personal details
- Their photos look like models or are found in many places online
- They fall in love or want to be close very quickly
- Their stories don’t make sense or keep changing

What Are the Dangers?

Catfishing can hurt people in many ways:

- Feeling embarrassed, hurt, or betrayed
- Being manipulated into sending money or private photos
- Losing trust in others
- In serious cases, it can lead to emotional abuse or threats

What To Do If You Think You're Being Catfished?

- Stop talking to the person right away
- Tell someone you trust, like a support worker or family member
- Block and report the person on the app or website
- Ask for help from an online safety service or support group

How Can You Stay Safe?

✅ DO:

- Talk to someone you trust about your online relationships
- Keep personal information private (like your address, phone number, or bank info)
- Use privacy settings on your accounts
- Ask someone to help you check if photos or stories are real

❌ DON’T:

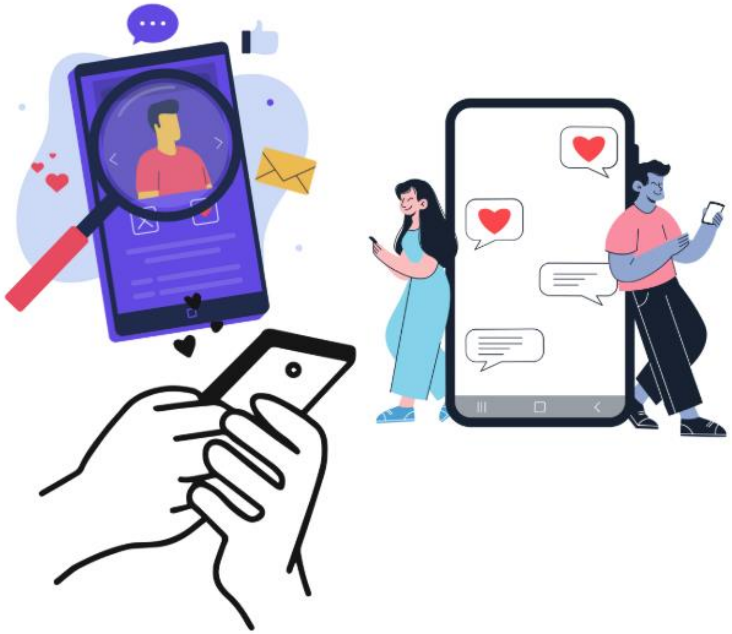
- Send money or gift cards to someone you don’t know
- Share private photos or passwords online
- Rush into relationships without knowing someone well
- Keep secrets if someone online makes you feel uncomfortable

Sextortion

What is Sextortion?

Sextortion is when someone:

- Tricks or pressures you into sharing naked photos or videos
- Then threaten you to get more photos, money, or private information



How Does Sextortion Happen?

Sextortion can happen:

- On social media, dating apps, or chat websites
- When someone pretends to be nice or friendly
- If someone sends you sexual photos and asks for photos back
- If you’ve already shared photos, they may blackmail you

What Do They Say?

The person might say things like:

- “Send me more photos or I’ll tell your family.”
- “Give me money or I’ll share your pictures online.”
- “If you don’t do what I say, I’ll ruin your life.”

Why Is Sextortion So Dangerous? It can make people feel:

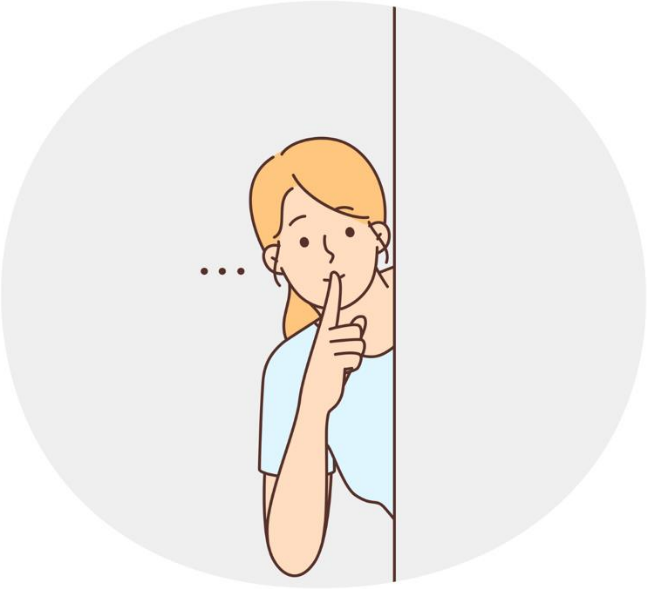
- Scared, ashamed, or confused
- Like they have no choice
- Worried about what others will think
- Unsafe online or in real life

People with learning disabilities may be targeted more often

It's Never Your Fault

If someone tricks or threatens you:

- You are not to blame
- The person who is threatening you is doing something wrong
- You deserve help and support



How To Stay Safe

✅ **DO:**

- Be careful who you talk to online
- Keep your photos and videos private
- Talk to someone you trust if something feels wrong
- Report or block people who ask for sexual photos

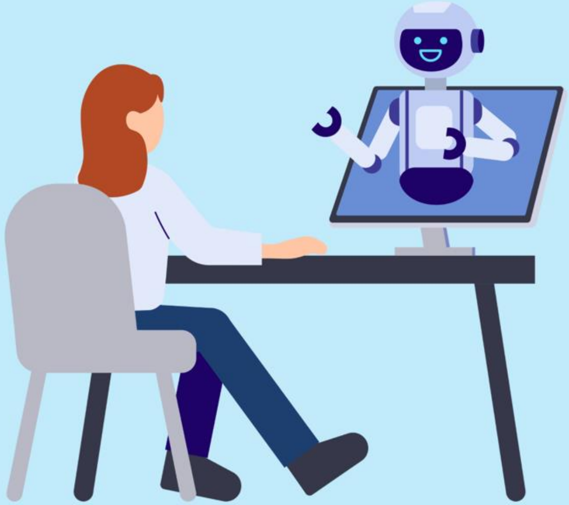
❌ **DON'T:**

- Send naked photos to someone you don't know well
- Share photos just because someone asks or pressures you
- Keep it a secret if someone is threatening you

What To Do If It Happens to You

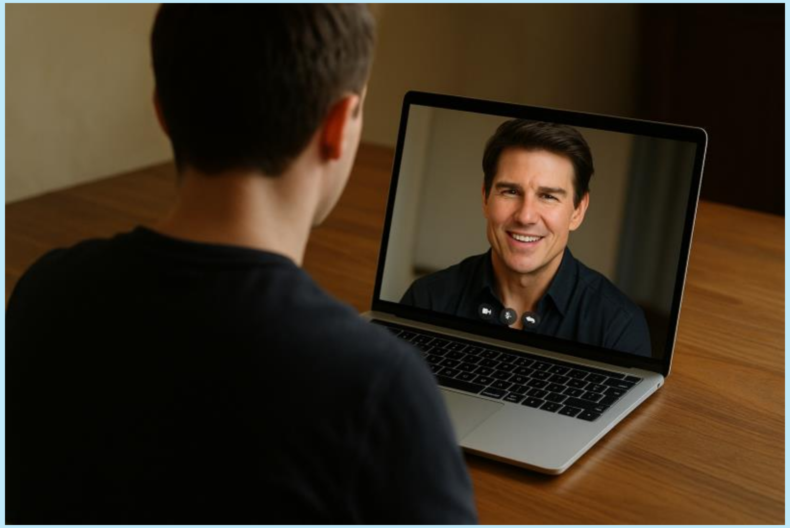
- Stop talking to the person right away
- Don’t send more photos or money
- Take screenshots of any threats or messages
- Tell someone you trust (like a support worker, friend, or family member)
- Report it to the app, website, or police

Artificial Intelligence (AI)



What is AI?

- AI (Artificial Intelligence) is when computers act smart, like people.
- AI is a computer program that learns from lots of information, like what's on the Internet. You can ask it questions or give it tasks, and it will try to help you. It's like Google, but smarter. It doesn't just find websites; it understands and gives you full answers.



AI can:

- Write messages or stories
- Make fake photos or videos
- Pretend to talk like a real person

AI can be helpful, but some people use it to trick or scam others

What is AI Misinformation?

Misinformation means wrong or fake information.

AI misinformation is when people use AI to create:

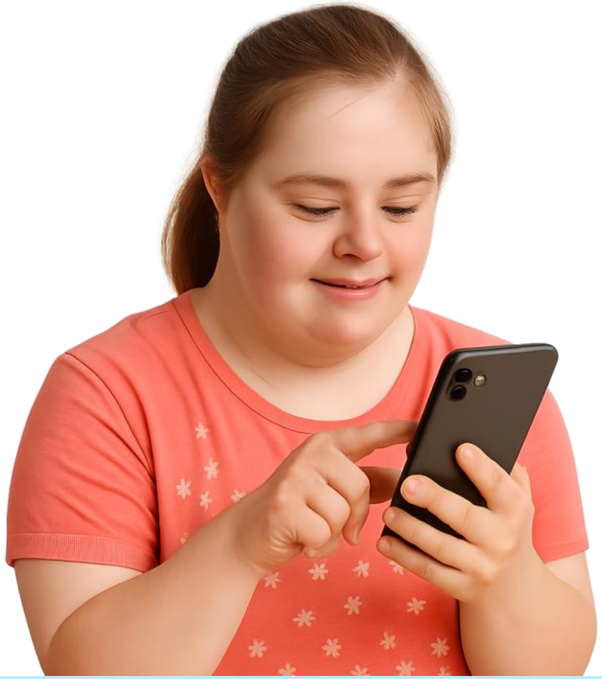
- Fake news
- False health advice
- Scary or confusing stories

Sometimes, AI makes it look real — but it’s not true.

What are AI-Generated Scams?

Some scammers use AI to:

- Copy voices and pretend to be a friend or family member
- Write fake messages that look real
- Make videos or photos that are not real
- Trick people into sending money or private details



Who Is Most at Risk of AI-Generated Scams?

People with disabilities, including learning disabilities, may be targeted more often:

- Because scammers think they are easier to trick
- Some people may trust others too quickly
- Some may not know how to check if something is fake

Signs of an AI Scam

Watch out if:

- Someone sounds like your friend or relative, but asks for money or help fast
- You get strange texts or emails with links
- A video looks odd, or their mouth and voice don’t match
- A message makes you feel scared or that you have to act fast

How To Stay Safe

✅ **DO**:

- Ask a trusted person if you're unsure about something
- Use two-step login if possible (like a password + code)
- Hang up and call back if someone says they're from a bank or family

❌ **DON'T:**

- Click on strange links or buttons
- Share your bank details, passwords, or photos with people you don't know
- Send money if someone says it's an emergency without checking

What To Do If You Think It's a Scam

- Stop talking to the person
- Tell someone you trust right away
- Report it to the app, website, or police
- Don’t send any money or information

🆘 Ask for help

If something online:

- Feels wrong
- Is confusing
- Makes you uncomfortable

👉 Talk to someone you trust — like a support worker, carer, or family member.

👉 Ask for help if you are using a new app or website.

CYBERSAFETY
EMPOWERING A CYBER-SAFE SOCIETY

Where to Get Help

- A trusted person (e.g., support worker or family member)
- Visit www.cybersafety.ie, where there is are list of more organisations and groups, such as the Crime Victims Helpline, that can help.
- You are never on your own. Help is always available.

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

NATIONAL CYBER SECURITY CENTRE
NCSC

CYBER EXPLORE

NATIONAL CHALLENGE FUND
From Ingenuity to Research and Solutions

Rialtas na hÉireann
Government of Ireland

Taighde Éireann
Research Ireland

Maoinithe ag an Aontas Eorpach
Funded by the European Union
NextGenerationEU